USB ANALISYS TOOL UNTUK INVESTIGASI FORENSIKA DIGITAL

Fietyata Yudha

Jurusan Teknik Informatika, Fakultas Teknologi Industri, Universitas Islam Indonesia,
Jl. Kaliurang Km. 14,5, Ngemplak, Sleman, Yogyakarta, 55584
Email : fietyatayudha@gmail. com

ABSTRACT

Analysis of the core phase of solving cases of computer crime. Evidence obtained is processed and analyzed to find things related. At this stage the goods with the case. There are some open source applications that can be used for the analysis phase. These applications must be installed in a computer investigator. Some devices are used based on open source operating system running on Linux. Besides some standard devices on the Linux operating system can also be used to perform the forensic analysis. UAT (USB Analisys Tool) is a solution offered. This device is a device based integrated Linux system and run without installing the system into the computer. This device uses a model of presistence disk. Presistence disk model is the means used to create a Linux-based operating system can run on USB flash drives. This model allows the operating system installed on a USB device flash drive can be developed as needed. In addition, the device also comes with UAT Luke encryption method to keep the data stored in the USB device remains secure. UAT resulting device features the Auto root login, Interactive menu, Global menu indicator, Calendar, these features may be easier for users to use this device. The results of tests carried out on 7 computers, devices UAT boot faster than booting Windows system, however tend to be slower than the Linux-based system installed on the hard drive. It can be affected by the process of data transfer through the USB interface which tends to be slower.

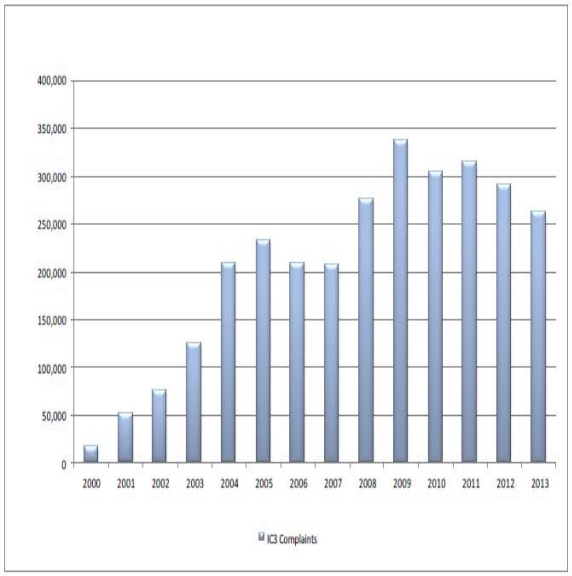
Keywords : Linux, USB, Flash Drive, Analysis.

1. LATAR BELAKANG

Perkembangan teknologi informasi memberikan imbas yang cukup signifikan pada dunia keamanan. Tindak kejahatan konvensional yang terjadi mulai memanfaatkan teknologi informasi sebagai alat bantu dalam melakukan tindak kejahatan. Penipuan merupakan kejahatan yang paling sering memanfaatkan adanya teknologi disamping kejahatan-kejahatan lain. Dengan memanfaatkan teknologi informasi tidak kriminal yang dilakukan terlihat lebih rapi, terstruktur dan lebih cepat. Selain itu dengan memanfaatkan teknologi informasi untuk melakukan tindak kejahatan, pelacakan pelaku dapat memakan waktu memanfaatkan teknologi informasi sebagai alat bantu, komponen teknologi informasi dapat dijadikan sebagai sasaran tindak kejahatan. *Cyber crime* merupakan istilah yang sering digunakan untuk merujuk kepada kejahatan yang memanfaatkan teknologi informasi. Gambar 1. menunjukkan perkembangan *Cyber Crime*.

Ilmu forensika digital muncul sebagai solusi untuk memecahkan kejahatan yang memanfaatkan teknologi informasi sebagai alat bantu, sasaran, maupun tempat kejadian. Ilmu forensika digital mempelajari berbagai hal untuk pemecahan kasus kejahatan yang memanfaatkan teknologi informasi atau lebih sering disebut dengan investigasi. Dalam melakukan investigasi terhadap suatu kasus, terdapat tahapan-tahapan yang harus dilalui. Tahapan tersebut antara lain :

1. Penjagaan (*Preservation*).
2. Pengambilan (*Acquisition*).
3. Analisi (*Analisys*).
4. Pelaporan (*Reporting*).
5. Presentasi (*Presentation*).



Gambar 1. *Internet Crime Complaint*. www. ic3. gov

Analisis merupakan tahapan inti dari pemecahan kasus kejahatan komputer. Pada tahap ini barang bukti yang didapat di proses dan dianalisa untuk menemukan hal-hal yang terkait dengan kasus yang terjadi. Terdapat beberapa aplikasi yang bersifat *open source* yang dapat digunakan untuk tahap analisis. Aplikasi-aplikasi tersebut harus dipasang kedalam komputer penyidik. Beberapa perangkat yang digunakan berbasis *open source* berjalan pada sistem operasi *Linux*. Selain itu beberapa perangkat standar pada sistem operasi *Linux* juga dapat dimanfaatkan untuk melakukan proses analisis forensik. Permasalahan muncul ketika penyidik hanya memiliki 1 sistem operasi dan bukan dari keluarga *Linux* pada komputer yang mereka miliki sehingga tidak dapat memanfaatkan perangkat yang berjalan pada *platform Linux*. Selain itu permasalahan muncul karena tidak semua penyidik terbiasa menggunakan sistem berbasis *Linux*.

Munculnya beberapa permasalahan diatas, maka perlu diberikan sebuah solusi. Perlu dibuat sebuah perangkat yang menjalankan sistem operasi *Linux* dan berisi perangkat-perangkat forensik yang bersifat *open source*. Dan juga ditambahkan beberapa fitur seperti menu untuk memudah kan investigasi yang kurang familiar dengan penggunaan perangkat *open source*. UAT (*USB Analisys Tool*) merupakan solusi yang ditawarkan. Perangkat ini merupakan perangkat terpadu berbasis sistem Linux dan dijalankan tanpa harus memasang sistem ke dalam komputer. Selain itu sistem UAT merupakan sistem yang berdiri sendiri, UAT hanya meminjam sumber daya komputer seperti memori, prosesor, dan lain-lain, kecuali *harddisk*. Sehingga penyidik tidak perlu khawatir akan kerusakan maupun kehilangan data pada komputer yang mereka gunakan.

1.1. Forensik Digital

Forensika digital semerupakan aplikasi ilmu pengetahuan dan teknologi komputer untuk melakukan pemeriksaan dan analisa terhadap barang bukti elektronik dan barang bukti digital dalam melihat keterkaitannya dengan kejahatan Selain itu terdapat juga pengertian dari *EC-Council* forensika digital merupakan aplikasi ilmu komputer untuk pencarian kepastian hukum bagi perbuatan kriminal dan sejenisnya. Pada ilmu forensika digital terdapat prinsip-prinsip dasar. Terdapat beberapa prinsip dasar yang dapat digunakan untuk melakukan investigasi forensik. Prinsip dasar dari merupakan prinsip yang banyak digunakan, prinsip dasar tersebut antara lain:

1. Sebuah lembaga hukum dan atau petugasnya dilarang mengubah data digital yang tersimpan dalam media penyimpanan yang selanjutnya akan dibawa ke pengadilan.
2. Seseorang yang merasa perlu mengakses data digital yang tersimpan dalam barang bukti berupa media penyimpanan, maka orang tersebut harus memiliki kejelasan dalam hal kompetensi, relevansi, dan implikasi dari tindakan yang dilakukan terhadap barang bukti.
3. Terdapat catatan teknis dan praktis mengenai langkah-langkah yang dilakukan terhadap barang bukti berupa media penyimpanan selama proses

pemeriksaan dan analisa berlangsung. Jika terdapat pihak ketiga yang melakukan investigasi terhadap media penyimpanan tersebut akan mendapatkan hasil yang sama.

4. *Person in charge* (PIC) pada proses investigasi memiliki seluruh tanggung jawab dari keseluruhan proses pemeriksaan dan juga analisis dan dapat memastikan bahwa keseluruhan proses berlangsung sesuai dengan hukum yang berlaku.

1.2. *Framework* Forensik

Menurut Al Azhar *framework* forensik meliputi:

1. Persiapan.
   Persiapan merupakan tahapan awal dari proses investigasi. Pada tahap ini dipersiapkan segala kebutuhan untuk melakukan proses investigasi. Kebutuhan peralatan baik perangkat keras maupun perangkat lunak dipersiapkan untuk mendukung kelancaran proses investigasi.
2. Administrasi penerimaan.
   Pada tahapan ini bukti elektronik yang masuk ke laboratorium diterima dan di dokumentasikan oleh pihak laboratorium. Semua barang bukti yang masuk harus dicatan pada formulir yang tersedia.
3. Akuisisi.
   Akuisisi barang bukti merupakan tahap dimana barang bukti digital diambil dari barang bukti elektronik. *Imaging* merupakan salah satu istilah yang digunakan pada tahapan akuisisi. *Imaging* dilakukan dengan metode *bit by bit copy*, yaitu proses penggandaan media penyimpanan 1 : 1. Media penyimpanan hasil *imaging* ini sama persis dengan media penyimpanan aslinya.
4. Pemeriksaan.
   Tahap pemeriksaan merupakan tahapan pemeriksaan secara koprehensif terhadap barang bukti digital sehingga analis forensik mendapatkan gambaran fakta-fakta tentang kasus yang sedang ditangani.
5. Analisis.
   Merupakan tahapan pemeriksaan secara lebih mendetail dari fakta-fakta yang didapatkan pada proses pemeriksaan. Analisis ini bertujuan untuk membuktikan kejahatan yang terjadi dan kaitannya dengan pelaku.
6. Laporan hasil investigasi.
   Laporan hasil investigasi merupakan bentuk tertulis dari keseluruhan proses analisis yang dilakukan dan juga berisi temuan-temuan dari proses analisis sesuai dengan aturan penulisan laporan hasil investigasi. Laporan yang dibuat harus dapat dipahami oleh pihak-pihak terkait seperti Hakim, Jaksa, dan lain-lain.

2. METODE PENELITIAN

USB Analisys tools merupakan sebuah alat yang dapat digunakan untuk melakukan analisis forensika digital. Untuk melakukan pembangunan perangkat ini, literatur didapatkan dari sumber buku, *paper*, thesis maupun halaman *web* yang berkaitan dengan forensika digital dan juga dokumen-dokumen mengenai aplikasi-aplikasi yang dipasang pada sistem UAT. Selain itu sistematika pada pembuatan menu mengacu *framework-framework* forensik yang sudah ada sebelumnya.

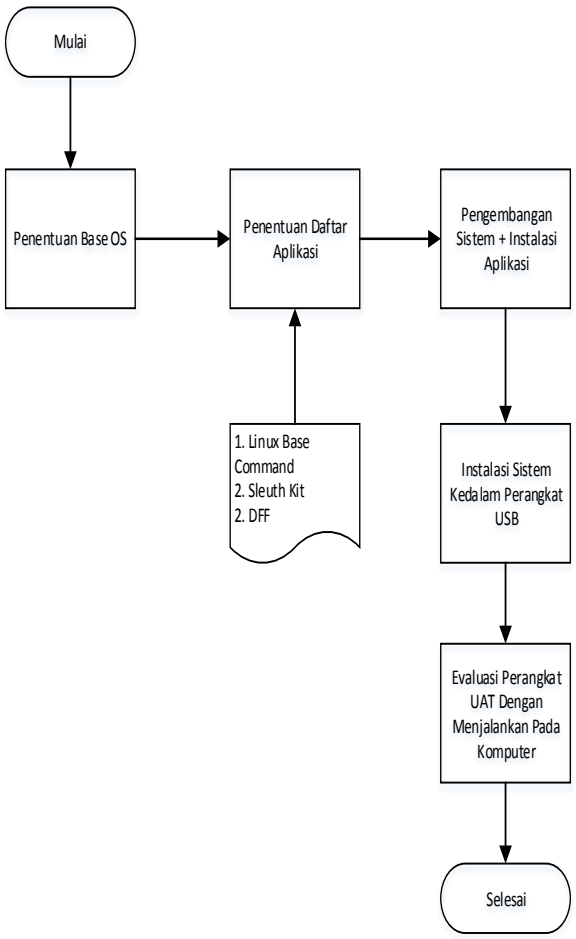
2.1. Analisis Permasalahan

Langkah-langkah yang dilakukan untuk menganalisa rumusan masalah yang dibuat sebelumnya antara lain adalah sebagain berikut:

1. Menentukan *base* sistem operasi yang akan digunakan untuk kepentingan pembuatan sistem.
2. Menentukan aplikasi apa saja yang akan dimasukkan ke dalam sistem operasi yang dibuat.
3. Melakukan pembangunan ulang sistem operasi dengan aplikasi-aplikasi yang sudah dipersiapkan sebelumnya.

4. Melakukan instalasi sistem operasi kedalam perangkat keras *flash drive* secara *persistence.*
5. Melakukan evaluasi terhadap sistem yang sudah dibuat.

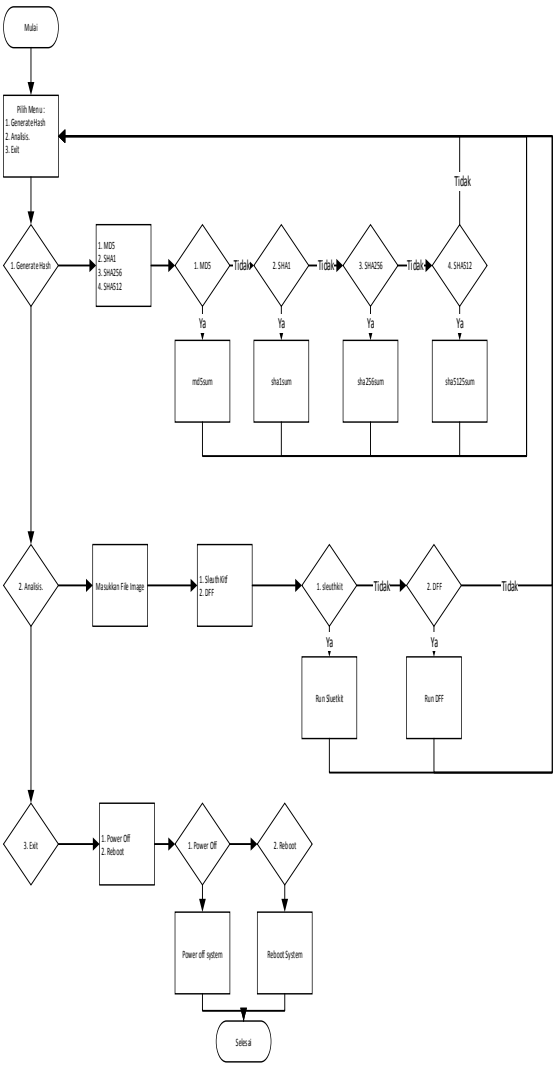
Langkah-langkah untuk penyelesaian permasalahan tersebut dapat dilihat pada Gambar 2.



Gambar 2. Alur Penyelesaian Masalah.

2.2. Pengembangan

Proses pengembangan sistem operasi dilakukan dengan mengembangkan sistem yang sudah ada dalam Kali *Linux* Mini dengan menambahkan paket-paket yang diperlukan. Pada dasarnya Kali Linux Mini merupakan sistem minimum dari Kali Linux. Didalamnya belum berisi paket-paket aplikasi, *driver*, *desktop environtment*, *service*, dan lain-lain seperti pada OS umumnya. Pengembangan dilakukan dengan melakukan instalasi perangkat *sleuthkit* dan DFF pada sistem operasi tersebut dan memberikan menu yang memudahkan penyidik untuk melakukan analisis. Adapun alur menu yang dibuat seperti Gambar 3. dibawah ini.



Gambar 3. Diagram Alir Menu Pada UAT.

3. HASIL DAN PEMBAHASAN

Base system yang dipilih merupakan sistem dengan basis Debian, hal ini dilakukan dikarenakan kemudahan dalam pengembangan sistem dan juga dukungan repositori yang lengkap. Kali *Linux* mini *distribution* merupakan salah satu sistem berbasis Debian yang memiliki ukuran kecil

dan sangat mudah dikembangkan sesuai dengan kebutuhan. Pengguna harus melakukan konfigurasi *file* secara mandiri ketika menggunakan kali *linux* versi mini ini.

3.1. Pengembangan Perangkat

Paket yang di kembangkan dalam *USB analisys tools* merupakan paket yang sudah terdapat di repositori dikembangkan agar mudah dalam menggunakan aplikasi-aplikasi tersebut sehingga dapat membantu penyidik yang belum familiar dalam melakukan investigasi dengan lingkungan berbasis *Linux*. Tabel 1 dibawah ini merupakan daftar aplikasi yang terpasang pada perangkat UAT berdasarkan beberapa kategori aplikasi.

Tabel 1. Daftar Aplikasi Pada UAT *Analisys*

Kategori	Aplikasi
Utility	• *Calculator* • *Dictionary* • *Connect to Server* • *Florence Virtual Keyboard* • *Gedit* • *Iceweasel* • VLC • Terminal
Hashing	• Md5sum • Md5deep • Sha1sum • Sha1deep
Disk Forensic	• Autopsy • DFF • Ghex
Data *Recovery*	• Foremost • *Testdisk*
Password Tools	• *John The Ripper* • Hydra
RAM Forensic	• Volatility
Network Forensic	• *Nmap* • *Wireshark* • *Pasco* • *Httrack*
Reverse Engineering	• *Lynis* • *Ollydbg*
Documentation	• *Keepnote* • *Maltego*

3.2. Pengembangan USB Presistence

Model *presistence disk* merupakan cara yang digunakan untuk membuat sistem operasi berbasis *linux* dapat dijalankan di perangkat *USB flash drive*. Model ini memungkinkan sistem operasi yang terpasang pada perangkat *USB flash drive* dapat dikembangkan sesuai kebutuhan. *Install* dan *Uninstall* merupakan hal yang dapat dilakukan pada perangkat dengan model ini.

Perangkat UAT ini juga dilengkapi dengan metode enkripsi *Luke*. Enkripsi dilakukan agar data yang disimpan didalam nya dapat terjaga dengan aman. Pada 1 buah *USB flash drive* akan dilakukan pembagian menjadi 2 buah partisi. 1 partisi digunakan untuk menyimpan sistem operasi dan 1 partisi digunakan untuk menginpan data *persistence* dengan enkripsi *Luke*.

Perangkat UAT yang dibuat merupakan perangkat yang di khususkan untuk melakukan analisis forensik pada barang bukti digital yang sudah dilakukan proses akuisisi sebelumnya. Seperti nama nya perangkat ini berbasis perangkat *USB flash drive* seperti terlihat pada Gambar 4.

Antarmuka aplikasi dibuat agar pengguna perangkat ini mudah untuk menggunakan. Adapun pengembangan yang dilakukan di sisi aplikasi perangkat UAT adalah sebagai beriku:

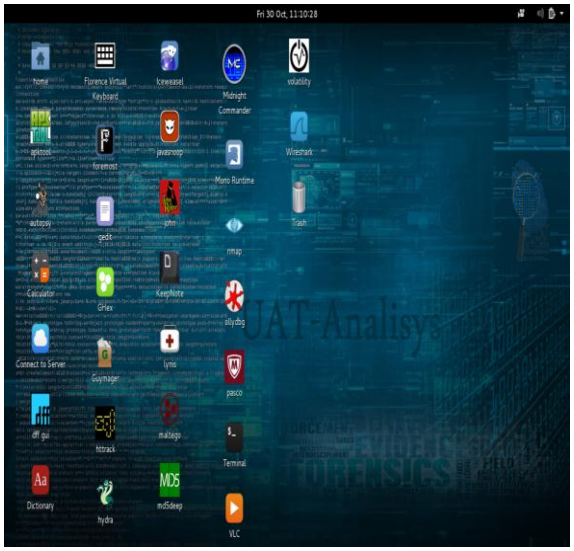
1. *Auto root login*.
2. *Interactive menu*.
3. *Global menu indicator*.
4. *Calendar*.

Gambar 4. Perangkat *USB* UAT.

3.3. *USB Analisys Tools*

Terdapat 2 tahapan dalam proses pengembangan aplikasi pada perangkat UAT. Tahap pertama merupakan pengembangan *bootloader* GRUB (*Grand Unified Bootloader*) yang betujuan untuk memudahkan pengguna dalam memilih sistem operasi dan tahap kedua merupakan pengembangan aplikasi-aplikasi untuk kebutuhan forensik yang akan dipasang pada perangkat UAT *analisys*.

Hasil dari pengembangan yang dilakukan pada tahap pengembangan makan akan menghasilkan perangkat UAT analisys. Bentuk *flash drive* yang dipilih adalah *flash drive* yang berukuran kecil sehingga dapat dengan mudah dibawa, dan *flash drive* yang memiliki kecepatan baca dan tulis cukup tinggi sehingga dapat mempercepat proses *booting*. Adapun antarmuka dari sistem operasi yang terpasang pada perangkat UAT dapat dilihat pada



Gambar 5. Tampilan Antarmuka UAT *Analisys*.

3.4. Evaluasi

Dari hasil yang telah didapat dilakukan evaluasi dengan menguji *USB Analisys Tools* pada 5 perangkat komputer PC dan 2 perangkat komputer laptop. Adapun rincian perangkat yang digunakan untuk melakukan pengujian ditunjukkan pada Tabel 2.

Tabel 2. Tabel Spesifikasi Komputer Sampel

No	Nama Perangkat	Spesifikasi		
1	Komputer 1	CPU RAM USB Port	: : :	AMDPhenom II X4 955 (3,2 Ghz) 4096 MB USB2. 0
2	Komputer 2	CPU RAM USB Port	: : :	AMDPhenom II X4 955 (3,2 Ghz) 4096 MB USB2. 0
3	Komputer 3	CPU RAM USB Port	: : :	Intel Core(2)Duo E7500 (2,93) 2048 MB USB2. 0
4	Komputer 4	CPU RAM USB Port	: : :	AMDPhenom II X4 955 (3,2 Ghz) 4096 MB USB2. 0
5	Komputer 5	CPU RAM USB Port	: : :	AMDPhenom II X4 955 (3,2 Ghz) 4096 MB USB2. 0
6	Laptop 1	CPU RAM USB Port	: : :	Intel Core i7-3610QM (2,3 Ghz) 4096 MB USB3. 0
7	Laptop 2	CPU RAM USB Port	: : :	AMDPhenom II X4 955 (3,2 Ghz) 4096 MB USB2. 0

Hasil pengujian berbentuk waktu rata-rata *booting* proses ketika menjalankan perangkat UAT *analisys*. Dari hasil evaluasi perangkat UAT memiliki kecepatan *booting* rata-rata 65,4 detik lebih lambat dari pada sistem operasi linux yang terpasang pada harddisk, seperti terlihat pada tabel 3. Hal ini dapat dipengaruhi oleh proses transfer data melaui antarmuka *USB* yang cenderung lebih lambat.

Tabel 3. Hasil penghitungan waktu

Waktu Booting	Perangkat							Rata-rata
	Komputer 1	Komputer 2	Komputer 3	Komputer 4	Komputer 5	Laptop 1	Laptop 2	
Linux	49.6	45.1	.	.	48.7	66.5	.	52.475
Windows	108.4	86.6	89.9	90	88.6	119.7	96.4	97.08571
UAT	65.9	71.1	61	64.9	62.3	69.4	63	65.37143

4. KESIMPULAN DAN SARAN

4.1. Kesimpulan

Berdasarkan hasil pembahasan yang sudah ada pada bab sebelumnya, maka dapat ditarik beberapa kesimpulan sebagai berikut :

1. Perangkat UAT melakukan *booting* lebih cepat dibandingkan dengan *booting* sistem Windows namun cenderung lebih lambat dibandingkan dengan sistem berbasis *Linux* yang terpasang pada *harddisk*.
2. Pengembangan aplikasi diperlukan waktu yang cukup banyak, dikarenakan sistem Kali *Linux* Mini memerlukan koneksi internet dalam melakukan proses pengembangan.
3. Diperlukan waktu untuk memasukkan sandi enkripsi ketika proses *booting*.

4.2. Saran

4.2.1. Penelitian Lanjutan

Berdasarkan kesimpulan tersebut diatas maka terdapat beberapa saran untuk pengenmbangan perangkat ini kedepannya. Adapun saran yang dapat diberikan antara lain:

1. Pengembangan aplikasi agar dapat di paasang pada perangkat berbasis ARM *processor*.
2. Pengembangan perangkat forensik berbasis perangkat keras yang berukuran kecil sehingga dapat mudah dibawa, seperti layaknya perangkat *USB* UAT.

UCAPAN TERIMA KASIH

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

DAFTAR PUSTAKA

ACPO & 7safe, “Good Practice Guide for Computer-Based Electronic Evidence,” 2008.

ECCouncil, “CHFI v8 Module 01 Computer Forensics in Today’s World. pdf. ” ECCouncil, Albuquerque, 2012.

ECCouncil, “CHFI v8 Module 21 Investigative Reports. pdf.” ECCouncil, Albuquerque, 2012.

M. N. Al-Azhar, *Digital Forensic Panduan Praktis Investigasi Komputer*, Edisi Pert. Jakarta: Salemba Infotek, 2012.

O. Security, “Kali Linux Live USB Persistence | Kali Linux Official Documentation,” 2014. [Online]. Available : http://docs. kali. org/installation/kali-linux-live-usb-persistence. [. Accessed: 30-Oct-2014]

O. Security, “Kali Linux Official Documentation,” 2014.

www. ic3. gov, “www. ic3. gov,” 2013.