PERANCANGAN NENGGALA *DISK DUPLICATOR* (NDD) UNTUK MENDUKUNG PROSES INVESTIGASI FORENSIK DIGITAL

Fietyata Yudha

Jurusan Teknik Informatika, Fakultas Teknologi Industri, Universitas Islam Indonesia
Jl. Kaliurang Km.14,5 Sleman, Yogyakarta 55501
E-Mail : yudha@uii.ac.id

ABSTRACT

The development of information technology simplify human life. Its evoke crime loopholes, cyber crime. When solving criminal cases that utilize information technology is required the digital forensic science. In carrying out a digital investigation known multiple frameworks around the worlds. Every devices, every organization has their own framework. The most common framework divided into 4 sections. Preservation, Acquisition, Analysis, and Reporting are the most common used around the worlds. Acquisition is a key part of the investigation process because in this process digital evidence is collected form the electronic evidence. The acquisition processes uses special equipment. Forensic acquisition equipment mostly made by forensic vendors in the world. The problems that arise in the academic realm is the price of the equipment is quite expensive. The existence of the above problem there is a gap to conduct research on the applied field of development of tools for forensic acquisition. This study provides an early overview of the design of a digital forensics acquisition tool called Nenggala Disk Duplicator.

Keywords : Digital Forensic, Acquisition, Hardware.

1. PENDAHULUAN

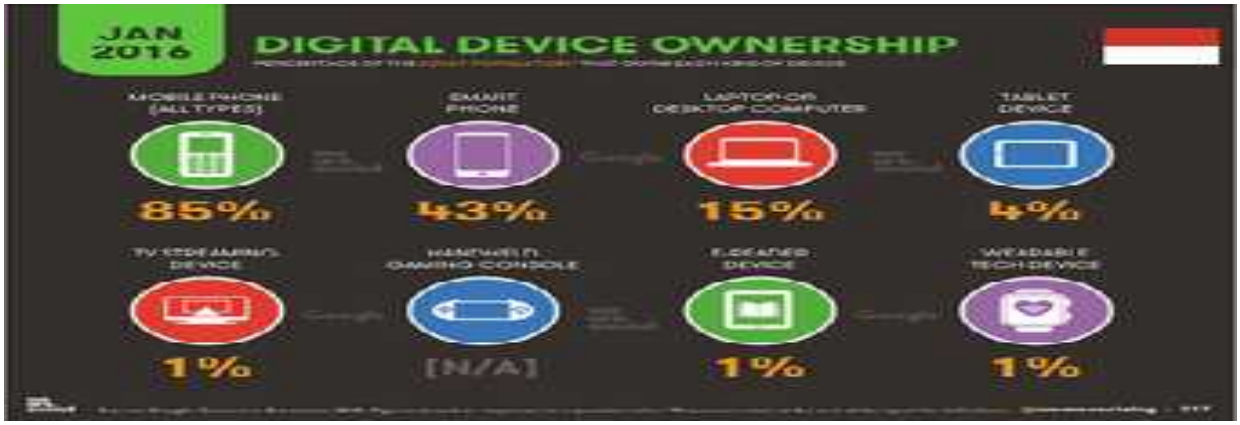
Teknologi informasi berkembang sedemikian pesatnya, semakin memudahkan manusia dalam beraktifitas. Berdasarkan data yang diperoleh dari *wearesocial.com*, 85% penduduk Indonesia memiliki perangkat telepon seluler (Gambar 1). Dengan segala kemudahan dan kelebihan yang dimiliki manusia sebagai pengguna, menyebabkan terdapat sebagian orang yang memanfaatkan teknologi untuk hal - hal yang melanggar norma - norma kehidupan. Terdapat berbagai jenis pelanggaran yang dilakukan dengan memanfaatkan teknologi khususnya teknoligi informasi dan internet.

Kejahatan siber merupakan istilah yang digunakan untuk menggambarkan tindakan kejahatan yang dilakukan dengan memanfaatkan teknologi informasi sebagai sarana, tempat melakukan kejahatan. Berdasarkan data tahunan yang diterbitkan oleh Verizon, setiap tahunnya kejahatan siber semakin meningkat. *Hacking*, *malware*, dan *social engineering* menempati 3 urutan teratas kejahatan siber. Data ini di konversi dari laporan masyarakat terhadap kejahatan siber yang meraka alami. Gambar 2 menunjukkan grafik tingkat kejahatan siber didunia berdasarkan data yang dimiliki oleh Verizon dari tahun 2005 hingga 2015. Pada grafik tersebut terlihat peningkatan jumlah kejahatan siber di tahun 2009 dan terus meningkat.

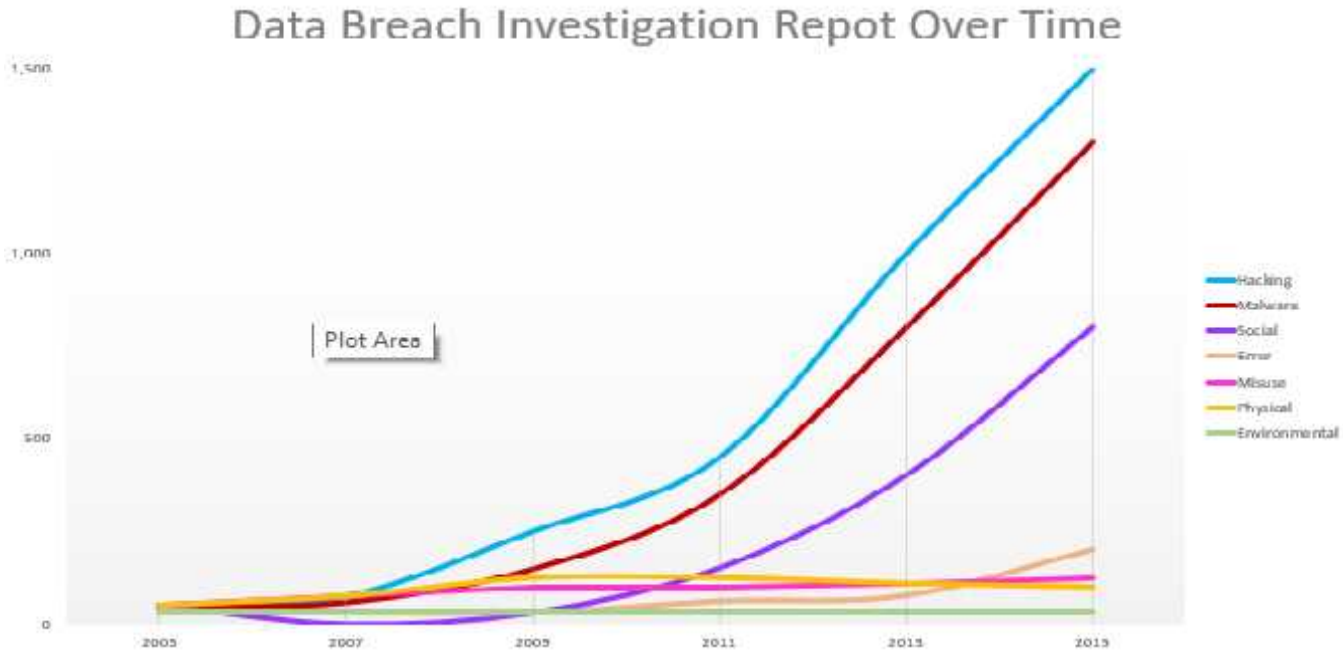
Forensik digital muncul sebagai implikasi penyalahgunaan teknologi informasi. Dalam bidang kelimuan forensik digital, dikenal tahapan yang disebut akuisisi. Dalam tahap akuisisi ini terdapat proses yang sering disebut sebagai imaging. Dalam melakukan proses imaging pada umumnya dapat mempergunakan perangkat komputer, namun ukuran perangkat merupakan permasalahan terbesar ketika melakukan proses imaging degnan menggunakan PC. Perangkat dengan ukuran yang kecil dan mudah untuk dibawa sudah pernah dirancang dan pernah ada sebelumnya, permasalahan dari perangkat tersebut adalah harga yang cukup mahal sehingga tidak semua penyidik forensik dapat memiliki perangkat tersebut. Sebagai sebuah solusi terdapat perangkat yang dapat

melakukan proses imaging lebih cepat dan memiliki ukuran yang tidak terlalu besar serta biaya yang murah. Sehingga mudah untuk digunakan dan dibawa oleh penyidik forensik.

Beberapa penilitian sebelumnya telah dilakukan dalam bidang forensika digital oleh peneliti terutama pada ranah konseptual dan juga ranah praktis. Pada ranah praktis telah dilakukan penelitian sebelumnya telah terkati pembuatan *tools analisys forensic digital* berbasis *USB*. Pada penelitian ini bertujuan untuk membangun sebuah purwarupa perangkat *imaging* barang bukti *harddisk* berbasis *single board* komputer dan aplikasi sumber terbuka. Dengan memanfaatkan *single board* komputer dan aplikasi sumber terbuka, biaya yang dibutuhkan untuk mengembangkan perangkat ini menjadi lebih murahsehingga perangkat yang dihasilkan dapat membantu proses investigasi digital dan mempermudah proses akuisisi data dan harga yang lebih murah. Pada penelitian ini peneliti berusaha melakukan perancangan sebuah perangkat untuk melakukan akuisisi barang bukti *harddisk* yang mudah untuk dibawa dengan biaya minimal yang nantinya hasil perancangan yang sudah dilakukan ini dapat diimplementasikan menjadi sebuah purwarupa perangkat akuisisi.



Gambar 1. Infografis Kepemilikan Perangkat Digital di Indonesia.
(sumber : S. Kemp, 2016)



Gambar 2. Data *Breach Investigation Report Over Time*.
(sumber : Verizon, 2016)

2. KAJIAN PUSTAKA

Perangkat forensik digital sudah menjadi hal yang umum digunakan untuk memecahkan kasus - kasus *cybercrime*. Penggunaan perangkat yang baik menentukan keberhasilan proses investigasi digital. Fungsi hash memiliki peranan penting dalam proses akuisisi, fungsi ini dapat menjamin keaslian barang bukti digital (N. Kishore and B. Kapoor, 2015).

Perdebatan antara sumber terbuka dan sumber tertutup dalam disiplin ilmu komputer sudah terjadi sejak dahulu. Hal ini juga berdampak pada alat analisis forensik digital, untuk mendefinisikan alat mana yang diterima untuk penegakan hukum. Untuk dapat dibuktikan dipengadilan, alat yang digunakan harus dapat diandalkan dan relevan. Kehandalan dapat diuji dengan pedoman *Daubert* (B. B. Carrier and I. Management, 2002).

D. R. Kamble dan N. Jain, ditahun 2015 menyatakan bahwa sebuah faktor kunci terpenting dalam proses penyidikan digital adalah bahwa, forensik digital mampu untuk melakukan pemetakan peristiwa yang terjadi. Berbagai sumber barang bukti dapat digunakan untuk pembuktian insiden. Aplikasi komputer yang digunakan untuk menyelidiki kejahatan berbasis komputer, telah menyebabkan pengembangan lapangan baru.

Sementara itu P. Kanellis dan kawan – kawan pada tahun 2006 mengungkapkan, penyidik forensik digital memiliki akses ke berbagai aplikasi, baik aplikasi komersial maupun aplikasi sumber terbuka yang dapat dipergunakan ditahap awal maupun tahap analisis. Beberapa aplikasi tidak dapat mengimbangi perkembangan media penyimpanan yang terus meningkat. Dengan mempergunakan perangkat dengan komputasi tinggi penyidik dapat mempergunakan waktu secara efisien dalam proses penyelidikan.

Saat ini *Graphics Processing Unit* (GPU) mengandung sejumlah besar prosesor, dimana unit perangkat keras ini memiliki tujuan khusus seperti tekstur dan *vertex shader*. Kemunculan forensik digital membuat ketersediaan kekuatan pemrosesan yang lebih penting. Hal ini mencakup peningkatan besar dalam ukuran rata - rata (diukur dalam *byte*) dari target forensik, peningkatan jumlah kasus forensik digital, dan pengembangan "generasi" alat yang memerlukan lebih banyak sumber daya komputasi (L. Marziale, etc, 2007).

Single board computer merupakan sebuah komputer yang dibuat dengan sirkuit tunggal. Komputer ini merupakan kombinasi antara *motherboard* dan *daughterboard* yang biasa digunakan pada perangkat komputer personal. Perangkat ini sering dipergunakan sebagai pengendali dan antarmuka dalam perangkat lain. Perangkat ini juga dikenal dengan *credit card PC* dikarenakan ukuran komputer ini hanya sebesar ukuran kartu kredit saja.

Raspberry Pi merupakan pelopor *single board* komputer dengan biaya rendah (gambar 3). Perangkat ini dapat dihubungkan ke monitor komputer atau TV, dengan menggunakan *keyboard* standar dan *mouse*. Merupakan perangkat kecil yang mampu yang memungkinkan orang dari segala usia untuk mengeksplorasi komputasi, dan belajar bagaimana program dalam bahasa seperti *Scratch* dan *Python*. Mampu melakukan segala sesuatu yang Anda harapkan komputer *desktop* untuk melakukan, dari *browsing internet* dan bermain *video high - definition*, untuk membuat *spreadsheet*, pengolah kata, dan bermain *game*.

Roseapple Pi adalah sebuah SBC yang memiliki kinerja yang baik dan memiliki efisiensi daya (Roseapple Pi, 2015). Perangkat ini juga memiliki spesifikasi yang cukup mumpuni dikelas *single board* komputer. Gambar 4 merupakan *single* komputer *board* keluaran dari *roseapple*, pada gambar tersebut dapat dilihat kapasitas RAM yang ditanamkan pada *Roseapple*

lebih besar dari kapasitas RAM pada perangkat *single board* komputer lainnya.

Salah satu *vendor* yang cukup gencar memasarkan produk perangkat keras forensik adalah *Tableau*. Produk *Tableau* dirancang dan dibangun untuk memenuhi kebutuhan masyarakat forensik digital diseluruh dunia. Duplikator, *write blocker*, dan berbagai *utilitas* dalam melakukan tugas penyidikan forensik digital.

Gambar 3. *Single Board Computer* Dari *Raspberry Pi*.

Gambar 4. *Single Board PC* Dari *Roseapple Pi*.

Gambar 5. *Tableau* $TD2_U$.

Tableau Forensic Bridge (*write-blocker*) merupakan perangkat *write blocker* yang banyak digunakan oleh penyidik forensik digital dan diakui di dunia (I. Guidance Software, 2016). *Tableau forensic bridge* mendukung beberapa *mode* penggunaan sesuai dengan kebutuhan penyidik. Selain *Tableau forensic bridge*, juga mengembangkan perangkat *forensic duplicator*. *Tableau TD2u forensic duplicator* merupakan perangkat yang digunakan untuk melakukan proses akuisisi data (*imaging*) (I. Guidance Software , 2016). Perangkat ini memiliki beberapa antarmuka dan juga layar *LCD* (gambar 5).

Imaging merupakan tahapan dimana isi dari seluruh media penyimpanan disalin. Poin penting pada proses ini adalah bahwa keseluruhan isi dari media penyimpanan disalin termasuk juga lokasi data. *Disk imaging* menyalin data dengan metode *sector – by - sector* yang sesuai tujuan investigasi forensik. Selain itu pada proses ini terdapat juga mekanisme (verifikasi internal) untuk membuktikan bahwa salinan tersebut tepat dan belum pernah diubah. Proses ini tidak selalu membutuhkan geometri yang sama dengan aslinya.

Model *forensic imaging disk to disk* merupakan metode *imaging* dengan sumber dan hasil sama - sama dalam berntuk perangkat keras, sehingga barang bukti yang dihasilkan mirip seperti aslinya. Kelemahan dari metode ini adalah terlalu banyak memakan tempat ketika akan melakukan penyimpanan barang bukti. Gambar 6 menunjukkan penggunaan model *disk to disk*. Namun dalam perkembangannya model ini membutuhkan sumber daya berupa media penyimpanan sejenis yang cukup banyak. Selain ini metode ini juga memiliki kendala berupa kebutuhan akan ruang penyimpanan barang bukti karena hasil dari proses akuisisi dengan metode ini adalah berbentuk fisik.

Gambar 6. Akuisisi Dengan Model *Disk to Disk*.

3. METODE PENELITIAN

Dalam proses penyelesaian masalah biasanya akan dibuat sebuah alur penyelsaian masalah. Begitu juga permasalahan yang ada dalam penelitian ini. Pada penelitian ini, peneliti membuat alur penyelsaian penelitian dalam bentuk diagram alir. Diagram alir dari penelitian ini dapat dilihat pada gambar 7. Adapun alur penelitian ini dibuat dengan membagi proses penelitian menjadi 3 tahapan. Tahapan tersebut antara lain :

1. Studi Pustaka

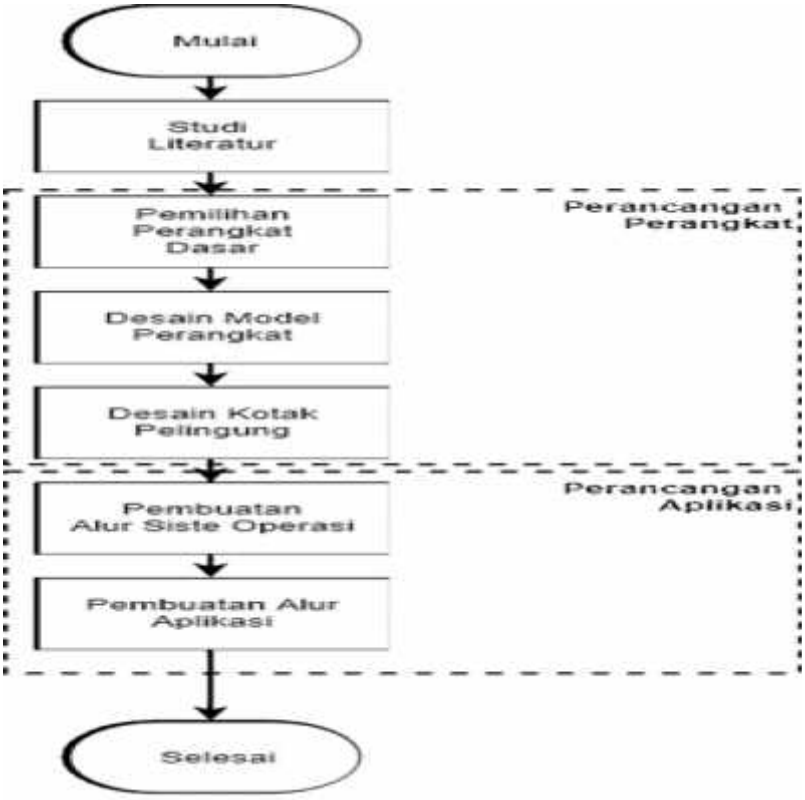
Tahap ini peneliti melakukan pengumpulan referensi terkait penelitian yang akan dilakukan. Peneliti mengumpulkan referensi terkait forensik digital, *raspberry pi*, *single board PC*, dan terkait *remasteing* sistem operasi *Linux*. Selain itu juga diperlukan pustaka mengenai perangkat akuisisi forensik digital yang sudah pernah ada sebelumnya. Pustaka mengenai perangkat yang ada sebelumnya diperlukan untuk melihat kemampuan, fitur, dan spesifikasi dari perangkat tersebut, sehingga dalam perancangan perangkat berikutnya dapat di analisa kebutuhan akan perangkat yang akan dipergunakan. Semua pustaka tersebut nantinya akan membantu proses perancangan yang akan dilakukan.

2. Perancangan Perangkat

Pada tahapan ini peneliti melakukan perancangan perangkat yang akan digunakan untuk membuat perangkat akuisisi nantinya. Tahapan ini dibagi menjadi 3 sub tahapan. Sub tahapan itu adalah pemilihan perangkat dasar yang akan digunakan, pembuatan desain model perangkat rancangan.

3. Perancangan Aplikasi

Tahapan ini peneliti melakukan perancangan aplikasi. Perancangan aplikasi dibagi ke dalam 2 sub tahapan. Sub tahapan tersebut adalah perancangan alur sistem operasi dan perancangan alur aplikasi akuisisi.



Gambar 7. Alur Penyelsaian Masalah.

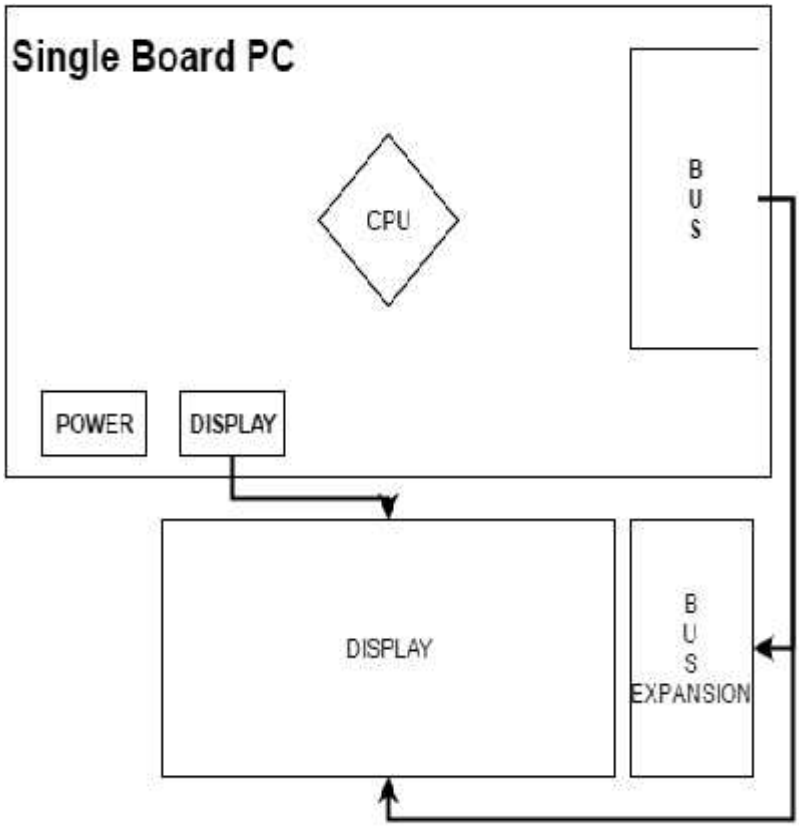
4. HASIL DAN PEMBAHASAN

Berdasarkan alur penelitian yang sudah dibuat sebelumnya, maka tahapan perancangan yang harus dilakukan adalah perancangan perangkat. Sub tahapan perancangan perangkat yang pertama adalah pemilihan perangkat dasar. Hal ini dilakukan karena terdapat berbagai jenis dan merek *single board PC* yang beredar di pasaran. Sehingga diperlukan pemilihan *single board PC* yang sesuai untuk menjalankan aplikasi dan sistem operasi.

Single board computer yang dipilih adalah *single board* keluaran dari *Raspberry Pi*. Alasan digunakan perangkat ini adalah karena *Raspberry Pi* merupakan pionir pengembangan *single board PC*. Selain itu penggunaan perangkat ini di dunia sudah sangat luas, sehingga dukungan untuk proses pengembangan juga tergolong mudah. Juga dukungan terhadap penggunaan perangkat-perangkat tambahan seperti layar, sensor dan lain - lain.

Kebutuhan akan kecepatan berbanding lurus dengan kebutuhan waktu pada perangkat yang dirancang ini. Dengan kecepatan transfer yang tinggi, waktu yang dibutuhkan untuk melakukan proses akuisisi akan lebih cepat. Model rancangan struktur perangkat yang dikembangkan dapat dilihat pada gambar 8. Selain perancangan struktur, dilakukan juga desain wadah yang akan digunakan. Wadah yang akan digunakan didesain untuk dapat menampung layar yang ada pada perangkat yang dirancang.

Selain perancangan struktur, dilakukan juga desain wadah yang akan digunakan. Wadah yang akan digunakan didesain untuk dapat menampung layar yang ada pada perangkat yang dirancang. Perangkat akan menampung layar sebesar 3,5 inci. Layar akan difungsikan sebagai informasi proses yang sedang dilakukan perangkat ketika melakukan akusisi bukti digital.

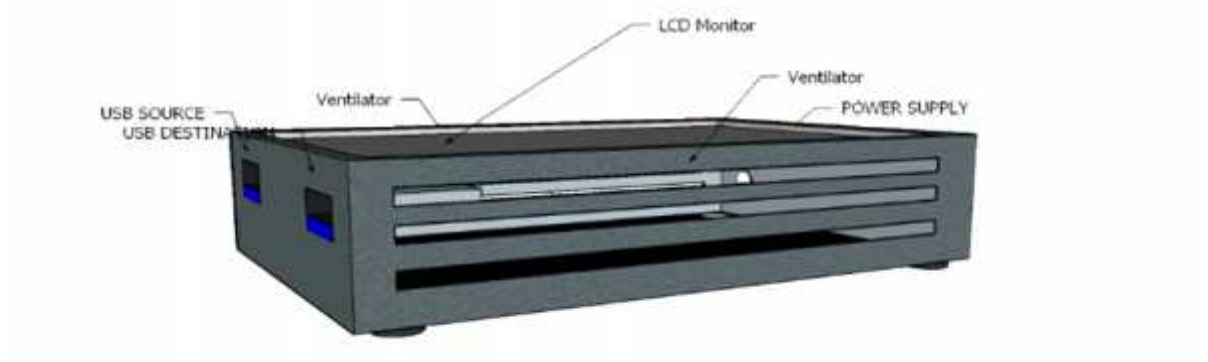


Gambar 8. Rancangan Struktur Perangkat NDD.

Tahapan berikutnya dalam proses perancangan ini adalah tahapan perancangan perangkat lunak. Tahapan perancangan perangkat lunak dibagi menjadi 2 sub tahapan yaitu bagian perancangan sistem operasi dan bagian perancangan aplikasi. Pembagian ini dimaksudkan agar perangkat yang dihasilkan nantinya memiliki hasil yang maksimal.

Pada gambar 11 menunjukkan diagram alir proses ketika perangkat dihidupkan. Proses yang terjadi adalah proses *booting* yang didalamnya akan ada proses pembacaan *kernel*, dilanjutkan dengan proses pengaktifan servis, dan proses yang teralkhir adalah proses menjalankan aplikasi akuisisi. Adapun sistem operasi dasar yang akan digunakan adalah sistem operasi berbasis *Debian*. Untuk memaksimalkan performa yang dimiliki oleh perangkat *single board* komputer tersebut dilakukan beberapa hal :

1. **Optimasi Kernel**
   Optimasi kernel dilakukan dengan mengubah konfigurasi kernel sehingga didapatkan hasil berupa proses *booting* yang lebih cepat. Konfigurasi ini akan di jalankan pada saat komputer melakukan proses *booting*.
2. **Menghapus Aplikasi**
   Sistem operasi yang digunakan pada model *single board* PC biasanya adalah sistem operasi dalam bentuk berkas *image*. Pengguna hanya perlu melakukan konversi berkas *image* tersebut kedalam media penyimpanan *sdcard*. Pada saat instalasi sistem operasi dasar terdapat beberapa aplikasi bawaan yang dimungkinkan akan memberatkan kinerja sistem, sehingga perlu dilakukan penghapusan untuk memperingan kerja sistem.
3. **Menghapus Servis**
   Sama halnya dengan poin nomor 3 diatas. Ketika melakukan instalasi sistem operasi, terdapat beberapa aplikasi yang membawa servis bawaan. Diperlukan pengecekan ulang terhadap servis yang berjalan pada sistem operasi yang dikembangkan. Servis merupakan kunci utama dalam sistem operasi. Seperti halnya aplikasi, ketika sistem operasi dasar dipasang makan aka nada servis - servis bawaan yang di mungkinkan memberatkan kinerja sistem.



Gambar 9. Desain Wadah NDD Keras Tampak Samping.

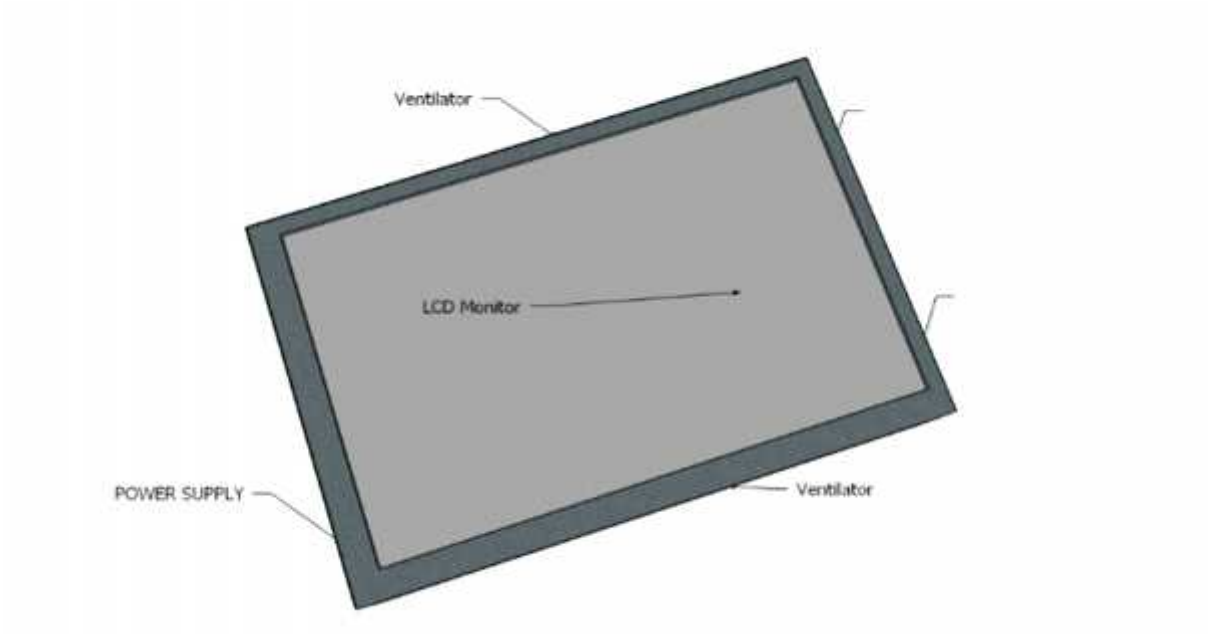
Gambar 1Gambar2 menunjukkan proses yang terjadi ketika aplikasi akuisisi berjalan. Proses dimulai dengan pembacaan perangkat yang terpasang pada antar muka USB. Pada sistem berbasis *Linux* setiap media penyimpan terpasang pada sistem operasi akan dibaca sebagai perangkat pada *direktori /dev/*. Untuk perangkat pertama yang terpasang akan mendapatkan label sebagai */dev/sda*, biasanya label ini diberikan kepada media penyimpanan internal yang berisi sistem operasi. sedangkan partisi yang ada dalam media penyimpanan tesebut, label yang diberikan ditambah angka dibelakang.

Proses yang dilakukan perangkat akuisisi ketika menerima perangkat penyimapanan baru (media penyimpanan kedua) maka perangkat tersebut akan mendapatkan label */dev/sdb*. Label ini akan digunakan sebagai perangkat sumber. Perangkat sumber akan diikat (*mount*) dengan *mode read - only*. Mode ini merupakan mode agar perangkat sumber tidak mendapatkan data tambahan ketika proses akuisisi. Hal yang sama dilakukan oleh perangkat *Forensic Bridge* dari *Tableau*.

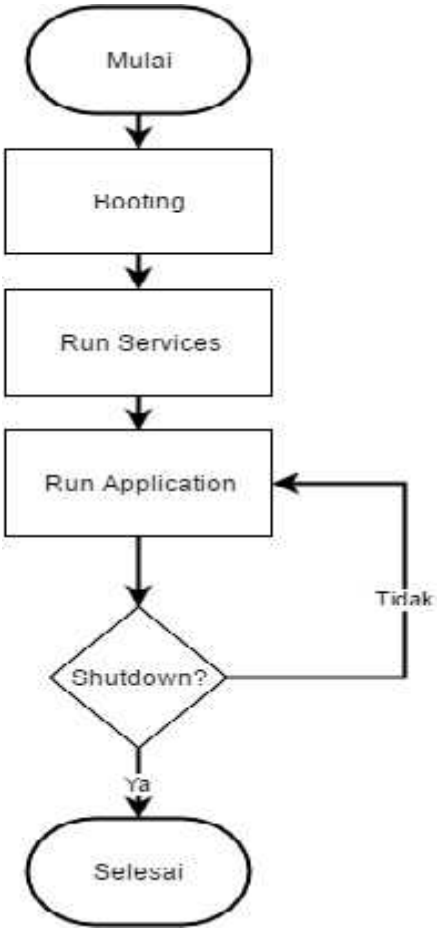
Perangkat penyimpanan ketiga yang terpasang diasumsikan akan mendapatkan label */dev/sdc*. Perangkat ini akan dipergunakan sebagai perangkat tujuan akuisisi. Para perangkat purwarupa ini akuisisi yang digunakan adalah akuisisi model *disk to file*.

Ketika kedua label tersebut sudah terbaca oleh aplikasi maka aplikasi akan menjalankan perintah *dd* untuk melakukan *imaging* dari perangkat penyimpanan sumber. Hasil dari proses ini akan menghasilkan berkas dalam format RAW dengan nama berkas sesuai tanggal saat menjalankan aplikasi tersebut. Dalam proses akuisisi perangkat juga akan menghasilkan nilai *hash* dan laporan hasil akuisisi.

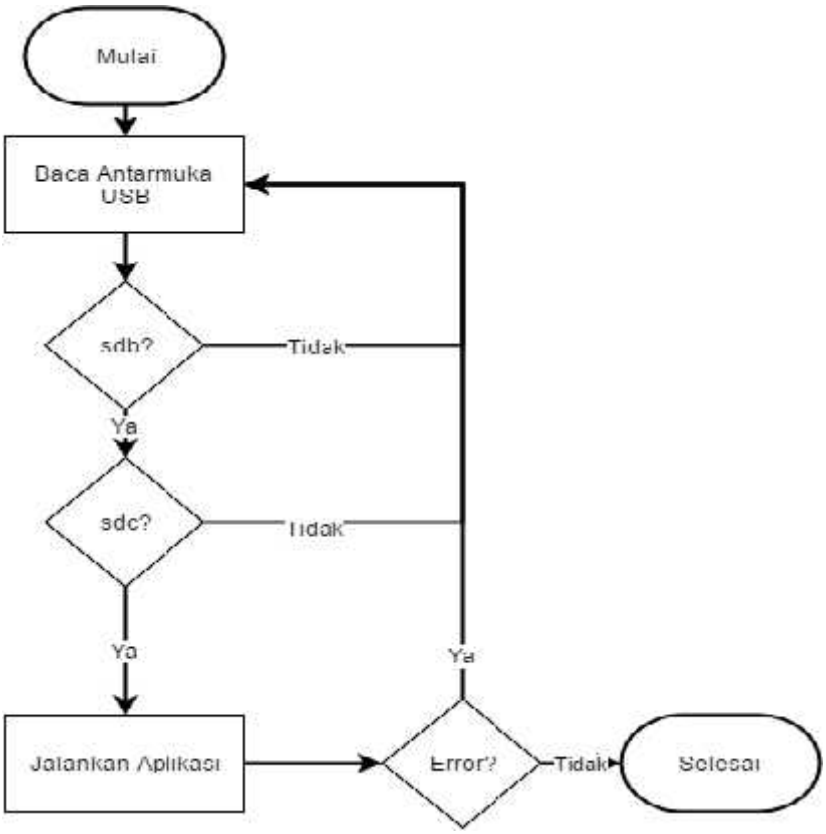
Ketika terjadi kesalah dalam proses yang terjadi maka aplikasi akan melakukan pembacaan ulang antarmuka USB dari awal proses. ketika salah satu label tidak terbaca maka proses akan diulang kembali. Begitu juga dengan proses *imaging* ketika terjadi kesalahan maka akan ada pesan kesalahan dan proses diulang kembali dari awal.



Gambar 10. Desain Wadah NDD Keras Tampak Atas.



Gambar 11. Diagram Alir Sistem Operasi Pada NDD.



Gambar 12. Diagram Alir Alur Aplikasi NDD.

5. KESIMPULAN DAN SARAN

5.1. Kesimpulan

Berdasarkan penelitian yang sudah dilakukan, permasalahan perancangan perangkat NDD pada penelitian ini dapat dipecahkan. Adapun kesimpulan yang dapat diambil dari penelitian yang dilakukan adalah sebagai berikut :

1. Berdasarkan kajian pustaka yang dikakukan belum banyak peneliti yang mencoba melakukan pengembangan perangkat akuisisi forensik digital diluar perusahaan-perusahaan forensik digital yang sudah mengembangkannya secara mandiri.
2. Perangkat NDD yang dirancangan akan mempergunakan jenis *single board PC* dari *Raspberry Pi*. Perangkat dipilih karena dukungan pengguna yang cukup luas.
3. Pada aplikasi yang dirancang, terdapat 2 tahapan yang diperlukan yaitu tahapan perancangan sistem operasi dan perancangan aplikasi. Perancangan sistem operasi dilakukan untuk membuat daftar proses yang harus dilakukan untuk optimalisasi sistem operasi, sehingga proses *booting* yan dilakukan berjalan cepat.

5.2. Saran

Berdasarkan proses yang dilakukan dan juga kesimpulan yang ditarik diatas. Maka saran dari penelitan ini adalah dilakukannya implementasi dari perancangan yang sudah dilakukan pada perangkat sesungguhnya, sehingga bisa didapatkan sebuah purwarupa perangkat akusisi forensik digital yang bukan berasal dari perusahaan komersil yang sudah ada dipasaran. Selain itu desain yang dibuat juga diperlukan penyempurnaan agar perangkat dapat berjalan dengan optimal.

Ucapan Terima Kasih

Penulis mengucapkan terima kasih kepada Direktorat Penelitian dan Pengabdian Masyarakat (DPPM), Universitas Islam Indonesia yang telah memberikan dana penelitian sehingga dapat terselesaikannya seluruh tahapan penelitian ini penelitian ini.

DAFTAR PUSTAKA

B. B. Carrier and I. Management. " *Open Source Digital Forensics Tools : The Legal Argument This paper addresses digital forensic analysis tools and their use in a legal setting . To enter scientific evidence into a United States court , a tool must be reliable and relevant . The reliabili* ". no. October., 2002

D. R. Kamble and N. Jain. " *Digital Forensic Tools : a Comparative Approach* ". Vol. 8354, no. 4., 2015.

I. Guidance Software. " Forensic Bridge Overview "., 2016.

I. Guidance Software. " TD2U FORENSIC "., 2016.

L. Marziale, G. G. Richard III, and V. Roussev. " *Massive threading : Using GPUs to Increase The Performance of Digital Forensics Tools* ". Digit. Investig., Vol. 4, pp. 73–81., 2007.

N. Kishore and B. Kapoor. " *Faster File Imaging Framework for Digital Forensics* ", Procedia Comput. Sci., vol. 49, pp. 74–81., 2015.

P. Kanellis, E. Kiountouzis, N. Kolokotronis, and D. Martakos. Digital Crime and Forensic Science in Cyberspace. Hesley, PA: Idea Group Publishing., 2006.

RoseapplePi. " About – Roseapple Pi., [Online]. Available : *http://roseapplepi.org/index.php/about/*. [Accessed: 29-May-2016]., 2015.

S. Kemp. Digital in 2016 - We Are Social UK ", wearesocial.com, 2016. [Online]. Available : *http://wearesocial.com/uk/special-reports/digital-in-2016*. Accessed : 06-May-2016., 2006.

Verizon. Data Breach Investigations Report," Verizon Bus. J., no. 1, pp. 1–65., 2016.