PENGEMBANGAN APLIKASI AKUISISI FORENSIK DIGITAL MENGGUNAKAN SISTEM OPERASI LINUX DEBIAN

Disusun Oleh:

N a m a : Anfika Sigma Prashinta
NIM : 16523114

PROGRAM STUDI INFORMATIKA – PROGRAM SARJANA
FAKULTAS TEKNOLOGI INDUSTRI
UNIVERSITAS ISLAM INDONESIA
2020

HALAMAN PENGESAHAN DOSEN PEMBIMBING

PENGEMBANGAN APLIKASI AKUISISI FORENSIK DIGITAL MENGGUNAKAN SISTEM OPERASI LINUX DEBIAN

TUGAS AKHIR

Disusun Oleh:

N a m a : Anfika Sigma Prashinta
NIM : 16523114

Yogyakarta, 13 Juli 2020

Pembimbing,

(Fietyata Yudha, S.Kom., M.Kom.)

HALAMAN PENGESAHAN DOSEN PENGUJI

PENGEMBANGAN APLIKASI AKUISISI FORENSIK DIGITAL MENGGUNAKAN SISTEM OPERASI LINUX DEBIAN

TUGAS AKHIR

Telah dipertahankan di depan sidang penguji sebagai salah satu syarat untuk memperoleh gelar Sarjana Komputer dari Program Studi Informatika di Fakultas Teknologi Industri Universitas Islam Indonesia

Yogyakarta, 13 Agustus 20120

Tim Penguji

Fietyata Yudha, S.Kom., M.Kom. _____

Anggota 1

Aridhanyati Arifin, S.T., M.Sc. _____

Anggota 2

Sri Mulyati, S.Kom., M.Kom. _____

Mengetahui,

Ketua Program Studi Informatika – Program Sarjana

Fakultas Teknologi Industri

Universitas Islam Indonesia

(Dr. Raden Teduh Dirgahayu, S.T., M.Sc.)

HALAMAN PERNYATAAN KEASLIAN TUGAS AKHIR

Yang bertanda tangan di bawah ini:

Nama : Anfika Sigma Prashinta

NIM : 16523114

Tugas akhir dengan judul:

PENGEMBANGAN APLIKASI AKUISISI FORENSIK DIGITAL MENGGUNAKAN SISTEM OPERASI LINUX DEBIAN

Menyatakan bahwa seluruh komponen dan isi dalam tugas akhir ini adalah hasil karya saya sendiri. Apabila dikemudian hari terbukti ada beberapa bagian dari karya ini adalah bukan hasil karya sendiri, tugas akhir yang diajukan sebagai hasil karya sendiri ini siap ditarik kembali dan siap menanggung resiko dan konsekuensi apapun.

Demikian surat pernyataan ini dibuat, semoga dapat dipergunakan sebagaimana mestinya.

Yogyakarta, 13 Juli 2020

(Anfika Sigma Prashinta)

HALAMAN PERSEMBAHAN

Alhamdulillah segala puji bagi Allah SWT atas rahmat dan hidayah-Nya penulis dapat menyelesaikan penyusunan tugas akhir ini. Shalawat dan salam senantiasa tercurahkan kepada Nabi Muhammad SAW, keluarga serta sahabat-sahabatnya. Semoga kelak kita mendapatkan syafa'at beliau di hari akhir nanti.

Selama penyusunan tugas akhir ini, penulis selalu dalam bimbingan, dorongan, dan bantuan baik bersifat materil maupun spiritual dari berbagai pihak. Oleh karena itu penulis mengucapkan ucapan terimakasih dan penghargaan setinggi-tingginya kepada:

1. Allah SWT, karena berkat rahmat dan karunia-Nya penulis dapat menyelesaikan tugas akhir ini.
2. Terimakasih kepada Ibu Sri Sujatmi yang senantiasa mendoakan dan membimbing anakmu dengan tulus.
3. Terimakasih kepada Bapak Dwi Supriyanto tercinta yang senantiasa mendoakan dan membimbing anakmu dengan tulus.
4. Kepada saudaraku yang kusayangi Unfika Shaffa Prashinta
5. Keluarga besar dari simbah Sutrisno dan simbah Susilo Saputro yang selalu memberikan motivasi kepada penulis.
6. Bapak Fietyata Yudha, S. Kom., M. Kom selaku dosen pembimbing tugas akhir yang telah bersedia meluangkan waktu ditengah-tengah kesibukannya untuk membimbing dan memberi dukungan dalam menyelesaikan tugas akhir ini.
7. Kepada sahabat-sahabat yang selalu menemani penulis selama menimba ilmu di Universitas Islam Indonesia.
8. Teman-teman Prodi Informatika angkatan 2016 yang selalu menemani penulis selama menimba ilmu di Prodi Informatika Universitas Islam Indoneisa.

HALAMAN MOTO

“Pendidikan adalah senjata paling mematikan di dunia, karena dengan pendidikan, Anda dapat mengubah dunia.”

(Nelson Mandela)

“Anak lelaki tak boleh dihiraukan panjang, hidupnya ialah untuk berjuang. Kalau perahunya telah dikayuhnya ke tengah dia tak boleh surut meski bagaimana besar gelombang. Biarkan kemudian patah, biarkan layar robek, itu lebih mulia, dari pada membalik haluan pulang.”

(Buya Hamka)

KATA PENGANTAR

بِسْمِ اللَّهِ الرَّحْمَٰنِ الرَّحِيمِ

Assalamualaikum Warahmatullahi Wabarakatuh.

Alhamdulillahirabbil'alamin. Puji syukur kepada Allah SWT atas rahmat dan karunia-Nya, sehingga penulis dapat menyelesaikan laporan tugas akhir ini. Shalawat serta salam kepada Nabi Muhammad SAW beserta para sahabatnya yang telah berjuang hingga kita bisa menikmati zaman sekarang yang kaya akan ilmu pengetahuan.

Tugas akhir tersebut diajukan untuk memenuhi salah satu syarat untuk memperoleh gelar sarhana pada program S1 Informatika, Fakultas Teknologi Industri, Universitas Islam Indoneisa.

Selama penyusunan tugas akhir ini, penulis selalu dalam bimbingan, dorongan, dan bantuan baik bersifat materil maupun spiritual dari berbagai pihak. Oleh karena itu penulis mengucapkan ucapan terimakasih dan penghargaan setinggi-tingginya kepada:

1. Allah SWT, karena berkat rahmat dan karunia-Nya penulis dapat menyelesaikan tugas akhir ini.
2. Bapak Prof. Fathul Wahid, ST., M.Sc., Ph.D., selaku rektor Universitas Islam Indonesia (UII) Yogyakarta.
3. Bapak Prof. Dr. Ir. Hari Purnomo, M.T. selaku dekan Fakultas Teknologi Industri Universitas Islam Indonesia (UII) Yogyakarta.
4. Bapak Dr. Raden Teduh Dirgahayu, S.T., M.Sc. selaku Ketua Prodi Studi Informatika Universitas Islam Indonesia (UII) Yogyakarta.
5. Bapak dan ibu dosen Informatika yang telah membimbing dan memberika ilmu kepada penulis selama menimba ilmu di Prodi Informtaika Universitas Islam Indonesia.
6. Bapak Fietyata Yudha, S. Kom., M. Kom selaku dosen pembimbing tugas akhir yang telah bersedia meluangkan waktu ditengah-tengah kesibukannya untuk membimbing dan memberi dukungan dalam menyelesaikan tugas akhir ini.
7. Segenap karyawan Fakultas Teknologi Industri Universitas Islam Indonesia yang telah membantu dari segi administrasi selama penulis menimba ilmu di Prodi Informatika.
8. Terimakasih kepada Ibu Sri Sujatmi yang senantiasa mendoakan dan membimbing anakmu dengan tulus.

9. Terimakasih kepada Bapak Dwi Supriyanto tercinta yang senantiasa mendoakan dan membimbing anakmu dengan tulus.
10. Kepada saudaraku yang kusayangi Unfika Shaffa Prashinta.
11. Kepada sahabat-sahabat yang selalu menemani penulis selama menimba ilmu di Universitas Islam Indonesia.
12. Teman-teman Hexadecima yang selalu menemani penulis selama menimba ilmu di Prodi Informatika Universitas Islam Indoneisa.
13. Teman-teman KKN unit 243

Penulis menyadari bahwa tugas akhir ini terdapat banyak kesalahan dan kekurangan dikarenakan kurangnya pengelaman dan ilmu pengetahuan. Maka, penulis mengharapkan kritik dan saran yang membangun untuk menyempurnakan tugas akhir ini. Dan semoga Laporan Kerja Praktik ini dapat bermanfaat bagi para pembacanya. Harapan penulis terhadap penelitian tugas akhir yang telah diselesaikan.

Penulis ucapkan terimaksih.

Wassalamualaikum Warahmatullahi Wabarakatuh.

Yogyakarta, 13 Juli 2020

(Anfika Sigma Prashinta)

SARI

Sebuah ilmu dari forensik seperti pemulihan dan investigasi dari perangkat digital, sering kali ada kaitannya dengan kejahatan komputer biasa disebut forensik digital. Akuisisi merupakan suatu proses penggandaan berupa barang bukti seperti media penyimpanan digital dengan pengambilannya bit demi bit. Pada penelitian ini untuk mendapatkan hasil akuisisi media penyimpanan dibutuhkan aplikasi untuk melakukan akuisisi media penyimpan, maka dikembangkannya aplikasi akuisisi forensik digital dengan hasil ekstensi .dd menggunakan sistem operasi linux debian.

Aplikasi mampu melakukan akuisisi media penyimpanan *flasdrive* dengan format *file* yang dihasilkan .dd dan .log yang berisikan informasi media penyimpanan yang diakuisisi. Aplikasi akuisisi forensik digital menggunakan sistem operasi linux debian telah diuji kecepatan transfer datanya yaitu sebesar 3,85 MB/s lebih cepat dari pada penelitian sebelumnya.

Kata kunci: Forensik Digital, Akuisisi.

GLOSARIUM

GUI	Antarmuka aplikasi yang ditampilkan dalam bentuk grafis agar mempermudah pengguna aplikasi.
Cybercrime	Segala akses illegal atau akses secara tidak sah terhadap data sehingga dalam suatu sistem komputer merupakan suatu kejahatan.
File	Identitas dari data yang disimpan di dalam sistem berkas yang dapat diakses dan diatur oleh pengguna.
Flash drive	Media penyimpanan berupa USB yang memliki bentuk yang kecil.
Debian	Sistem operasi yang digunakan peneliti.

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

BAB I
PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi dari waktu ke waktu ada saja beberapa pihak yang memanfaatkan untuk melakukan hal-hal yang negatif yang mengarah pada kejahatan. Segala macam penggunaan jaringan komputer untuk tujuan kriminal dana atau kriminal berteknologi tinggi dengan menyalah gunakan kemudahan teknologi digital disebut *cybercrime* (Riadi, 2018). Dilansir dari situs *cnnindonesia.com* Wakil kepala kepolisian RI Komisaris Jenderal Syafruddin mengatakan bahwa Indonesia masuk dalam jajaran dua besar negara di dunia dengan kejahatan di dunia maya atau *cybercrime*, Syafruddin mengatakan bahwa data yang dihimpun pihaknya mendapati 90 juta kali serangan terjadi di Indonesia selama Januari hingga akhir Juni 2016 (CNN Indonesia, 2018).

Kejahatan siber pun kini semakin 'bertumbuh subur'. Berdasarkan data yang diperoleh Okezone dari Direktorat Tindak Pidana Kejahatan Siber (Dit Tipidsiber) Bareskrim Polri sepanjang 2017, yakni Januari-Oktober, jajaran Polri di Indonesia menangani 1.763 kasus kejahatan siber. Dari angka tersebut, polri setidaknya sudah menyelesaikan perkara (crime clearance) *cybercrime* sebanyak 835 kasus. Penyelesaian kasus itu dikategorikan dari berkas perkara dinyatakan lengkap (P21) atau surat permohonan penghentian proses penyidikan (SP3). Dalam data tersebut, kejahatan siber yang paling tinggi adalah penipuan (Batubara, 2017). Menurut Menteri Kominfo Rudiantara, dalam ranah "*cybercrime*" Indonesia memiliki UU Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE). "UU ITE mengatur perbuatan-perbuatan yang dilarang serta ancaman pidananya. Selain itu, dalam UU ITE itu juga mengatur mengenai bukti digital," kata Rudiantara usai Kick Off Pembentukan Asosiasi Forensik Digital Indonesia, di Press Room, Kantor Kementerian Kominfo, Selasa (17/11). Menurut Menkominfo, bukti digital dianggap sah dan dapat diajukan ke persidangan dengan syarat bahwa informasi yang tercantum di dalamnya secara teknis dapat diakses, ditampilkan, dijamin keutuhannya, dan dapat dipertanggung jawabkan. "Maka diperlukan tindakan forensik digital yang terdiri atas pengumpulan, akuisisi, pemulihan, penyimpanan, dan pemeriksaan bukti digital berdasarkan cara dan dengan alat yang dapat dipertanggung jawabkan secara ilmiah untuk kepentingan pembuktian," kata Rudiantara (YDR, 2015).

Saat ini banyak aplikasi yang dapat digunakan, mulai dari yang berbayar hingga gratis. Secara garis besar perangkat untuk kepentingan forensik komputer dibedakan berdasarkan *hardware* dan *software*, namun baik dari sisi *hardware* dan *software* perangkat forensik

komputer diharapkan memenuhi 5 fungsi yaitu, untuk kepentingan akuisisi (*aquisition*), validasi dan diskriminasi (*validation and discrimination*), ekstraksi (*extraction*), rekontruksi (*reconstruction*) dan pelaporan (*reporting*) (Prayudi & Alfrianto, 2007).

Forensik digital sering dikenal sebagai digital forensik ilmu adalah cabang dari ilmu forensik meliputi pemulihan dan investigasi dari bahan yang ditemukan dalam perangkat digital, seringkali dalam kaitannya dengan kejahatan komputer. Dalam buku Forensic Examination of Digital Evidence, terdapat 4 tahap untuk memproses bukti digital, yaitu: Assessment; pemeriksa computer forensic harus menilai bukti digital sepenuhnya dengan mematuhi ruang lingkup dari kasus untuk menentukan tindakan yang harus diambil, Acquisition; Secara alami, bukti digital rentan dan dapat diubah, rusak, atau dihancurkan oleh pemeriksaan atau penanganan yang tidak tepat. Pemeriksaan yang paling tepat dilakukan pada copy dari bukti asli tersebut. Bukti asli harus diperoleh dengan cara melindungi dan mempertahankan integritas dari bukti tersebut, Examination; Tujuan dari proses ini adalah untuk mengekstrak dan menganalisis bukti digital. Ekstrak disini mengacu pada proses pemulihan data (recovery data) dari sebuah media. Analisisnya mengacu pada penafsiran dari data dan menempatkannya dalam format logis dan berguna, dan Documenting dan reporting; Tindakan dan observasi harus didokumentasikan selama proses forensic berlangsung. Hal ini termasuk dengan persiapan laporan tertulis dari temuan yang ada (U.s. Department of Justice, 2014).

Debian merupakan sistem operasi komputer sebagai perangkat lunak, serta menggunakan kernel linux yang bersifat bebas dan terbuka. Debian dapat digunakan pada beragam perangkat keras mulai dari komputer, laptop, dan dapat dijalankan divirtual box. Debian banyak digunakan karena keberagamannya yang memuat lebih dari 29000 paket perangkat lunak. Sistem operasi debian yang ringan sehingga dapat memasangnya dengan minimal HDD sebesar 1,6 GB (untuk server) dan 600MB (untuk *client* dan *workstation*) (Kunicki, 2020).

Penelitian yang berjudul "FORENSIC IMAGING APPLICATION USING RASPBERRY PI" sudah ada sebelumnya namun kecepatan transfer data membutuhkan waktu lama. Kemudian aplikasi diuji coba menggunakan enam buah media penyimpanan dan mendapatkan waktu serta kecepatan transfer data yang berbeda-beda namun kecepatan rata-rata transfer data pada aplikasi dalam proses akuisisi yaitu: 1,85 MB/s. Peneliti memberikan saran untuk meningkatkan kecepatan transfer data sehingga proses akuisisi yang berjalan dapat lebih cepat (K, 2018).

Penelitian ini dilakukan untuk mengembangkan aplikasi akuisisi forensik digital menggunakan bahasa pemrograman *python*. Dalam mengembangkan aplikasi untuk mengoperasikan aplikasi akuisisi forensik digital, maka dibuatlah aplikasi yang berbasis *Graphical User Interfaces* (GUI) supaya memudahkan pengguna dalam interaksi dengan aplikasi akuisisi forensik digital. Dengan ini peneliti mampu mengembangkan aplikasi akuisisi forensik digital yang dapat melakukan akuisisi media penyimpanan berbasis *Graphical User Interfaces* (GUI).

1.2 Rumusan Masalah

Berdasarkan latar masalah diatas, penulis merumuskan pertanyaan penelitian sebagai berikut:

a. Bagaimana mengembangkan aplikasi berbasis GUI untuk mengoperasikan akuisisi forensik digital?
b. Bagaimana mengetahui kecepatan transfer data aplikasi terbaru dalam memperoleh hasil akuisisi?

1.3 Batasan Masalah

Agar pengerjaan lebih terarah, dalam penelitian ini terdapat beberapa batasan masalah, diantaranya:

a. Hasil akuisisi*(Imaging)* media penyimpanan.
b. Format file yang dihasilkan .dd.

1.4 Tujuan Penelitian

Adapun tujuan dari peneliti yang ingin dicapai pada penelitian ini yaitu:

a. Mengembangkan aplikasi berbasis GUI menggunakan sistem operasi linux debian untuk mengoperasikan akuisisi forensik digital.
b. Menghitung kecepatan transfer data akuisisi dari aplikasi akuisisi forensik digital menggunakan sistem operasi linux debian.

1.5 Strategi Penyelesaian

Untuk menyelesaikan masalah atau menjawab pertanyaan penelitian, ada beberapa penyelesaian yaitu:

a. Membuat pengembangan perangkat aplikasi akuisisi forensik digital.
b. Membuat aplikasi berbasis GUI untuk mengoperasikan aplikasi akuisisi forensik digital.
c. Mengetahui kecepatan transfer data akuisisi dari perangkat sebelumnya.

Dalam membantu dalam proses pengembangan aplikasi akuisisi forensik digital, ada beberapa strategi penelitian untuk menunjang pengembangan yaitu:

a. Studi literatur

   Pada tahap studi literatur peneliti mencari berbagai literatur dari berbagai sumber baik itu *online* atau *offline*. Pada saat mendapatkan literature peneliti disini mencari secara *online* melalui internet dengan menggunakan mesin pencarian *sciencedirect.com* yang didalamnya terdapat banyak jurnal, karya ilmiah, dan buku. Sedangkan mencari secara *offline* dengan membaca buku-buku dan tugas akhir sebelumnya. Peneliti mengumpulkan dan mempelajari literatur yang sesuai untuk dijadikan referensi.

b. Perancangan aplikasi

   Pada tahap perancangan aplikasi ini, peneliti melakukan analisis kebutuhan sistem untuk merancang sistem yang akan dibuat. Selain analisis kebutuhan sistem, peneliti juga melakukan analisis kebutuhan perangkat keras, analisis kebutuhan perangkat lunak, analisis kebutuhan masukan, analisis kebutuhan proses, dan analisis kebutuhan akhir. Perancangan aplikasi ini dilakukan sebelum peneliti melakukan tahap pembuatan aplikasi. Analisis mengacu pada studi literatur, selanjutnya akan melakukan perancangan yang akan dibuat terlebih dahulu dalam bentuk *flowchart* dan tampilan antarmuka aplikasi. Dalam pembuatan tampilan antarmuka aplikasi peneliti menggunakan perangkat lunak yaitu QT Desaigner.

c. Pembuatan aplikasi

   Pada tahap pembuatan aplikasi, peneliti membuat aplikasi yang mengacu pada *flowchart* sebagai alur aplikasi berjalan dan tampilan antarmuka aplikasi yang telah dibuat pada tahap perancangan aplikasi. Peneliti menggunakan Pycharm sebagai *text editor* yang digunakan sebagai tempat peneliti menuangkan semua kode program supaya aplikasi dapat berjalan. Semua ide peneliti dituangkan pada tahap ini untuk menghasilkan aplikasi sesuai dengan kebutuhan.

d. Pengujian aplikasi

Pada tahap pengujian ntuk melihat dan menilai apakah aplikasi yang dibuat peneliti sudah berjalan dengan baik dan sesuai, maka perlu dilakukan pengujian untuk menguji aplikasi. Dalam pengujian aplikasi akuisisi dengan ekstensi .dd menggunakan tujuh buah *flashdrive* dengan berbagai merek dan ukurun. Maka akan dilakukan pengujian aplikasi dengan menggunakan beberapa cara untuk menguji aplikasi dari mulai fungsi-fungsi dan tombol.

1.6 Sistematika penulisan

Sistematika penulisan penelitian ini disusun untuk mempermudah dalam memahami tentang penelitian yang dilakukan. Secara garis besar, sistematika penulisan sebagai berikut:

BAB I PENDAHULUAN

Pada bab ini berisikan latar belakang, rumusan masalah, batasan masalah yang akan dibahas, menjelaskan tujuan penelitian, dan strategi penyelesaian dalam menyelesaikan masalah.

BAB II LANDASAN TEORI

Pada bab ini berisikan penelitian-penelitihan terdahulu yang digunakan sebagai landasan teori, dan isikan tentang forensik digital, file hasil ekstensi, dan python.

BAB III METODOLOGI PENELITIAN

Pada bab ini berisikan tentang metodologi penelitian yang dimana merupakan sebuah proses cara mengumpulkan data, analisisi untuk pembuatan aplikasi, dan juga merancang aplikasi sehingga dapat memberikan gambaran untuk membuat sistem.

BAB IV HASIL DAN PEMBAHASAN

Pada bab ini berisikan hasil-hasil yang sudah dikerjakan dan implementasi dari rancangan gambaran sebelumnya. Implementasi ini terdapat tampilan antar muka aplikasi akuisisi forensik digital dan pengujian aplikasi.

BAB V KESIMPULAN DAN SARAN

Pada bab ini berisikan kesimpulan dari apa yang telah dicapai dari hasil dan saran untuk pengembangan selanjutnya.

BAB II
LANDASAN TEORI

21 Penelitian Terdahulu

Dalam tugas akhir yang berjudul" *FORENSIC IMAGING APPLICATION USING RASPBERRY PI*" melakukan penelitian dengan membuat alat *forensic imaging*, bersifat *portable* yang artinya mudah dibawa karena memanfaatkan *single board computer* yaitu Raspberry Pi 3. Pada perangkat forensik dilakukan akuisisi media penyimpanan dan menghasilkan *file image* dengan format .dd dengan 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 (K, 2018). Berikut beberapa penelitian terdahulu lainnya dapat dilihat pada tabel 2.1 Penelitian Terdahulu:

Tabel 2. 1 Penelitian Terdahulu

No	Judul	Penulis	Ringkasan (Masalah dan Hasil)	Metode	Saran
1	Low Budget Forensic Drive Imaging Using Arm Based Single Board Computer (2016)	• Eric Olson	Ketika ingin melakukan analisa forensik terhadap harddisk ataupun media penyimpanan lain biasanya dalam keadaan mati. Ketika melakukan analisa tersebut dibutuhkan duplikator forensik tersendiri, perangkat keras writeblocker yang tertanam di laptop dan sistem operasi untuk forensik yang di boot	Software write-blocking methods	• Diwindows belum tersedia untuk layanan ini.

			dari USB ataupun virtual machines. Karena alat–alat untuk melakukan analisa forensik mahal, maka disini peneliti membuat alat yang mampu melakukan kegiatan forensik dengan harga yang murah.		
2	Analyse digital forensic evidences through a semantic-based methodology and NLP techniques(2019)	• Flora Amato • Giovanni Cozzolino • Vincenzo Moscato • Francesco Moscato	Meningkatnya teknologi digital untuk mengelola dan memproses informasi yang digunakan dalam kehidupan sehari-hari, menghasilkan peningkatan permintaan data digital untuk keperluan investigasi. Faktanya, rekonstruksi kejahatan komputer dan telematik, atau, secara umum, kejahatan yang dilakukan dengan sistem komputer, memerlukan	Method of data processing for procedural	• Mengusulkan sistem untuk bukti forensik yang bertujuan untuk memberikan peningkatan pengambilan bukti.

			penerapan praktik terbaik Forensik Komputer untuk mengekstraksi bukti yang relevan dari perangkat elektronik, menjamin integritas data dan keberterimaannya selama sebuah persidangan. Proses ekstraksi, konservasi, analisis, dan dokumentasi investigasi forensik dapat ditingkatkan dengan kerangka kerja yang mendukung penyelidik selama pekerjaan mereka, menghubungkan bukti yang dikumpulkan oleh berbagai alat forensik.		
3	Faster File Imaging Framework for Digital	• Neha Kishore	Penggunaan alat digital forensik telah menjadi hal umum dalam kejahatan komputasi dan komunikasi. Fungsi oyptogphichash(CHr	Parallel algorithm in the image creation process	• Adanya eksperimen dengan kode pada file yang lebih besar, biasanya

	Forensics (2015)		s) diberikan alat forensic untuk barang bukti digital selama akuisisi. Komunikasi CFH pararel mempercepat proses pembuatan gambar dan membandingkan hasilnya dengan metode sekuensial yang ada		harddisk dengan ukuran terabyte.
4	Extending the advanced forensic format to accommodate multiple data sources, logical evidence, arbitrary information and forensic workflow (2009).	• Michael Cohen	Analisis forensik memerlukan perolehan dan pengelolaan berbagai jenis bukti, termasuk disk drive individual, set RAID, paket jaringan, gambar memori, dan file yang diekstraksi. Seringkali bukti yang sama ditinjau oleh beberapa alat atau penguji yang berbeda di lokasi yang berbeda. Format file yang dapat diperluas untuk menyimpan dan berbagi bukti, informasi terkait kasus arbitrer dan	compression	• Adanya fitur-fitur baru seperti kemampuan untuk menyimpan berbagai jenis bukti dari beberapa perangkat dalam satu arsip, dan pemisahan yang ditingkatkan antara mekanisme penyimpanan perangkat lunak forensik

			hasil analisis di antara berbagai alat. Spesifikasi baru, disebut AFF4, dirancang agar mudah diimplementasikan, dibangun di atas spesifikasi format file ZIP yang didukung dengan baik. Lebih lanjut, implementasi AFF4 memiliki komparabilitas ke bawah dengan file AFF yang ada		
5	Wirespeed: Extending the AFF4 forensic container format for scalable acquisition and live analysis(2015)	• Bradley Schatz	Mengidentifikasi keterbatasan dalam format gambar forensik yang digunakan membatasi kemampuan untuk memperoleh bukti. Ekstensi ke format AFF4 diusulkan untuk mengatasi keterbatasan. Sebagian diambil pada tingkat bit akuisisi.	Aff4:compression Method	• Ekstensi format lain.

6	Hash based disk imaging using AFF4(2010)	• Michael Cohen	Seiring pertumbuhan kapasitas disk yang terus melampaui bandwidth IO penyimpanan, permintaan yang ditempatkan pada penyimpanan dan waktu semakin meningkat. Pengurangan data dan teknologi deduplikasi sekarang biasa di ruang Enterprise, dan berpotensi berlaku untuk akuisisi forensik. Menggunakan format file forensik AFF4 yang baru, kami menggunakan skema kompresi berbasis hash untuk memanfaatkan kumpulan gambar yang ada, mengurangi waktu akuisisi dan persyaratan penyimpanan. Makalah ini juga menjelaskan	AFFLIB Compression level 1	• Kemungkinan perbaikan dapat dilakukan pada algoritma segmentasi, meningkatkan kemungkinan de-duplikasi pada gambar. Optimalisasi lainnya termasuk menyeimbangkan kompresi dengan kecepatan untuk mengkompres hanya byte byte yang dapat dikompres, dan mengadaptasi algoritma segmentasi kami dengan tipe gambar

			beberapa evolusi terbaru dalam format file AFF4 menjadikan implementasi pencitraan berbasis hash yang efisien menjadi kenyataan.		tertentu yang diperoleh.
7	The Forensic Image Generator Generator (Forensig)(2009)	• Christian Moch • Felix C. Freiling	Penelitian ini menghasilkan alat digital forensic untuk edukasi. Peneliti mendesain dan membuat alat digital forensic yang dapat digunakan oleh instruktur untuk membuat file system image untuk edukasi analisis forensik	identify the script in document fragments	• Banyak aspek yang masih bisa dikembangkan di Forensig. Alat yang dibuat masih sulit di gunakan oleh instruktur yang tidak memiliki pemahaman dasar tentang pemrograman. Kemudian kedepannya Forensig dikembangakan dengan dibuatkan GUI nya.
8	MyPyTutor: an	• Peter J. Robinson	MyPyTutor adalah sebuah sistem	compiler	• Masih ditemukan

	Interactive Tutorial System For Python(2011)		tutorial interaktif yang diperuntukan bagi orang yang ingin mempelajari Bahasa pemrograman python. Di dalamnya terdapat banyak materi python mulai dari yang dasar hingga membuat GUI dengan Tkinter.		bug, maka pihak developer dalam hal ini peniliti masih terus menyempurnakan.
9	Forensic Imaging Aplication Using Raspberry Pi(2018)	• Razan Maulida K	Sebuah aplikasi forensic imaging yang mudah dibawa dengan memanfaatkan Raspberry Pi 3. Pengoperasian perangkat forensic imaging berbasis GUI dengan Bahasa pemrograman Python. Bahasa pemrograman Python adalah Bahasa pemrograman yang mudah untuk dipelajari.	RAW	• Mampu menghasilkan file format yang lain tidak hanya format .dd. • Mampu meningkatkan kecepatan transfer datanya sehingga proses akuisisi yang berjalan dapat lebih cepat.

Dari literatur yang sudah dibaca peneliti akan menggunakan dalam proses pengembangan aplikasi akuisisi. Nantinya aplikasi akuisisi forensik digital ini akan mengembangkan untuk mengetahui kecepatan transfer data dari aplikasi terbaru. Aplikasi akuisisi forensik digital akan dikembangankan berbasis GUI supaya tampilan menarik sehingga pengguna akan lebih mudah dalam menggunakannya. Dalam mengembangkan aplikasi akuisisi peneliti menggunakan Bahasa pemrograman python dan menggunakan sistem operasi linux debian.

22 Cybercrime

Cybercrime adalah setiap aktivitas seseorang, sekelompok orang, badan hukum yang menggunakan komputer sebagai sarana melakukan kejahatan, atau menjadikan komputer sebagai sasaran kejahatan. Semua kejahatan tersebut adalah bentuk-bentuk perbuatan yang bertentangan dengan peraturan perundang-undangan, baik dalam arti melawan hukum secara material maupun melawan hukum secara formal (Widodo, 2011:7). Sedangkan menurut Organization of European Community Development (OECD), *cybercrime* atau kejahatan komputer adalah segala akses illegal atau akses secara tidak sah terhadap suatu transmisi data sehingga terlihat bahwa segala aktivitas yang tidak sah dalam suatu sistem komputer merupakan suatu kejahatan (Karnasudiraja, 1993:3).

23 Forensik Digital

Forensik berdasarkan Kamus Besar Bahasa Indonesia (KBBI) adalah cabang ilmu kedokteran yang berhubungan dengan penerapan fakta medis pada masalah hukum dan ilmu bedah yang berkaitan dengan penentuan identitas mayat seseorang yang ada kaitannya dengan kehakiman dan peradilan. Sedangkan digital berdasarkan Kamus Besar Bahasa Indonesia (KBBI) adalah berhubungan dengan angka-angka untuk sistem perhitungan dengan angka-angka untuk sistem perhitungan tertentu yang berhubungan dengan penomoran. Forensik digital adalah cabang ilmu forensik yang biasanya digunakan untuk penemuan dan penyelidikan isi atau konten dari perangkat digital, dan ada kaitannya dengan kejahatan komputer (Selamat datang di KBBI Daring!, 2020). *Forensic imaging* adalah 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 (Rouse, 2017).

Dasar dari forensik digital adalah praktik pengumpulan, menganalisa dan melaporkan data digital. Investigasi forensik digital sangat beragam untuk diterapkan. Penggunaan paling sering adalah sebagai pendukung atau penyanggah akuisisi tentang kriminalitas dalam pengadilan perdata atau pidana. Pada sektor swasta forensik juga dilakukan untuk penyelidikan diinternal perusahaan atau untuk menyelidiki kasus eksploitasi dan jaringan yang tidak benar atau sah. Proses forensik biasanya meliputi *forensic imaging* (akuisisi), penyitaan, dan analisis media digital digunakan untuk menyusun laporan untuk dikumpulkan berdasarkan bukti yang ada (Raharjo, 2013).

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, *laptop/notebook*, dan tablet. Pemeriksaan terhadap jenis barang bukti ini biasanya berkaitan dengan *file recovery*, yaitu suatu metode 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 (Al-Azhar, 2012).

2*4* File Ekstensi Hasil Akuisisi

Pengamanan barang bukti yang biasanya tertinggal dikomputer, untuk barang bukti yang asli tidak mengalami perubahan bit data untuk tetap terjaga keasliannya maka dapat dilakukan akuisisi media penyimpanan pada komputer. Pada saat dilakukannya proses akuisisi media penyimpanan bisa menggunakan banyak *file* format ekstensi, banyak file ekstensi yang dapat digunakan dalam akuisisi antara lain: dd, e01, dan aff.

File format ekstensi dd merupakan format tertua dikarenakan lahir sebelum e01 dan aff. *File* format dd ini masuk kedalam tipe RAW yang cara bekerjanya menyalin seluruh data media penyimpanan yang menyalin setiap sektor pada media penyimpanan sehingga tidak ada sektor yang terlewatkan pada proses akuisisi. Hasil dari akuisisi format dd ini menyalin data asli dari media penyimpanan asalnya (Garfinkel, Malan, Stevens, & Pham, 2006).

Sedangkan *file* format e01 merupakan format ekstensi yang masuk ke dalam *file* dengan tipe EXPERT WITNESS Format(EWF). Cara kerja dari e01 ini hampir menyerupai dd, e01 bekerja dengan menyalin bit demi bit dalam akuisisi dari sumber media penyimpanan tanpa ada bit demi bit yang terlewat. E01 memiliki perbedaan dengan dd yaitu: memiliki *header* pada file yang isinya waktu dan tanggal akuisisi, nama penguji dan catatan *file* akuisisi yang berisikan informasi tentang *hashing* MD5 (Garfinkel, Malan, Stevens, & Pham, 2006).

Sedangkan *file* format ekstensi aff (Advanced Forensic Format) merupakan format ekstensi yang memberikan kepada investigator forensik alternatif dalam memilih format ekstensi *file* hasil akuisisi. Ada keuntungan yang didapatkan ketika memilih *file* format hasil ekstensi aff yaitu: ekstensi aff dapat menyimpan metadata lebih besar sehingga lebih fleksibel dan ekstensi aff dibandingkan dengan *file* ekstensi yang lain memiliki ukuran *file* yang lebih kecil karena pengkompresan pada *file* ekstensi aff sehingga ukurannya menjadi lebih kecil dari *file* ekstensi yang lain karena tidak ada yang dikompres (Garfinkel, Malan, Stevens, & Pham, 2006).

25 Python

Guido Van Rossum pada tahun 1990 di Strichting Marhematisch Centrum (CWI) mengembangkan python sebagai kelanjutan dari bahasa pemrograman ABC. Python terus berkembang yang dilakukan oleh pengembang dari python 1.2 sampai ke python 3.8.

Python merupakan bahasa pemrograman yang berfokus pada keterbacaan suatu kode dan dilengkapi dengan fungsionalitas pustaka standar yang besar serta adanya komunitas yang besar. Python juga digunakan diberbagai platform sistem operasi untuk mengembangkan perangkat lunak dan secara bebas dapat menggunakan bahasa pemrograman python (Rossum). Pada tabel 2.2 aplikasi akuisisi forensik digital menggunakan beberapa *library* yaitu: PyQT5 adalah *library* yang digunakan untuk tampilan GUI aplikasi, *sys* adalah *library* yang digunakan untuk mengakses konfirmasi interpreter pada *runtime*, *hashlib* adalah *library* yang digunakan untuk menjalankan fungsi *hashing*, baik MD5 atau SHA512, *subprocess* adalah *library* yang digunakan untuk mengakses terminal untuk menjalankan komen tertentu di terminal, *logging* adalah *library* yang digunakan untuk membuat *file logging* sehingga *log-log* selama proses akuisisi berjalan dapat disimpan, *time* adalah *library* yang digunakan untuk menyediakan fungsi waktu dan tanggal, dan *os* adalah *library* yang digunakan untuk mengakses terminal serta menjalankan komen tertentu di terminal.

Tabel 2. 2 *Tabel Library*

No	Nama *Library*	Fungsi
1	PyQt5	PyQt5 merupakan *library* yang digunakan sebagai tampilan GUI aplikasi akuisisi forensik digital.
2	sys	sys digunakan untuk mengakses konfigurasi interpreter pada saat runtime dan berinteraksi dengan environment system operasi.

3	os	os merupakan modul yang peneliti gunakan supaya dapat mengakses terminal, untuk menjalankan komen tertentu di terminal.
4	hashlib	Library yang berfungsi untuk menjalankan fungsi hashing, baik MD5 dan SHA512.
5	subprocess	Modul subprocess peneliti gunakan agar dapat mengakses terminal, untuk menjalankan komen tertentu di terminal.
6	time	Library time berfungsi untuk menyediakan fungsi waktu.
7	datetime	Library datetime berfungsi untuk menyediakan fungsi waktu dan tanggal.
8	logging	Berfungsi untuk membuat file logging. Sehingga log-log selama proses aplikasi berjalan dapat disimpan didalam sebuah file yang disebut file logging.

BAB III
METODOLOGI PENELITIAN

3.1 Metodologi Penelitian

Dalam menyelesaikan masalah yang ada peneliti menggunakan metode atau untuk memecahkan suatu masalah guna membantu peneliti menyelesaikan masalah. Pada proses pengumpulan data ini menjadi suatu proses yang penting dalam proses penelitian, karena data yang terkumpul akan menjadi bahan untuk memperkuat argumen dalam penelitiannya. Dalam mengembangkan aplikasi akuisisi forensik digital peneliti akan menggunakan studi literatur atau studi pustaka sebagai untuk memperoleh data-datanya.

Studi pustaka adalah mempelajari berbagai buku referensi serta hasil penelitian sebelumnya yang sejenis yang berguna untuk mendapatkan landasan teori mengenai masalah yang ditelitinya (Sarwono, 2006). Metode studi literatur dapat memperoleh data untuk mengembangkan aplikasi akuisisi forensik digital dengan cara mencari artikel ilmiah, membaca buku, dan membaca tugas akhir terkait diinternet ataupun mencari keorang terkait. Dalam proses pengembangan akuisisi forensik digital ada kata kunci, yaitu: akuisisi forensic, *phyton,* RAW, E01, dan AFF2. Dalam mengembangkan aplikasi akuisisi forensik digital peneliti mempelajari penelitian yang sudah ada sebelumnya untuk mengetahaui langkah-langkah dan gambaran dalam mengembangkan aplikasi peneliti.

Ada data-data yang diperlukan untuk mengembangkan aplikasi akuisisi forensik digital yaitu proses kerja dari akuisisi forensik digital, Bahasa pemrograman *phyton*, tampilan GUI dalam Bahasa pemrograman *phyton*, pengembangan dalam file formatnya, proses *hashing*, dan bagaimana cara mendapatkan proses akuisisi dengan kecepatan transfer data yang cepat. Setelah mengetahui gambaran, langkah-langkah, dan semua data terkumpul peneliti lalu mengolah semua aspek tersebut untuk menggembangkan aplikasi dengan metode yang sesuai, kemudian diterapkan dalam proses pengembangan aplikasi akuisisi forensik digital nantinya. Gambar 3.1 merupakan diagram alir dalam proses perencanaan aplikasi hingga aplikasi selesai dalam pembuatannya.

Gambar 3. 1 Diagram Alir Perencanaan Akuisisi Forensik Digital Menggunakan Sistem Operasi Linux Debian

3.2 Analisis Kebutuhan Perangkat Keras

Dalam pengembangan aplikasi akuisisi forensik digital peneliti membutuhkan beberapa perangkat keras untuk proses pembuatan aplikasi forensik digital diantaranya adalah:

3.2.1 Laptop

Dalam mengembangkan aplikasi akuisisi forensik digital peneliti menggunakan laptop sebagai perangkat keras dalam proses pengembangan aplikasi dan untuk menjalankan virtual box yang didalamnya terdapat sistem operasi debian. Pada saat pengujian aplikasi laptop yang digunakan memiliki kapasitas RAM 8GB.

3.2.2 Flash drive dan Hard disk

Pada saat pengujian aplikasi diperlukan *flash drive* sebagai media yang akan diakuisisi, *flash drive* yang digunakan sebayak tujuh buah diantaranya adalah 1.9 GB Kingston, 3.8 GB VGen, 7.2 GB Toshiba, 14.5 GBToshiba, 14.7 GB Generic Custem "Astra Honda", 14.3 GB Sandisk, dan 28.7 GB Sandisk.

Harddisk digunakan sebagai tempat penyimpanan hasil akuisisi dengan ukuruan 1TB, menggunakan *harddisk* sebagai tempat penyimpanan hasil akuisisi karena membutuhkan media penyimpanan yang cukup besar untuk menyimpan semua hasil akuisisi.

3.3 Analisis Kebutuhan Perangkat Lunak

Dalam pengembangan aplikasi akuisisi forensik digital peneliti membutuhkan beberapa perangkat lunak atau biasa disebut *software* yang digunakan untuk proses pengembangan aplikasi akuisisi forensik digital. Dibawah ini ada beberapa perangkat lunak yang digunakan dalam proses pengembangan aplikasi akuisisi forensik digital, yaitu:

3.3.1 JetBrains PyCharm Community Edition 2019.2.3 x64

Dalam pengembangan aplikasi akuisisi forensik digital *text editor* yang digunakan adalah JetBrains PyCharm Community Edition 2019.2.3 x64. JetBrains PyCharm Community Edition 2019.2.3 x64 merupakan sebagai wadah untuk menuliskan kode-kode program yang digunakan untuk pengembangan aplikasi akuisisi forensik digital supaya aplikasi ini dapat selesai. Gambar 3.2 adalah perangkat lunak yang digunakan peneliti sebagai *text editor* untuk menuangkan kode-kode program:

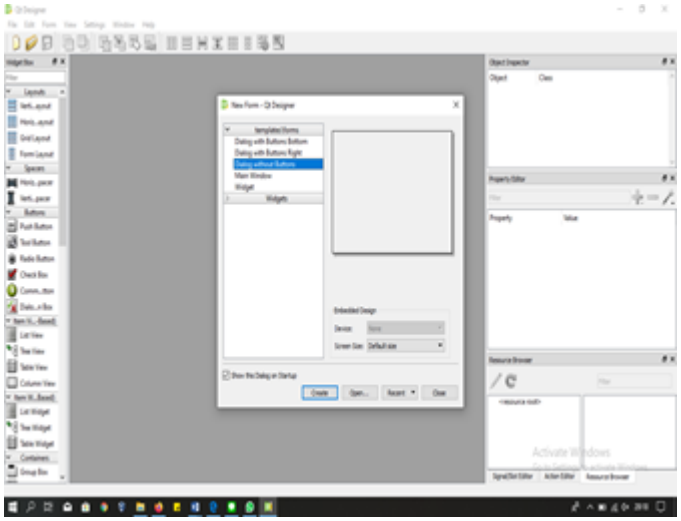
Gambar 3. 2 PyCharm

3.3.2 Python

Pyhton adalah bahasa pemrograman interpretatif multiguna dengan filosofi perancangan yang berfokus pada tingkat keterbacaan kode. Python diklaim sebagai bahasa yang menggabungkan kapabilitas, kemampuan, dengan sintaksis kode yang sangat jelas, dan dilengkapi dengan fungsionalitas pustaka standar yang besar serta komprehensif. Python juga didukung oleh komunitas yang besar. Dalam pengembangan aplikasi akuisisi forensik digital menggunakan versi *Python 3.7.3.* Bahasa pemrograman *Python* ini bisa berjalan banyak atau lintas *platform* sehingga bahasa pemrograman ini banyak orang yang menggunakannya.

3.3.3 Qt Designer

Dalam pengembangan aplikasi akuisisi forensik digital untuk membuat tampilan antarmuka menggunakan perangkat lunak atau *software* Qt Designer. Qt Designer ini merupakan perangkat lunak untuk membuat tampilan antarmuka aplikasi akuisisi forensik digital yang berbasis *Graphical User Interface*(GUI), seperti yang terlihat pada gambar 3.3.



Gambar 3. 3 Qt Designer

3.3.4 Sistem Operasi

Sistem operasi merupakan jembatan untuk berkomunikasi antara pengguna perangkat komputer dengan perangkat komputer itu sendiri, sehingga setiap input dari pengguna dapat dimengerti dengan baik oleh sebuah perangkat komputer. Disebuah perangkat komputer untuk dapat berjalan dengan baik dan benar maka didalam perangkat komputer harus ada sumber daya yang itu disebut sistem operasi.

Gambar 3. 4 Sistem Opersi

Sumber: https://erlanggablc.blogspot.com/2017/03/sejarah-dan-pengertian-linux-debian.html

Sistem operasi pada gambar 3.4 merupakan system operasi yang peneliti gunakan dalam mengembangkan aplikasi akuisisi adalah sistem operasi debian. Debian adalah sistem operasi GNU/Linux yang sering digunakan untuk kebutuhan yang dikembangankan sejak 1993. Selain sebagai sistem operasi, debian memberikan banyak *software* dalam repostorinya.

3.4 Analisis Kebutuhan Masukan

Analisis kebutuhan masukan merupakan analisisi kebutuhan yang digunakan peneliti untuk mengetahui apa saja yang dibutuhkan aplikasi akuisisi sebelum proses akuisisi dijalankan. Serta memilih data apa yang sesui untuk data masukan yang dibutuhkan oleh aplikasi akuisisi sehingga dapat berjalan sesuai yang diharapkan.

Ada beberapa data masukan yang dibutuhkan saat pertama kali sebelum proses akuisisi yaitu pemilihan perangkat media penyimpanan yang ada diaplikasi akuisisi untuk dilakukannya proses akuisisi, kemudian memilih perangkat media penyimpanan yang akan dilakukan proses akuisisi. Selanjutnya mengisi beberapa data dalam kolom yang ada diaplikasi akuisisi seperti: *image directory, filename, notes, examiner,* dan *image type* sebelum melakukan proses akuisisi.

3.5 Analisis Kebutuhan Proses

Analisis kebutuhan proses dilakukan untuk mengetahui tahapan-tahapan yang sesuai untuk melakukan akuisisi terhadap media penyimpanan. Kebutuhan untuk proses akuisisi untuk yang pertama, melakukan *scanning* menditeksi perangkat media penyimpanan yang ada, selanjutnya menampilkan perangkat yang terditeksi dalam bentuk table untuk dipilih dan dilakukannya proses akuisisi. Kemudian mengisi data pada kolom yang sudah tersedia. Kemudian, proses akuisisi yaitu menyalin data dari media penyimpanan dengan mengambil data bit demi bit data asli dari media penyimpanan.

3.6 Analisis Kebutuhan Keluaran

Analisis kebutuhan keluaran dilakukan untuk mengetahui keluaran apa yang akan dihasilkan dari aplikasi akuisisi setelah semua proses lain sudah terlaksana. Keluaran yang dihasilkan dari aplikasi akuisisi yaitu:

a. File format .dd

   Format ekstensi .dd yang masuk dalam tipe *file* RAW ini dihasilkan setelah proses akuisisi media penyimpanan. *File* ini paling sering digunakan dalam proses akuisisi.

b. File logging

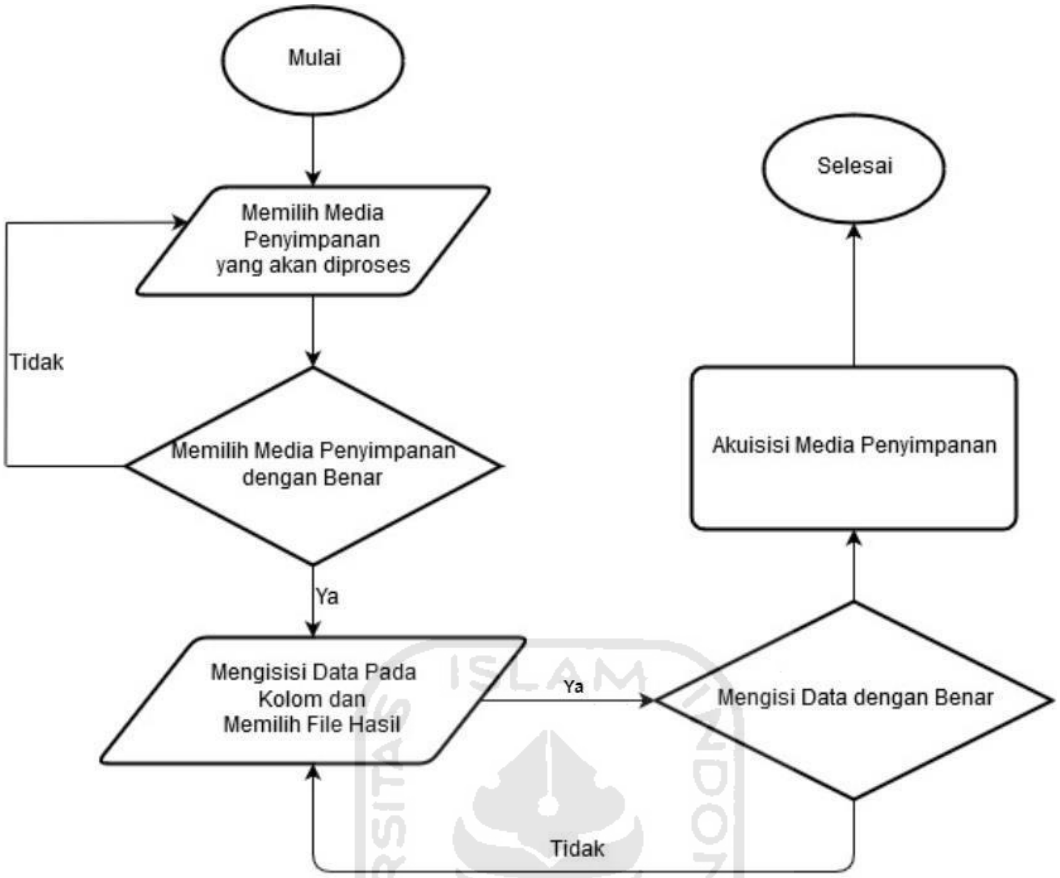
Hasil keluaran dari proses akuisisi selain .dd di aplikasi akuisisi forensik digital yaitu *file logging*, yang berisikan data-data informasi mengenali media penyimpanan yang diakuisisi oleh aplikasi akuisisi forensik digital.

3.7 Perancangan Aplikasi

Perancangan menurut KBBI adalah proses, cara, perbuatan merancang. Maka perancangan aplikasi merupakan proses dimana membuat konsep dan merencanakan proses sistem untuk memenuhi kebutuhan aplikasi akuisisi sehingga dapat berjalan sesuai yang diinginkan. Ada beberapa rancangan aplikasi yang digunakan yaitu:

3.7.1 Flowchart Penggunaan Aplikasi

Diagram alir atau yang biasa disebut *flowchart* merupakan langkah-langkah untuk memberikan gambaran tentang alur kerja sebuah sistem atau aplikasi dan bisa menjadi pedoman dalam mengerjakan aplikasi, yang dalam hal ini adalah aplikasi akuisisi forensik digital, gambar 3.5 merupakan *flowchart* pada aplikasi.



Gambar 3. 5 Flowchart Penggunaan Aplikasi Akuisisi Forensik Digital Menggunakan Sistem Operasi Linux Debian

Pada saat pertama kali dijalankan aplikasi akuisisi maka akan muncul tabel yang menampilkan media penyimpanan apa saja yang terhubung diperangkat. Pengguna memilih media penyimpanan mana yang ingin dilakukan akuisisi dan mengeklik nomornya, kemudian klik tombol *next.* Apabila ingin merubah pilihan media penyimpanan yang ingin di akuisisi, maka pilih kembali nomor media penyimpanan yang ingin diakuisisi, kemudian klik tombol *next*.

Kemudian mengisi kolom-kolom yang tersedia untuk mengisi data yang diperlukan sebelum melakukan akuisisi media penyimpanan. Kolom-kolom yang tersedia untuk diisi yaitu: image directory, *filename, notes, examiner,* dan *image type.* Isi semua kolom tersebut dengan benar jangan sampai dikosongkan supaya proses akuisisi dapat berjalan. Setelah itu klik *start* untuk memulai proses akuisisi berjalan dengan ditandai dengan progres pada *progress bar* yang berjalan.

Setalah selesai menyalin semua bit demi bit pada proses akuisisi, maka akan muncul hasil proses akuisisi pada folder yang ditentukan dikolom. Hasil berada folder yang sudah ditentukan sesuai dengan *file* ekstensi yang dipilih sebelum proses akuisisi. Dapat dilihat pada Gambar 3.6 merupakan algoritma yang digunakan peneliti dalam mengembangkan aplikasi akuisisi forensik digital.

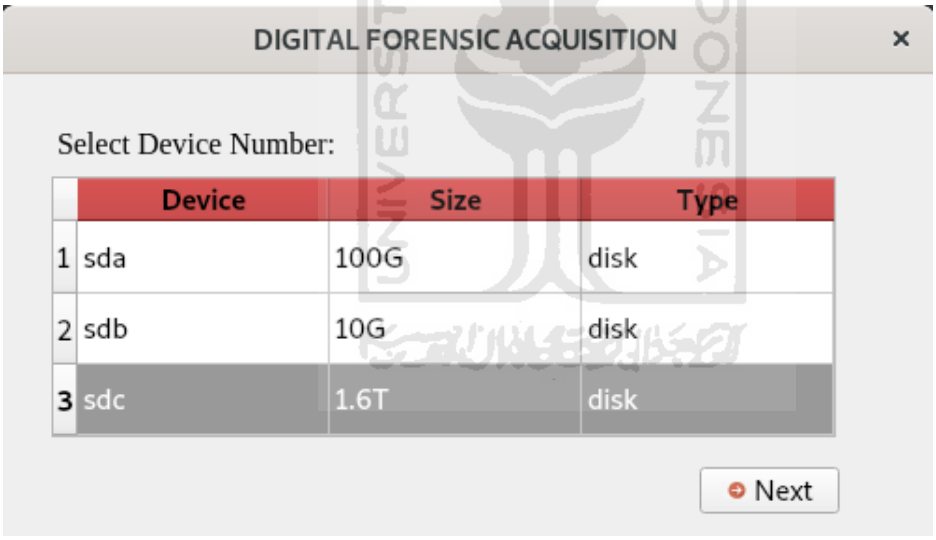
```
Deskripsi Algoritma :

if (os.path.exist) then
    output("file exist")
elif (direktori="" or filename="" or note="" or examiner="" or radioDD="")
then
    output("complete the field")
else
    usbInfo1 ← subprocess.getoutput("blkid -s LABEL")
    usbInfo2 ← subprocess.getoutput("blkid -s UUID")
    usbInfo3 ← subprocess.getoutput("fdisk -l")

open(source, read)
    open(direktori, write)
        while true
            if write = 0
            output("imaging finished")
            break

open(source)
    while true
        read(blockSize)
        if not read
            break
    md5.update
    sha512.update

open(direkori)
    while true
        read(blockSize)
```

Gambar 3.6 Algoritma Akuisisi

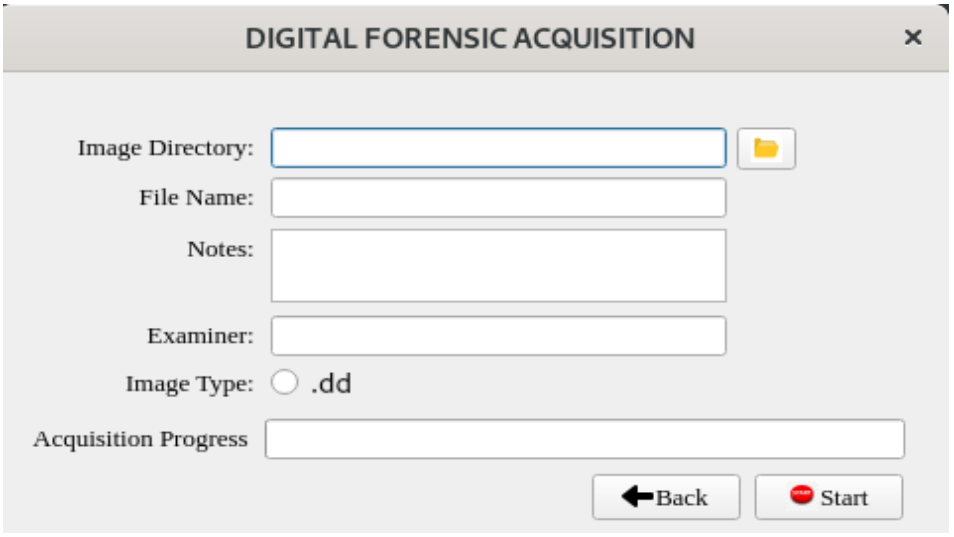
3.7.2 Desain Antarmuka

Desain antarmuka adalah proses merencanakan desain, dan pengimplementasikan dari desain ke sebuah tampilan aplikasi. Dalam menggembangkan aplikasi akuisisi forensik digital peneliti membuat tampilan antarmuka yang sederhana namun mudah dipahami oleh pengguna sehingga pengguna dalam berinteraksi atau menggunakan aplikasi tidak kesulitan dalam mengoperasikan aplikasi. Tampilan antarmuka aplikasi ini sangat penting dalam pembuatan aplikasi karena sebagai wajah dan jembatan pengguna dalam menggunakan aplikasi dapat menggunakannya dengan baik.

Dalam proses pembuatan tampilan antarmuka aplikasi akuisisi forensik digital peneliti menggunakan QT Designer sebagai perangkat lunak yang membantu peneliti membuat tampilan antarmuka aplikasi. Peneliti mengembangkan aplikasi akuisisi berbasis GUI sehingga QT Designer ini tepat untuk membantu proses pembuatan tampilan antarmuka sebuah aplikasi seperti pada Gambar 3.7 dan Gambar 3.8.



Gambar 3. 7 Tampilan Halaman 1 Aplikasi Akuisisi Forensik Digital Menggunakan Sistem Operasi Linux Debian



Gambar 3. 8 Tampilan Halaman 2 Aplikasi Akuisisi Forensik Digital Menggunakan Sistem Operasi Linux Debian

3.8 Pengujian Aplikasi

Pada pengujian aplikasi akuisisi menggunakan proses pengujian *blackbox* dan pengujian performa aplikasi. *Blackbox* adalah pengujian berdasarkan spesifikasi persyaratan dan tidak perlu dilakukan pemeriksaan kode dalam pengujian *blackbox*. Pengujian *blackbox* hanya pengujian pada input dan output yang dapat diprediksi (Nidhra & Dondeti, 2012). Pada pengujian *blackbox* terdapat pengujian tombol yang menguji setiap tombol diaplikasi dan *error handling* yang menguji apabila setiap kolomnya tidak diisi dengan benar diaplikasi.

Pengujian performa aplikasi merupakan tahap yang dilakukan untuk mengetahui aplikasi akuisisi berhasil mengakuisisi media penyimpanan *flashdrive*. Pada pengujian performa aplikasi mendapatkan hasil akuisisi dari setiap *flashdrive* yang diakuisisi kemudian akan dihitung kecepatan transfer data dari *flashdrive* dalam bentuk tabel.

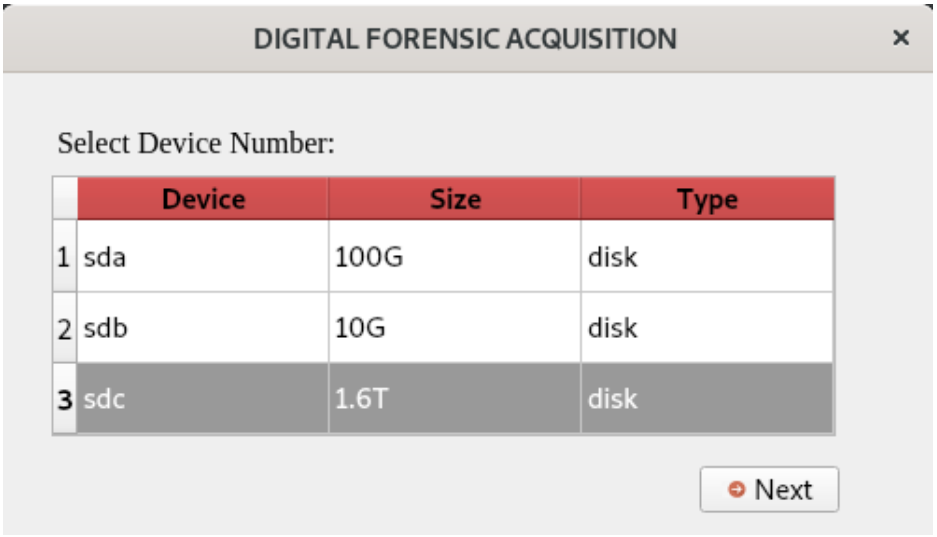
BAB IV
HASIL DAN PEMBAHASAN

4.1 Hasil

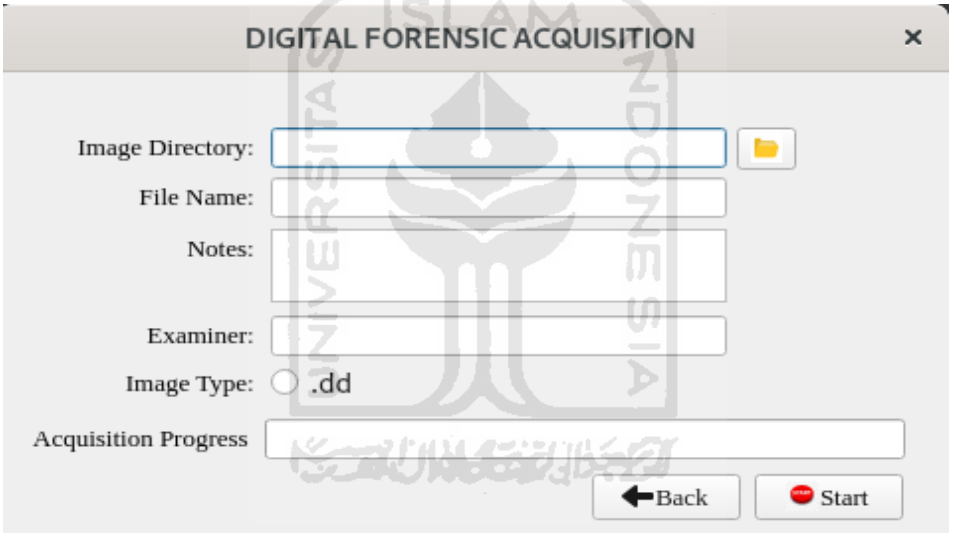
4.1.1 Perangkat Lunak

Untuk mengoperasikan aplikasi akuisisi forensik digital maka peneliti membuat aplikasi guna melakukan proses akuisisi. Aplikasi yang peneliti buat menggunakan Bahasa pemrograman *Phyton* versi 3.7.3 sesuai dengan desain yang sudah peneliti buat dengan perangkat lunak QT Designer. Aplikasi akuisisi forensik digital menggunakan sistem operasi linux debian memiliki dua tampilan antarmuka, yakni halaman pertama yang berisikan tabel penyimpanan seperti yang terlihat pada gambar 4.1 dan halaman kedua adalah halaman tempat pengguna aplikasi memasukkan data yang diperlukan.

Pada halaman utama aplikasi berisikan tabel yang memuat seluruh perangkat penyimpanan yang tersedia pada perangkat keras Raspberry Pi. Pada halaman utama ini pengguna aplikasi diminta untuk memilih media peyimpanan mana yang ingin pengguna aplikasi dapat menekan nomor pada tabel penyimpanan yang ingin diakuisisi. Setelah berhasil memilih penyimpanan yang ingin diakuisisi, maka tombol *Next* pada halaman utama akan aktif, selanjutnya pengguna dapat menekan tombol *next* tersebut untuk pindah ke halaman selanjutnya. Pada halaman kedua aplikasi berisikan kolom-kolom data yang harus diisi oleh pengguna aplikasi akuisisi forensik digital menggunakan sistem operasi linux debian. Kolom data yang harus diisi adalah *image directory*, *file name*, *note*, *examiner*, dan *image type* seperti yang terlihat pada gambar 4.2. Pada halaman kedua aplikasi ini pengguna harus mengisi semua kolom-kolom data secara lengkap dan benar, setelah melengkapi kolom data secara lengkap dan benar meka pengguna selanjutnya menekan tombol start untuk memulai proses aplikasi. Ketika proses aplikasi berjalan, maka pengguna harus menunggu hingga proses akuisisi selesai.



Gambar 4. 1 Halaman Tabel List Media Penyimpanan



Gambar 4. 2 Halaman Pengisian Data

4.2 Pembahasan Implementasi Aplikasi

4.2.1 Pembahasan Implementasi Kode Program

Bahasa pemrograman yang digunakan peneliti untuk membantu menuangkan algoritma pada aplikasi menggunakan Bahasa pemrograman *Python* versi 3.7.3 yang menjadi versi bawaan dari system operasi debian 10. Dalam mengembangkan aplikasi peneliti mengimplementasikan kode program, peneliti membuat dua buah tampilan antarmuka yang juga digunakan peneliti untuk menuangkan kode-kode untuk proses akuisisi dalam mengembangkan aplikasi akuisisi forensik digital.

Pada tampilan antarmuka pertama yang berfungsi sebagai halaman satu sebagai halaman utama untuk aplikasi akuisisi forensik digital, pada Gambar 4.3 peneliti menggunakan *library* PyQt5, sys, dan os. Modul PyQt5 peneliti menggunakan untuk kepentingan tampilan *Graphical User Interface* (GUI) aplikasi akuisisi forensik digital, *library* PyQt5 digunakan sebagai tampilan tabel hingga tombol. Sedangkan modul sys digunakan untuk mengintegrasikan antara *Python* dengan system supaya bisa saling terhubung satu sama lain. Os digunakan peneliti untuk menjalankan terminal didalam *Python* dan memberikan komen perintah "lsblk | grep disk" pada terminal seperti pada Gambar 4.4.

```
import sys
from PyQt5.QtWidgets import *
from PyQt5 import QtCore, QtGui, QtWidgets
from interface2 import *
import psutil
import subprocess
import os
```

Gambar 4. 3 *Library* Tampilan Halaman Pertama

```
diskx = [s.split() for s in os.popen("lsblk | grep disk").read().splitlines()]
        i=0
        j=0
        k=0
        for line in diskx:
            listAx = line[0]
            listBx = line[3]
            listCx = line[5]
            mystruct = {'A':listAx, 'B':listBx, 'C':listCx}
            self.datax = mystruct
            jmlhRow = len(diskx)
            self.display.setRowCount(jmlhRow)
            self.display.setColumnCount(3)
            self.display.setHorizontalHeaderLabels(["Device", "Size", "Type"])
```

Gambar 4. 4 Fungsi Menampilkan List Media Penyimpanan

Sedangkan pada halaman kedua yang mana berfungsi sebagai tampilan untuk menampilkan aplikasi akuisisi forensik digital sebagai tampilan pengisian data yang digunakan untuk proses akuisisi, peneliti pada halaman dua menggunakan beberapa modul atau *library* seperti pada Gambar 4.5 yaitu: PyQt5, sys, hashlib, subprocess, logging, time, datetime dan os. Setiap dari library memiliki fungsi masing-masing.

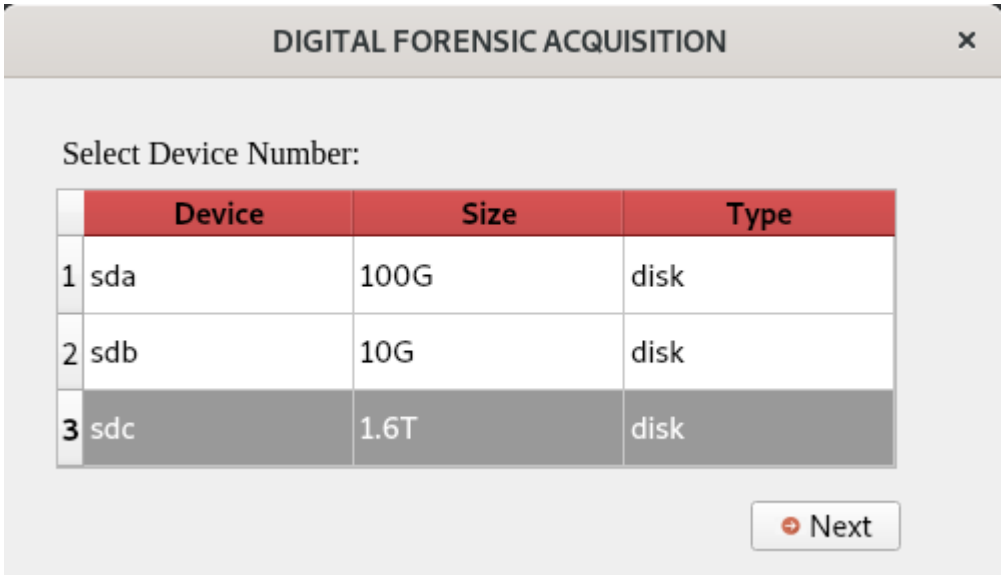
```
from PyQt5.QtWidgets import *
from PyQt5 import QtGui, QtCore
from PyQt5.QtCore import QThread, pyqtSignal
import sys
import hashlib
import subprocess
import logging
import time
import datetime
import os
```

Gambar 4. 5 *Library* Tampilan Halaman Ke Dua

4.2.2 Pembahasan Implementasi Antarmuka

Pada aplikasi akuisisi forensik digital ini terdapat dua halaman tampilan antarmuka yaitu: halaman 1 yang berisikan kode-kode untuk menampilkan daftar media penyimpanan yang dapat dipilih untuk dilakukan proses akuisisi, sedangkan halaman 2 yang berisikan kode-kode untuk menampilkan kolom-kolom berupa data masukan yang diisikan untuk data proses akuisisi.

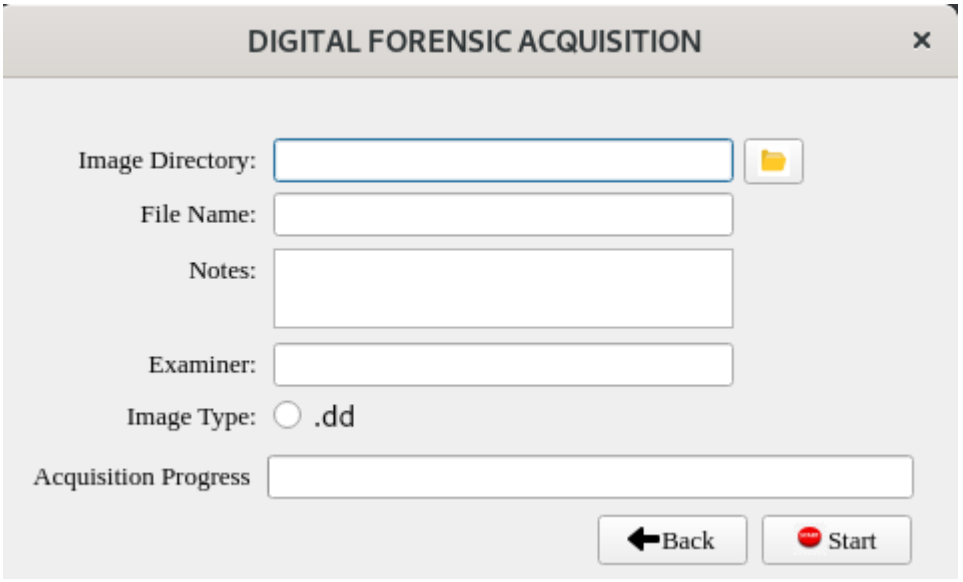
Pada halaman tampilan antarmuka 1 aplikasi akuisisi forensik digital berisi daftar madia penyimpanan yang tersambung di perangkat yang pengguna dapat memilihnya media penyimpanan mana yang akan dilakukan proses akuisisi seperti Gambar 4.6. Di tampilan halaman pertama terdapat tabel yang didalamnya menampilkan baris dan kolom. Baris berisikan nomer perangkat ke 1, 2, 3, ... (n), sedangkan kolom berisikan *Device, Size,* dan *Type*. Setiap kolom menampilkan sesuai dengan keterangannya seperti: kolom *Device* merupakan kolom yang memuat nama setiap media penyimpanan, sedangkan kolom *Size* merupakan kolom yang memuat ukuran kapasitas dari setiap media penyimpanannya, dan kolom *Type* memuat tipe dari setiap media penyimpanan.



Gambar 4. 6 Halaman 1 Aplikasi Akuisisi Forensik Digital Menggunakan Sistem Operasi Linux Debian

Pada halaman 1 aplikasi akuisisi forensik juga terdapat menu *exit* digunakan ketika pengguna aplikasi akuisisi forensik ingin keluar dari aplikasi, dengan menggunakan tanda silang yang berada di pojok kanan atas aplikasi.

Kemudian pada halaman 1 ini juga terdapat tombol dengan nama tombol *Next*, tombol tersebut bisa digunakan oleh pengguna jika ingin berpindah ke halaman selanjutnya. Tombol *next* tidak bisa ditekan oleh pengguna karena telah didesain tidak aktif sampai pengguna telah memilih media penyimpanan yang ingin diakuisisi. Pada saat memilih media penyimpanan, pengguna menekan pada bagian nomor yang terdapat tabel.

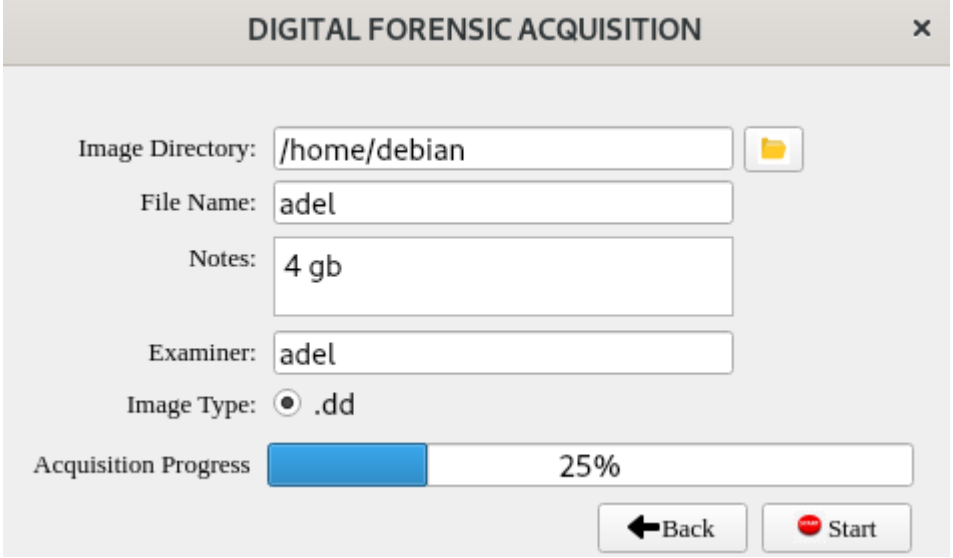


Gambar 4. 7 Halaman 2 Aplikasi Akuisisi Forensik Digital Menggunakan Sistem Operasi Linux Debian

Pada halaman 2 aplikasi akuisisi forensik terdapat kolom-kolom yang harus diisi oleh pengguna seperti pada Gambar 4.7. Kolom *image directory* berguna untuk menyimpan letak lokasi penyimpanan *file* hasil dari akuisisi. Aplikasi tersebut sudah menyiapkan tombol yang dapat digunakan untuk menentukan letak lokasi penyimpanan *file* hasil akuisisi.

Kemudian terdapat kolom *filename*, digunakan untuk penamaan *file* akuisisi. Pengguna cukup menuliskan nama *file* hasil akuisisi, kemudian mengisi kolom *filename*, dan kemudian mengisi kolom *notes*. Dimana kolom *notes* berguna untuk memberikan catatan singkat terkait media penyimpanan yang ingin diakuisisi. Selanjutnya terdapat kolom *examiner* yang berguna sebagai informasi siapa pengguna aplikasi dan siapa yang melakukan akuisisi. Kolom terakhir yang harus diisi oleh pengguna pada aplikasi akuisisi forensik adalah kolom *image type*. Kolom tersebut berguna untuk menentukan format yang ingin dihasilkan oleh aplikasi ini.

Pada halaman 2 juga terdapat tombol yang dapat digunakan oleh pengguna seperti tombol *back*. Tombol tersebut dapat digunakan untuk kembali ke halaman sebelumnya, kemudian juga ada tombol *start* yang digunakan untuk menjalankan proses akuisisi. Tombol dengan logo *folder* adalah tombol yang digunakan untuk mengisi kolom *image directory*.



Gambar 4. 8 *Progress* Akuisisi

Pada halaman dua juga terdapat *progress* dari aplikasi ketika sudah ditekan tombol *start* yang berarti proses akuisisi sudah berjalan terlihat pada gambar 4.8. *Progress bar* akan mencapai 100% ketika poses akuisisi pada aplikasi akuisisi forensik digial telah selesai dalam proses akuisisi.

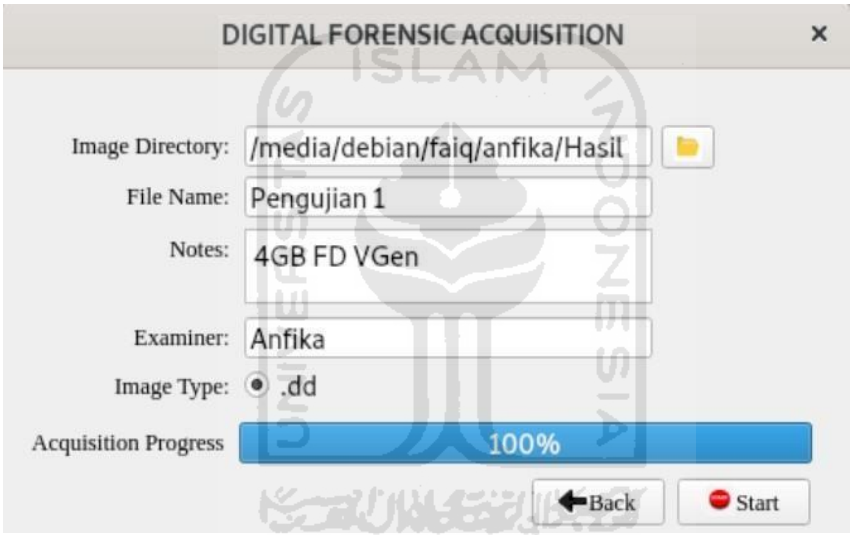
4.2.3 Pembahasan Implementasi Proses Akuisisi

Implementasi proses akuisisi dilakukan untuk menguji sejauh mana aplikasi akuisisi forensik dapat bekerja. Pada saat memulai proses akuisisi dalam menjalankan aplikasi akuisisi forensik digital pada halaman 1, kemudian memilih media peyimpanan mana yang dilakukan akuisisi. Setelah selesai memilih media penyimpanan mana yang di akuisisi, selanjutnya klik tombol next untuk ke halaman selanjutnya yaitu halaman dua dari aplikasi akuisisi forensik digital.

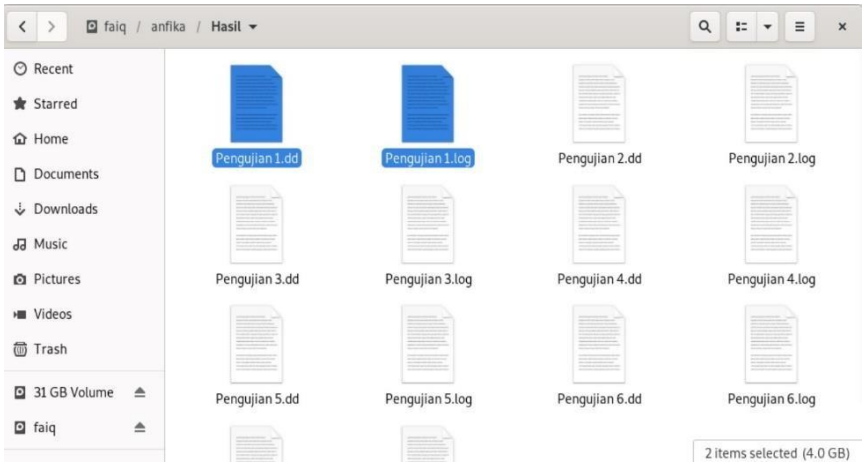
Pada tampilan halaman dua aplikasi akuisisi forensik digital, diminta untuk memasukan data-data pada kolom-kolom yang telah tersedia pada aplikasi akuisisi forensik digital. Pada kolom image directory diisikan tempat penyimpanan atau lokasi untuk menyimpan file hasil akuisisi dari perangkat yang dipilih sebelumnya. Selanjutnya pada kolom *filename* diisikan dengan nama *file* yang ingin dinamakan sesuai dengan keinginan untuk hasil dari hasil akuisisi forensik digital. Kemudian pada kolom *notes* tersebut diisi sesuai catatan-catatan yang ingin ditulis untuk memberikan informasi dari media penyimpanan yang di akuisisi oleh aplikasi akuisisi forensic digital. Selanjutnya kolom *examiner* diisi dengan nama siapa yang menguji perangkat dari proses akuisisi. Terakhir tersedia kolom *image type* yang dimana tersedia *radio botton* untuk dipilih dengan format *file .dd* untuk proses akuisisi forensik digital. Setelah

melengkapi semua data pada kolom dan jika yakin semua data telah benar, maka selanjutnya dilanjutkan dengan menjalankan akuisisi dengan cara menekan tombol *Start.*

Setelah menekan tombol *Start*, maka media penyimpanan yang dipilih akan terjadi proses akuisisi media penyimpanan yang terpilih. Ketika berlangsungnya proses akuisisi, pada tampilan halaman 2 aplikasi akuisisi forensik digital dapat diketahui waktu lamanya proses akuisisi berjalan dan besar ukuran kapasitas penyimpanan melalui *progress bar*, serta dapat juga melihat persentase dari proses akuisisi yang sedang berjalan. Seperti gambar 4.9 setelah proses akuisisi mencapai 100% maka berarti proses tersebut telah selesai dan menghasilkan *file* akhir dengan format ekstensi dd. Hasil dari proses akuisisi dapat dilihat pada folder yang dipilih pada *image directory* pada kolom yang sebelumnya diisi seperti gambar 4.10. Gambar 4.11 merupakan kode program dari proses akuisisi.



Gambar 4. 9 Progress Akuisisi 100%



Gambar 4. 10 Hasil Akuisisi

```
class Akuisisi(QtCore.QThread):
    countChanged = pyqtSignal(int)
    selesai = pyqtSignal(int)

    def run(self):

        c = mainWindow_2.c

        source = mainWindow_2.source

        val = 0

        with open(source,'rb') as f:
            with open(c, "wb") as i:
                 while True:
                       val += 1
                       self.countChanged.emit(val)
                       if i.write(f.read(512)) == 0:
                           print("Acquisition Finished")
                           break
       self.play = Checksum()
        self.play.finished.connect(self.acquisitionFinished)
        self.play.start()

    def acquisitionFinished(self):
        nil = 1
```

Gambar 4. 11 Fungsi Proses Akuisisi

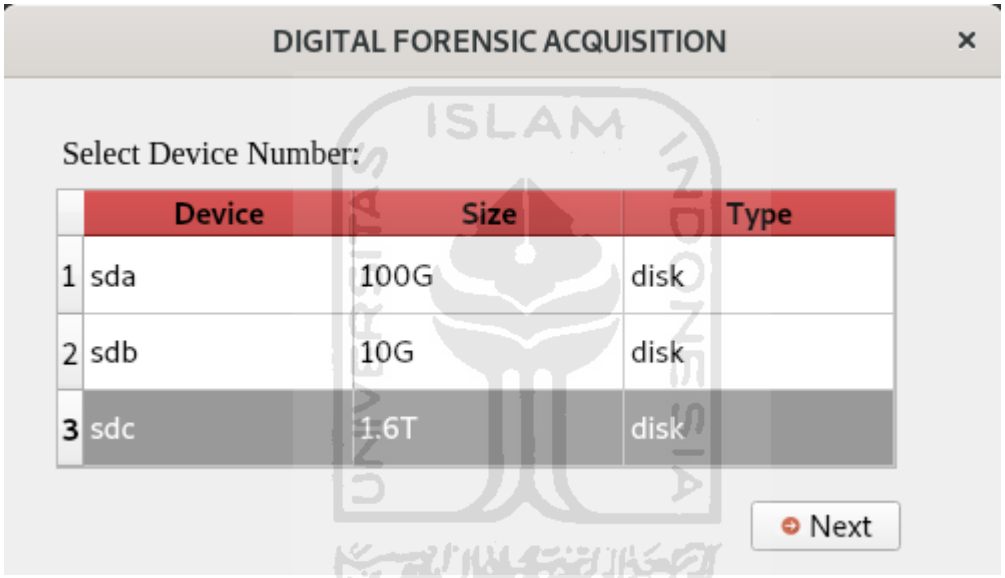
43 Pengujian

4.3.1 Blackbox

Proses pengujian dengan menggunakan teknik *Blakblox* dilakukan dengan cara mengamati apa yang terlihat dari aplikasi akuisisi forensik digital oleh mata pengguna. Ada pengujian yang dilakukan untuk menguji aplikasi akuisisi forensik digital meliputi pengujian fungsi tombol dan *error handling*.

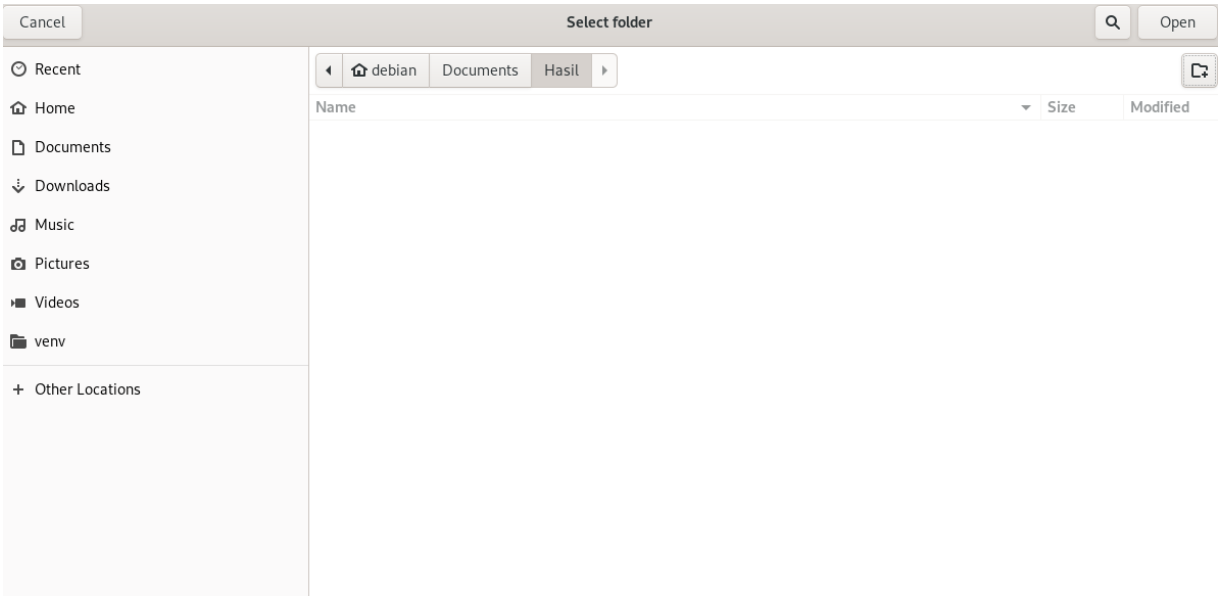
1. Pengujian Tombol

Pada pengujian Halaman 1 aplikasi akuisisi forensik digital terdapat tombol untuk melanjutkan ke halaman berikutnya yaitu tombol *Next* seperti Gambar 4.12. Disini menampilkan semua media penyimpanan yang terhubung dengan perangkat.

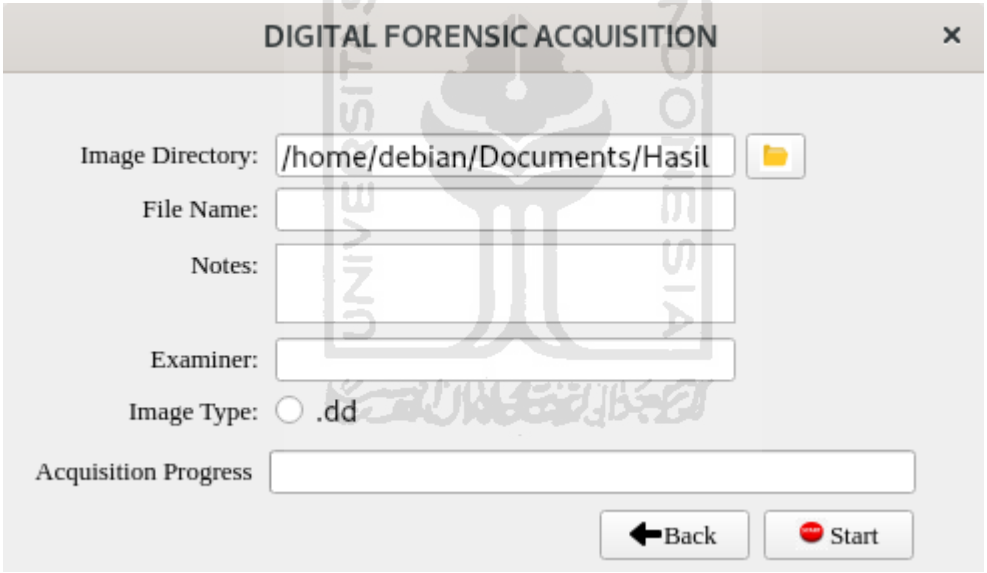


Gambar 4. 12 Fungsi *Next*

Selanjutnya pada pengujian tampilan aplikasi akuisisi forensik digital terdapat 3 tombol. Pertama adalah tombol yang dimana untuk menyimpan hasil akuisisi atau untuk mengisikan *image directory*. Ketika tombol folder maka akan memilih tempat penyimpanan sesuai dengan keinginan seperti pada Gamabr 4.13. Pada Gambar 4.14 merupakan tampilan ketika telah memilih tempat penyimpanan.

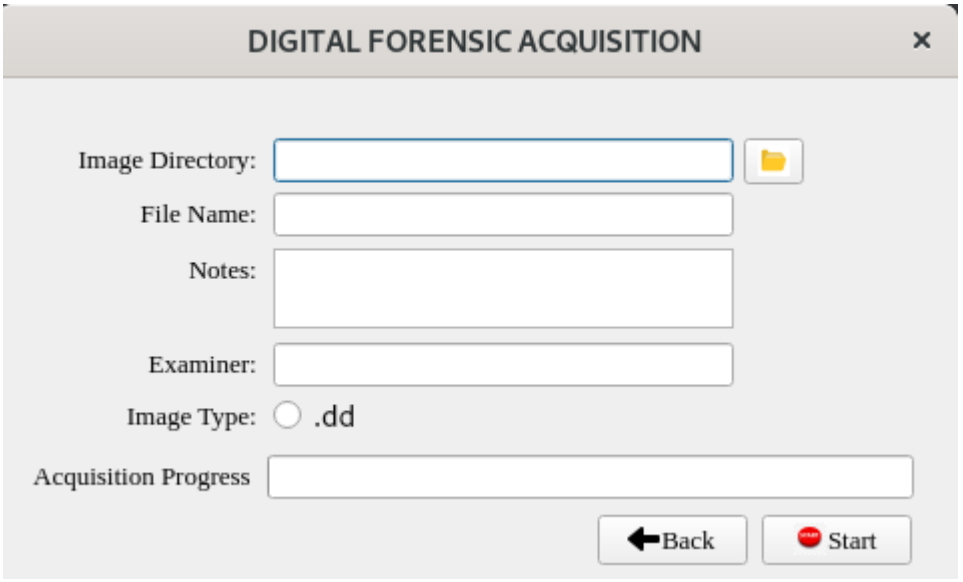


Gambar 4. 13 Pengujian Tombol Direktori

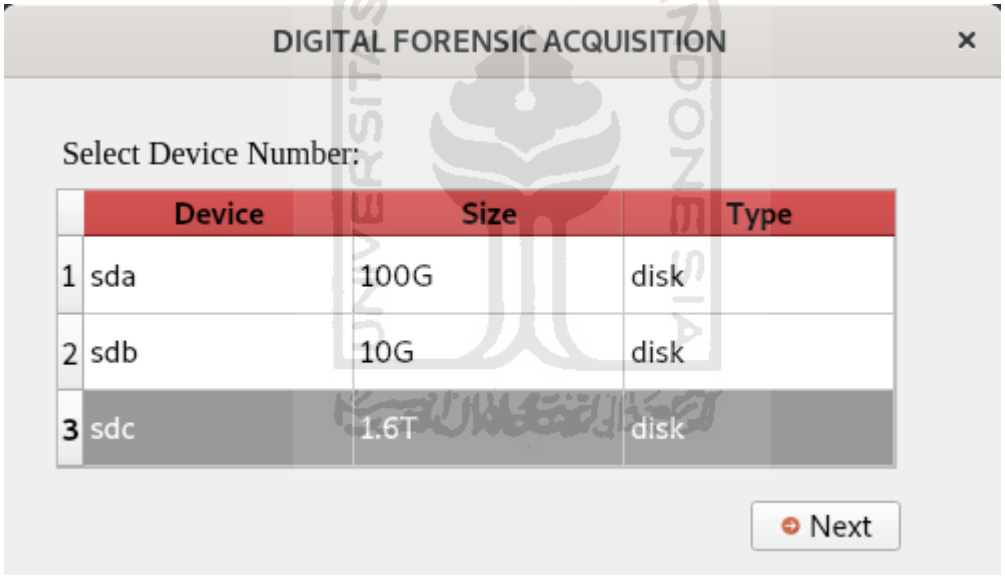


Gambar 4. 14 Pengujian Tombol Direktori

Kedua tombol *back* seperti Gambar 4.15 adalah tombol yang berfungsi untuk kembali ke halaman sebelumnya yaitu Halaman 1, ketika tombol diklik maka akan kembali ke halaman 1 seperti pada Gambar 4.16.



Gambar 4. 15 Pengujian Tombol Fungsi *Back*



Gambar 4. 16 Pengujian Tombol Back

Pada pengujian tombol menggunakan teknik *blackbox* semua tombol sudah dapat berfungsi dengan baik pada aplikasi. Semua tombol pada aplikasi dimulai dari tombol *next, image directory, back,* dan *start* semua berfungsi dengan baik sesuai dengan fungsi masing-masing tombol.

2. Pengujian *error handling*

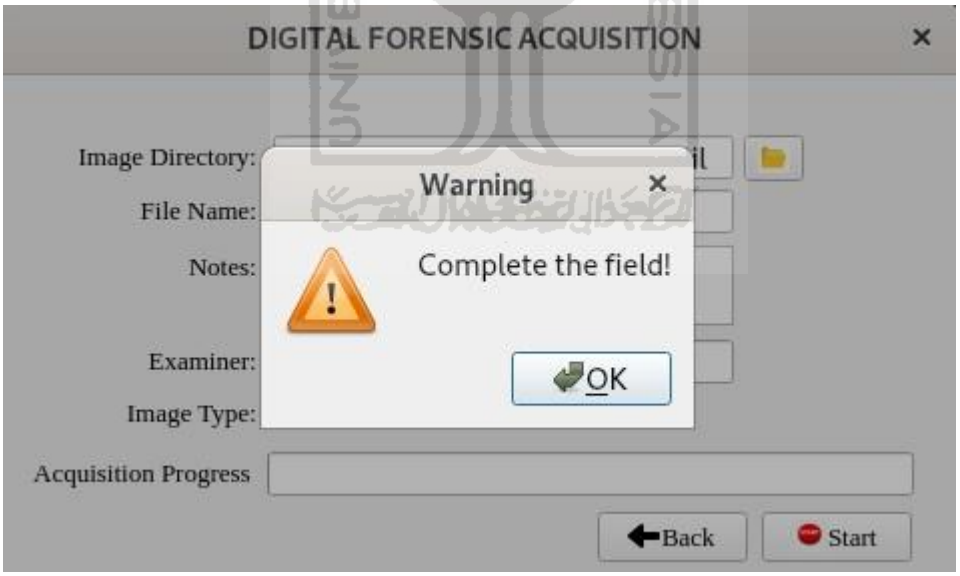
Tahap pengujian *error handling* pada aplikasi akuisisi forensik digital dilakukan dengan cara dibuat berbagai skema yang dapat menguji aplikasi apakah aplikasi dapat tetap berjalan dengan baik apabila data-data yang aplikasi butuhkan tidak dipenuhi oleh pengguna. Skema pertama yang dijalankan adalah peneliti tidak mengisi semua data masukan yang tersedia melalui kolom-kolom, maka ketika skema itu dijalankan aplikasi tidak akan menjalankan proses akuisisi, melainkan mengeluarkan sebuah peringatan yang memberitahukan bahwa pengguna harus melengkapi data masukan melalui kolom-kolom yang tersedia seperti yang terlihat pada Gambar 4.17.

Gambar 4. 17 *Error Handling* Skema 1

Skema kedua yang dijalankan adalah peneliti mengisi kolom *image directory*, tetapi sisa kolom yang tersedia tidak peneliti masukan data. Maka ketika skema ini dijalankan yang terjadi adalah aplikasi tetap tidak dapat menjalankan proses akuisisi dan mengeluarkan peringatan untuk melengkapi data masukan melalui kolom-kolom yang tersedia di aplikasi seperti yang terlihat pada Gambar 4.18.

Gambar 4. 18 *Error Handling* Skema 2

Selanjutnya peneliti menjalankan skema 3 yaitu peneliti mengisi kolom *filename* dan kolom *image directory*. Maka ketika proses skema ini dijalankan yang terjadi adalah aplikasi tidak dapat melakukan proses akuisisi dan mengeluarkan peringatan agar melengkapi data masukan yang dibutuhkan seperti yang terlihat pada Gambar 4.19.

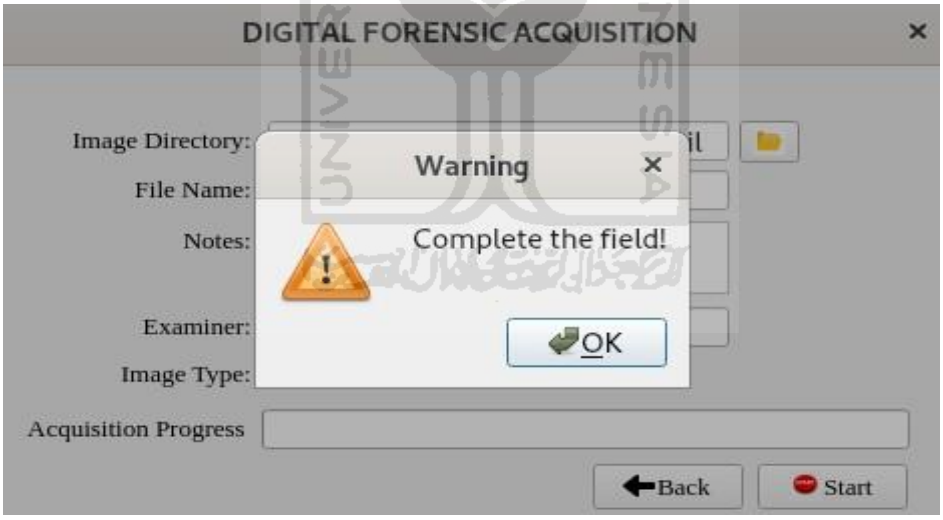


Gambar 4. 19 *Error Handling* Skema 3

Selanjutnya peneliti melanjutkan ke skema empat dimana peneliti mengisi tiga kolom awal, yaitu kolom *image directory*, *filename*, dan *notes*. Pada saat skema ini dijalankan maka yang terjadi adalah aplikasi tetap tidak dapat melanjutkan ke proses akuisisi seperti yang terlihat pada Gambar 4.20.

Gambar 4. 20 *Error Handling* Skema 4

Skema selanjutnya adalah peneliti mengisi empat kolom awal, yaitu kolom *image directory, filename, notes*, dan *examiner*. Maka ketika skema ini dijalankan yang terjadi adalah sama seperti yang terjadi pada skema sebelumnya, yakni aplikasi tidak dapat melakukan proses akuisisi sampi semua kolom-kolom yang tersedia dilengkapi seperti yang terlihat pada Gambar 4.21.



Gambar 4. 21 *Error Handling* Skema 5

Pada pengujian *error handling* menggunakan teknik *blackbox* semua sudah dapat berfungsi dengan baik pada aplikasi. Mulai dari skema 1 sampai skema 5 berjalan sesuai dengan fungsi *error handling* masing-masing pada aplikasi.

4.3.2 Pengujian Performa Aplikasi

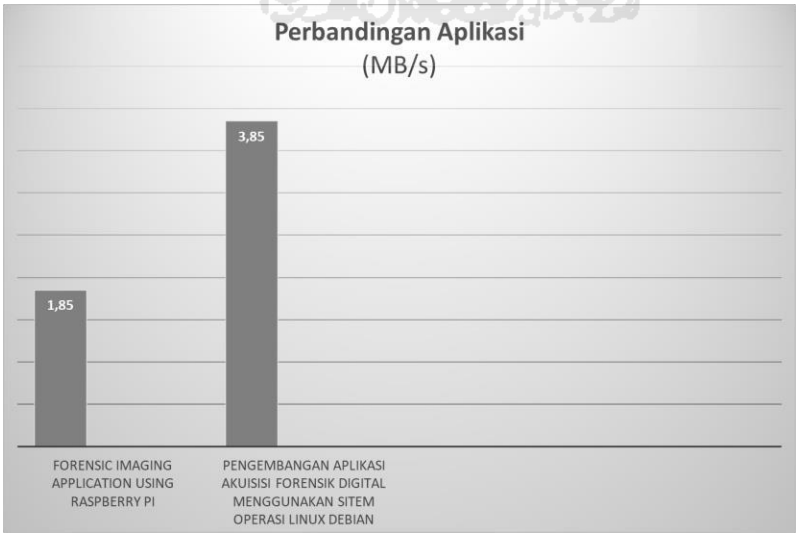
Pada tahap pengujian aplikasi ini merupakan sebuah tahap yang dilakukan untuk mengetahui aplikasi akuisisi forensik digital dalam proses bekerja untuk mengakuisisi media penyimpanan. Dalam pengujian performa aplikasi juga digunakan untuk mengetahui kecepatan proses dalam melakukan akuisisi media penyimpanan dengan menggunakan *flash drive* yang berbeda ukuran maupun sama ukurannya dan berbeda merek. Aplikasi akuisisi forensik digital diuji dalam beberapa kali percobaan mengakuisisi media penyimpanan yang ada dan untuk mengetahui apakah aplikasi akuisisi forensik digital dapat bekerja. Aplikasi akuisisi forensik digital dicoba sebanyak tujuh kali untuk mengakuisisi media penyimpanan yang ada, dapat dilihat cara bekerja aplikasi akuisisi forensik digital dengan melihat dari waktu dalam proses akuisisi dan kecepatan transfer data pada proses akuisisi.

Terdapat tujuh *flashdrive* dengan kapasitas atau ukuran yang berbeda dan merek berbeda untuk proses akuisisi, ukuran dan merek yang digunakan yaitu: 2GB Kingston, 4GB VGen, 8GB Toshiba, 16GB Toshiba, 16GB Generic Custem “Astra Honda”, 16GB Sandisk, dan 32GB Sandisk. Tujuh buah *flash drive* yang ada nantinya dilakukan proses akuisisi dengan menggunakan aplikasi akuisisi forensik digital menggunakan sistem operasi linux debian dan hasil dari proses akuisisi tadi disimpan di *hard disk* berukuran 1TB. Semua *flash drive* dilakukan proses akuisisi secara bergantian dalam melakukan proses akuisisi hingga selesai dan menghitung kecepatan transfer data dari setiap proses akuisisi yang dilakukan. Kemudian dihitung nilai rata-rata dari semua proses untuk kecepatan transfer data dari proses akuisisi pada aplikasi akuisisi forensik digital menggunakan sistem operasi linux debian. Pada tabel 4.1 merupakan daftar *flash drive* yang digunakan dalam proses akuisisi dalam aplikasi forensik digital.

Tabel 4. 1 Hasil Pengujian Media Penyimpanan

No	Ukuran (GB)	Waktu (Menit)	Kecepatan (MB/Second)	Keterangan
1	1.9 GB	8	4,1	Kingston
2	3.8 GB	16	4,1	VGen
3	7.2 GB	32	3,8	Toshiba
4	14.5 GB	62	3,9	Toshiba
5	14.7 GB	68	3,7	Generic Custem “Astra Honda”
6	14.3 GB	66	3,6	Sandisk
7	28.7 GB	130	3,8	Sandisk
Kecepatan rata-rata			**3,85**	

Setelah melakukan semua proses akuisisi satu-satu pada aplikasi akuisisi forensik digital, ada *flash drive* yang ukurannya sama namun berbeda merek yaitu 16GB Toshiba, 16GB Generic Custem “Astra Honda”, dan 16GB Sandisk. Setalah semua kecepatam transfer data dari semua *flash drive* diketahui kecepatan rata-rata dari seluruh *flash drive* yang dilakukan proses akuisisi yaitu sebesar 3,85 MB/s.



Gambar 4. 22 Grafik Perbandingan Kecepatan Transfer Data Aplikasi

Pada Gambar 4.22 terdapat grafik perbandingan “Pengembangan Aplikasi Akuisisi Forensik Digital Menggunakan Sistem Operasi Linux Debian” didapatkan kecepatan rata-rata sebesar 3.85 MB/s dengan menggunakan laptop RAM 8GB dan menggunakan virtual box dalam pengerjaannya. Sedangkan, pada aplikasi “FORENSIC IMAGING APPLICATION USING RASPBERRY PI” dipenelitian sebelumnya didapatkan kecepatan rata-rata sebesar 1.85 MB/s dengan menggunakan Raspberry Pi RAM 1GB. Dapat disimpulkan “Pengembangan Aplikasi Akuisisi Forensik Digital Menggunakan Sistem Operasi Linux Debian” lebih cepat dibandingkan “FORENSIC IMAGING APPLICATION USING RASPBERRY PI” dengan perbandingan 3:1.

BAB V
KESIMPULAN DAN SARAN

5.1 Kesimpulan

Setelah proses penelitian yang dilakukan oleh peneliti dan mengimplementasikannya, kesimpulan yang dapat diambil dari kegiatan tugas akhir dengan judul Pengembangan Aplikasi Akuisisi Forensik Digital adalah:

a. Berhasil mengembangkan aplikasi berbasis Graphical User Interface (GUI) berhasil mengoperasikan perangkat akuisisi berekstensi .dd dengan baik.
b. Berhasil menghitung kecepatan transfer data setiap *flashdrive* berbagai merek dan ukuran, kecepatan rata-rata pada proses akuisisi dalam aplikasi akuisisi forensik digital menggunakan sisten operasi linux Debian yaitu sebesar 3,85 MB/s.

5.2 Saran

Pada Pengembangan Aplikasi Akuisisi Forensik Digital masih terdapat beberapa kelemahan serta kekurangan yang dalam waktu yang akan datang masih dapat dikembangkan agar aplikasi ini dapat lebih baik lagi. Berikut beberapa hal yang masih dapat dikembangkan dari aplikasi Pengembangan Aplikasi Akuisisi Forensik Digital yaitu:

a. Untuk pengembangan aplikasi ini kedepannya diharapkan mampu mengakuisisi semua media penyimpanan tidak hanya *flashdrive*.
b. Diharapkan kedepannya bisa dijalankan di semua sistem operasi.

DAFTAR PUSTAKA

Al-Azhar, M. N. (2012). *Digital Forensic.* Jakarta: Salemba Empat.

Batubara, P. (2017, Desember 21). *Tahun 2017, Polisi Tangani 1.763 Kasus Kejahatan Siber*. Retrieved from Okezone: https://news.okezone.com/read/2017/12/21/337/1833784/tahun-2017-polisi-tangani-1-763-kasus-kejahatan-siber

CNN Indonesia. (2018, Juli 17). *Polri: Indonesia Tertinggi Kedua Kejahatan Siber di Dunia*. Retrieved from CNN Indonesia: https://www.cnnindonesia.com/nasional/20180717140856-12-314780/polri-indonesia-tertinggi-kedua-kejahatan-siber-di-dunia

Garfinkel, S., Malan, D., Stevens, K.-A., & Pham, C. (2006). Advanced Forensic Format: an Open Extensible Format for Disk Imaging.

Hendrik, Anjomshooa, A., & Tjoa, A. M. (2014). Towards Semantic Mashup Tools For Big Data Analysis. *Proceding of the Information & Communication Technology-EurAsia Conference 2014*, (pp. 100-145). Bali.

K, R. M. (2018). *FORENSIC IMAGING APPLICATION.* Yogyakarta.

Kunicki, M. (2020). Data acquisition system for on-line temperature monitoring in power transformers. *Measurement*, 161.

Marwan. (2016, Oktober 19). Retrieved from http://marwannbinadarma.blogspot.com/2016/10/akuisisi-digital-forensik.html

Nidhra, S., & Dondeti, J. (2012). BLACK BOX AND WHITE BOX TESTING. *International Journal of Embedded Systems and Applications (IJESA).*

Prayudi, Y., & Alfrianto, D. S. (2007). Antisipasi Cybercrime Menggunakan Teknik Komputer Forensik. *Snati*, 1-4.

Raharjo, B. (2013). SEKILAS MENGENAI FORENSIK DIGITAL.

Riadi, M. (2018, Maret 3). *Pengertian Cyber Crime* . Retrieved from Kajian Pustaka: https://www.kajianpustaka.com/2018/03/pengertian-bentuk-dan-tindak-pidana-cyber-crime.html

Rossum, G. V. (n.d.). Python tutorial. *Computer Science*.

Rouse, M. (2017, Agustus). *forensic image*. Retrieved from https://whatis.techtarget.com/definition/forensic-image

Sarwono, J. (2006). *Metode penelitian kuantitatif & kualiatif.* Yogyakarta: Graha Ilmu.

Selamat datang di KBBI Daring! (2020). Retrieved from KBBI Daring: https://kbbi.kemdikbud.go.id/

Setiawan, A. M. (2013). *Integrated Framework For Business Process Complexity Analysis*. Retrieved from ECIS 2013 Completed Research: http://aisel.aisnet.org/ecis2013_cr/49

Taufiq, H. (2015). *Argumentasi dan Validitas.* Yogyakarta: Darqin.

U.s. Department of Justice. (2014). *Forensic Examination of Digital Evidence: A Guide for Law Enforcement.* CreateSpace Independent Publishing Platform.

Wahid, F. (2014). The Antecedents And Impacts of a Green Eprocurement Infrastructure: Evidence From The Indonesian Public Sector. *International Journal of internet Protocol Technology*, *7*(4), 210-218.

YDR. (2015, November 17). *Kemkominfo Tengah Siapkan Standardisasi Bukti Digital*. Retrieved from KOMINFO: https://kominfo.go.id/index.php/content/detail/6418/Kemkominfo+Tengah+Siapkan+Standardisasi+Bukti+Digital/0/berita_satker

Zukhri, Z. (2014). *Algoritma Genetika: Metode Komputasi Evolusioner untuk Menyelesaikan Masalah Optimasi.* Yogyakarta: Andi Publisher.

LAMPIRAN