PENGEMBANGAN UJI DATA DIGITAL PADA WEBSITE DENGAN DIGITAL FORENSICS

Asep Budiman Kusdinar
Program Studi Teknik Informatika, Fakultas Sains dan Teknologi,
Universitas Muhammadiyah Sukabumi
Jln. R Syamsudin SH No. 50 Kota Sukabumi, Jawa Barat 43113
Email: asep.budiman.k@gmail.com, abkus@live.com

Abstract

Testing development of data digital is processing the whole of important information is stored in digital of website. This study in order to give understanding of data digital was a specification stored in website. The using method is a digital forensic. The focus of this methods are used to provide direct identification and understanding of information the data digital will be proved. To smooth the use of testing that included also forensic software. This Developing tested can be hoped to complete information, such as: the action of what is being done at the time of website attacked, any application that is installed, how the website and network systems configured, How to restore the files that have been missing, and finally, how to collect the returned information is missing. This testing Results was collected for using as occurring data digital legality or illegal, so that key questions such as: who, what, when, how, where and why can be answered scientifically.

Keywords: Testing, Development, Data Digital, Digital Forensics, Website.

Pendahuluan

Latar Belakang

Teknologi Komputer secara fisik *(hardware)* maupun non fisik *(software)* merupakan dua teknologi yang tidak terpisahkan satu sama lain. *Hardware* merupakan sarana fisik kebutuhan penyimpanan seluruh informasi elektronik sedangkan *software* merupakan sarana bukan fisik untuk melakukan interaksi, komunikasi, manipulasi, dan transaksi data antara Personal dengan Komputer baik secara individu maupun secara bersama melalui jalur digital. Sedangkan teknologi informasi merupakan gabungan dari kedua teknologi tersebut yaitu teknologi komputer dan teknologi komunikasi atau secara umum disebut sebagai teknologi informasi dan komunikasi. Dilihat dari sisi perangkat keras dan teknologi komunikasi, komputer dikelola selain oleh sistem operasi juga perangkat lunak aplikasi yang khusus mengelola perangkat keras dan jaringan komunikasi yang sesuai dengan kebutuhannya masing-masing. Sedangkan secara perangkat lunak, komputer dikelola oleh perangkat lunak sistem *(system software)* dan perangkat lunak aplikasi *(aplication software)* sebagai sarana untuk mengakomodasi semua kebutuhan-kebutuhan informasi tersebut. Dari kedua teknologi tersebut pasti ada kelemahan yang biasanya terjadi akibat dari tingkat kompleksitas pembuatan teknologi tersebut sangat rumit. Hal ini menjadi peluang bagi pelaku kejahatan untuk memanfaatkan kerawanan kedua sistem tersebut.

Kriminalitas yang biasanya sering dilakukan pada Dunia digital, selalu diikuti dengan perkembangan teknologi yang diadopsinya. Perkembangan kebutuhan dalam Dunia digital akan meningkatkan kebutuhan positif maupun negatif secara langsung ataupun tidak langsung terhadap bidang usaha, maka disitulah potensi kriminalitas bisa terjadi kapan saja tanpa diketahui. Perkembangan kriminalitas saat ini sudah merasuk ke Dunia digital dan jalur kemunikasi khususnya website. *Website* merupakan tempat para pelaku kejahatan untuk melakukan penetrasi dengan berbagai cara dan tujuan yang berbeda. Tujuannya ada yang memang untuk menguji keamanan situs tersebut dan sebaliknya ada pula yang hanya ingin popularitas, mencoba-coba, merusak, dan mengambil informasi untuk kepentingan tertentu.

Pada kondisi seperti itu, perlu proses pengujian data digital terhadap website yang telah dipenetrasi walaupun sangat menyulitkan. Penyusup biasanya secara kontinu menyimpan dan menyembunyikan kode-kode berbahaya *(malicious code)*, menghapus, ataupun memodifikasi *file log*, dan mencari teknologi baru untuk menghilangkan jejak yang mereka tinggalkan. Teknik yang mereka gunakan untuk memasuki sistem target adalah *DDoS, Spoofing, Social Engineering, BotNet, Spyware*, dan *SQL Injection* dengan berbagai turunannya. Jika dilihat dari teknik kejahatannya dapat dikelompokkan kedalam dua jenis yaitu kejahatan sistem organisasi atau konfigurasi atau sistem file atau basis data dari teknologi sistem Komputer *(Computer froud)* dan kejahatan menggunakan media digital dalam melakukan pelanggaran hukum *(Computer as a Tool). Computer froud* seperti: *abuse, cracking, hacking, carding, stealing*, dan lain sebagainya merupakan kejahatan yang paling populer. Sedangkan C*omputer as a Tool* biasanya digabungkan dengan media digital lainnya seperti: *mobile, wireless, bluetooth,* dan lain sebagainya untuk melakukan kejahatan. Dibalik perlakuan kriminalitas tersebut, semua informasi positif maupun negatif disimpan dalan sistem komputer khususnya *website* walaupun penyimpanan informasi tersebut tidak semua ditampilkan di bagian paling depan *(front end)*. *Website* inilah yang menjadi fokus dalam penelitian ini sebab proses uji data digital pada bagian ini bisa dilakukan secara jelas tempat dan kejadian perkaranya sehingga dapat dibuktikan di lapangan dan di laboratorium. Oleh karena itu, penelitian ini dapat digunakan untuk membantu menganalisis, menguji, dan membuktikan *data digital* yang tersimpan di dalam *website* baik secara legal maupun ilegal untuk diuji, dilacak, diungkap, dan dibuktikan secara ilmiah.

Permasalahan

Maraknya kriminalitas pada dunia digital. Tujuannya diantaranya untuk menguji keamanan situs tersebut, ada pula yang hanya ingin popularitas, mencoba-coba, merusak, dan mengambil informasi untuk kepentingan tertentu dari data yang disimpan dalam sistem komputer khususnya *website.* Sulitnya melacak pelaku, sehingga diperlukan proses pengujian data digital terhadap website yang telah dipenetrasi oleh *hacker*.

Tujuan Penulisan

Tujuan penulisan pada penelitian ini adalah melakukan pengembangan uji data digital dengan metode digital forensic

Landasan Teori

Pengujian merupakan proses pembuktian kebenaran data secara kuantitatif berdasarkan informasi akurat dan objektif dari awal sampai akhir untuk mencapai hasil yang diinginkan berdasarkan keputusan dan kesimpulan yang jelas.

Investigasi merupakan upaya penelitian, penyelidikan, pengusutan, pencarian, pemeriksaan, pengumpulan data, pengumpulan informasi, dan temuan lainnya untuk mengetahui, membuktikan kebenaran, atau bahkan kesalahan sebuah fakta yang kemudian menyajikan kesimpulan atas rangkaian temuan dan susunan kejadiannya.

Bukti Digital merupakan data yang disimpan dalam media, sistem Komputer, atau dalam perangkat lain yang sama, yang bisa dibaca, dan disimpan oleh seseorang, atau oleh sistem Komputer, atau oleh perangkat lain yang sama bisa berupa printout atau output data.

Digital Forensic merupakan salah satu cabang ilmu forensik yang berkaitan dengan bukti-bukti legal yang ditemui pada komputer dan media penyimpanan digital. Tujuan dari digital forensic adalah untuk menjabarkan keadaan terkini dari suatu artifak digital (seperti flash disk, hard disk, CD-ROM, printer, jaringan, mobile, dll), dokumen elektronik (misalnya sebuah pesan email atau gambar JPEG), atau bahkan sederetan paket yang berpindah dalam jaringan Komputer. Penjelasan bisa sekedar "ada informasi apa saja yang ada disini?" sampai serinci "apa urutan peristiwa yang menyebabkan terjadinya situasi terkini?".

Bukti-bukti Data Digital Buki-bukti pencarian data digital bisa ditemukan dari *extention file, log file, file dat, file sys,* dan *file-file* lainnya, termasuk tanggal dan waktu yang biasanya tertera dalam pembuatan *file,* dan *file-file* tersembunyi yang disimpan di lokasi *free spac*e, dan *unallocated space*.

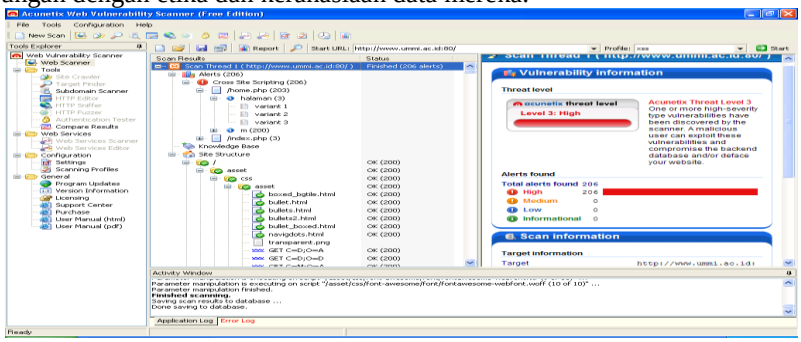
Metode Penelitian

Metode yang digunakan adalah *digital forensic* untuk pengujian dan pembuktian *data digital* yang mencakup analisis, proses dan teknik *digital forensic*. Pemahaman mengenai *digital forensic* secara filosofis dan teknis diuraikan secara singkat berikut ini berdasarkan definisi dan pemahaman yang ditulis oleh **Casey Eoghan (Eoghan, 2013)** dan **Stave Debora (Debora. 2013)**.

Hasil dan Pembahasan

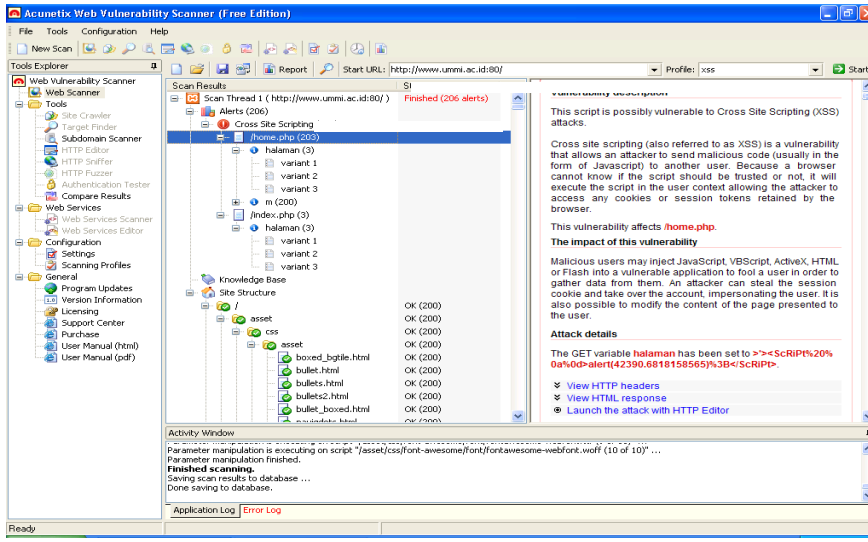
Hasil Uji Data Digital

Nama *Website* yang diuji tidak disebutkan. Selanjutya di beri nama “X” karena berhubungan dengan etika dan kerahasiaan data mereka.



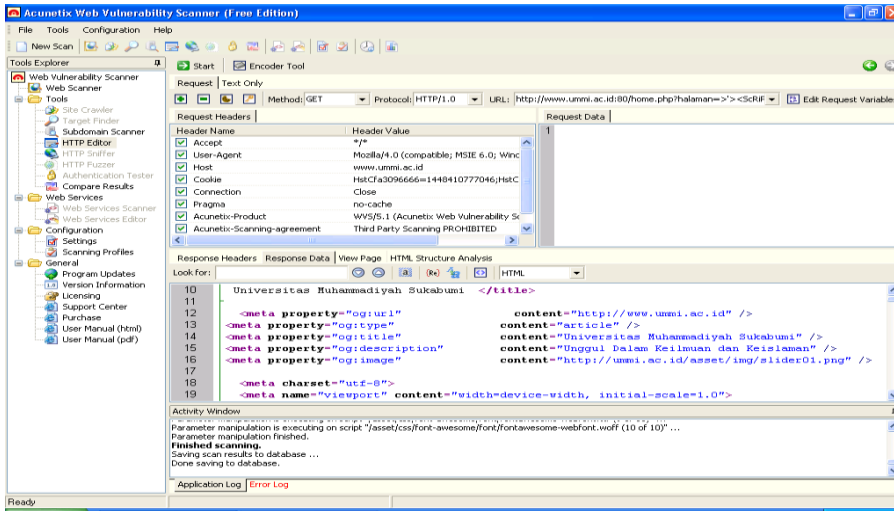
Gambar 1. Informasi Kerawanan Situs “X”

Pada penelitan ini melakukan pengujian sekaligus ingin mengetahui seberapa tangguh tingkat keamanan jaringan internet yang ada di situs tersebut. Pengujian ini dibantu juga dengan perangkat lunak forensik sekaligus keamanan jaringan.



Gambar 2. Informasi Peringatan Kerawanan Situs "X"

Pada gambar 1 dan 2 terlihat jelas bahwa situs "X" setelah diuji memiliki tingkat kerawanan yang sangat tinggi diposisi 3 (tiga) dengan jumlah berkas dan jalur data dapat dipenetrasi sebanyak 206 lubang keamanan. Ancaman keamanan tersebut berada di port 80 yang memang memakai gerbang standar. Selain port 80 ada juga halaman utama (home.php) yang bisa dimasuki penyusup dengan *script* yang diberi tanda warna merah.



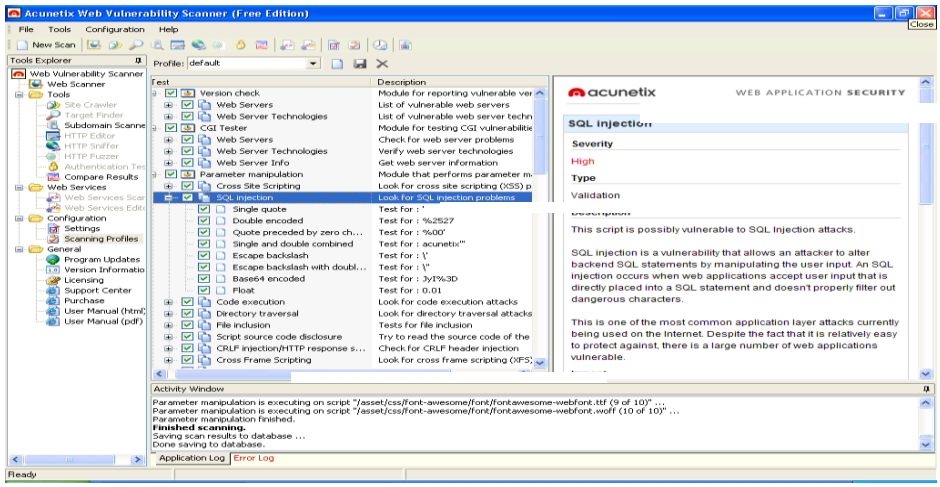
Gambar 3. Eksploitasi Terhadap Situs "X"

Uji data tersebut memakai *digital forensics request encoder tool*. Pada bagian ini terlihat jelas kerawanan situs tersebut berada diposisi script.html yang dapat

dimodifikasi langsung terhadap situs tersebut. Dari kerentanan tersebut dapat dilihat pada tabel 1 untuk kerawanan ancaman dan cara mengatasinya.

Tabel 1: Informasi Kerawanan

Ancaman (*Threat*)	**Bukti Informasi**
Tinggi (High)	Semua Pengguna bias masuk
Gerbang (Port)	80 (Standard).
Halaman	Home.php dan Index.php
Server	Apache32. http://..home.php



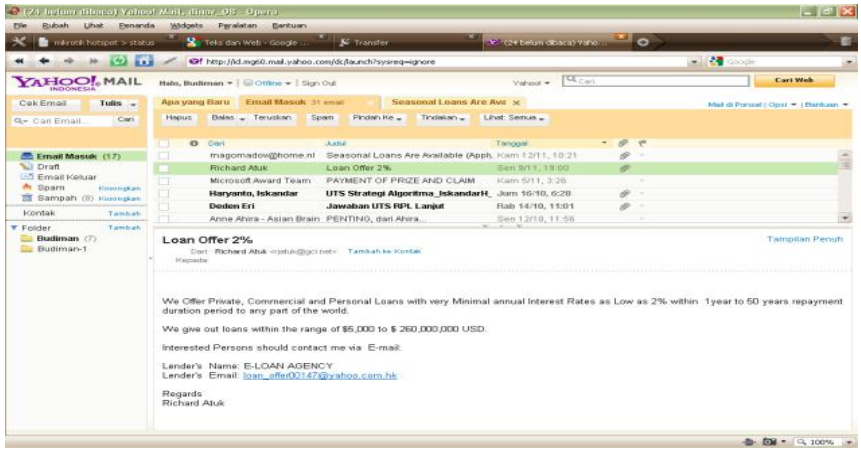
Gambar 4. Penetrasi SQL Injection

Berikutnya uji data dilakukan terhadap eksploitasi berkas dan basis data. Ternyata eksploitasi tersebut sangat mudah dilakukan oleh siapa pun sehingga terlihat di gambar 3 dan 4, selain *script html* yang bisa dipenetrasi juga basis data *MySQL* yang bisa diserang dengan menggunakan teknik *SQL Injection*. Dalam gambar 4, perangkat lunak memberi tahu bahwa bagian ini sangat riskan sekali apabila penyusup merubah dan menghapus data-data penting di situs tersebut. Informasi tersebut dapat dijelaskan dalam bentuk tabel 2 berikut ini.

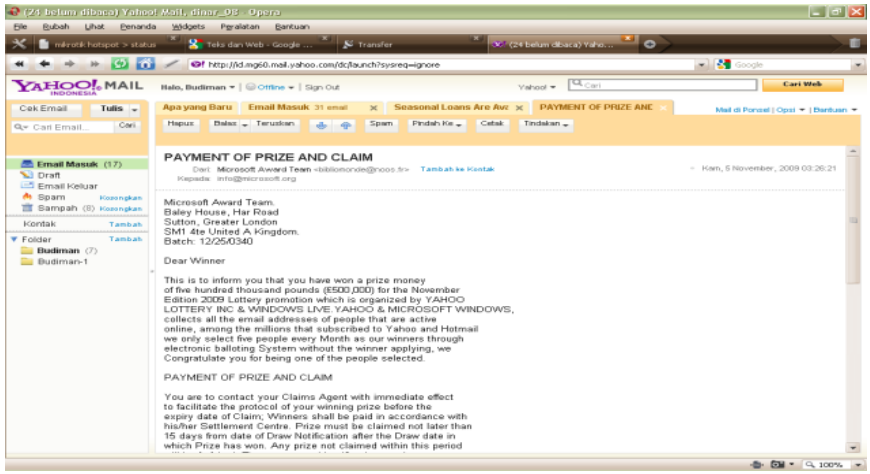
Tabel 2. Kerawanan SQL Injection

Ancaman (Threat)	**BUKTI INFORMASI**
Tinggi (High)	Penetrasi bisa dilakukan oleh siapa pun
Halaman Situs	Script.html (Utama)
Basis Data	MySQL ver.25.2.32. ext : 32 bit
Status	High

Pengujian dan investigasi pada bagian ini dilakukan pada surat elektronik (email) spam loan dan undian berhadiah dari Microsoft Team. Spam email ini sebagai sampel data. Oleh karena itu saya coba uji kembali di tempat kejadian perkara terhadap email pribadi saya di Laboratorium. Walaupun email sekarang sudah memblokir pesan spam.



Gambar 5. Email Spam Loan



Gambar 6. E-mail Spam Undian Berhadiah

Pengujian dan pembuktian pada ke dua kasus tersebut memakai dua cara yaitu: *log file* dan *IIS log*. Kedua cara itu instruksinya bisa dilakukan secara langsung di Komputer. Uji data digital ini bertujuan untuk mengetahui **siapa, apa, mengapa, kapan, dimana,** dan **bagaimana** proses terjadinya.

***Log File*:**

Received: from NIH2WAAF (id.mg60.yahoo.com [149.xxx.183.75])by Magomadov.com (8.8.3/8.6.9) with ESMTP id XAA20854 for <fplh@discuz.org>; Tue, 10 Nov 2016 10:07:01 GMT Received: from CISPPP - 199.xxx.193.176 by csi.com with Microsoft SMTPSVC; Mon, 09 Nov 2016 11:53:36 -0400 Message-Id:<2.2.16. 20090428082132.2cdf5 loan_offer147@yahoo.com.hk> X-Sender: E-Loan Agency X-Mailer: Windows Eudora Pro Version 2.2 16) Mime-Version: 1.0 Content-Type: text/plain; charset="us-ascii" To: dinar_08@yahoo.co.id From: "Richard Atuk" rjatuk@gci.net

Tabel 3. Uji Data e-Mail Dengan Log File

AKSI	BUKTI INFORMASI
Siapa	Richard Atuk sebagai pengirim
Apa	Menawarkan kredit (loan) keuangan.
Mengapa	Ingin mendapatkan keuntungan pribadi dari pengguna awam
Kapan	Tue, 10 Nov 2016 10:07:01 GMT
Dimana	NIH2WAAF (id.mg60.yahoo.com [149.xxx.183.75]) by Magomadov.com (8.8.3/8.6.9) with ESMTP id XAA20854…. (server situs yahoo.com dan magomadov.com dengan IP address berbeda serta nama identitas dienkripsi).
Bagaimana	Message-Id:<2.2.16.20090428082132.2cdf5 loan_offer147@yahoo.com.hk> X-Sender: E-Loan Agency X-Mailer: Windows Eudora Pro Version 2.2 (16) Mime-Version: 1.0….(proses pesan yang dikirim dienkripsi tujuannya agar tidak diketahui).

IIS Log:

219.88.67.33,-,10/11/2016,0:48:43,W3SVC1,webserver,x.x.x.x,15,72,4184,404, 123,GET,/<Rejected-By-UrlScan>,~/scripts/root.exe,219.88.67.33,- ,10/11/2015,0:48:49, 3SVC1,webserver,x.x.x.x,0,70,4184,404,123,GET,/<Rejected-By-UrlScan>,~/MSADC/root.exe, 219.88.67.33, -, 10/11/2016, 0:48:55, W3SVC1, webserver,x.x.x.x, 0, 80, 4184, 404, 123, GET, /<Rejected-By-UrlScan>,c/winnt/system32/cmd.exe,219.88.67.33,-,10/11/2016,0:49:01, W3SVC1,webserver,x.x.x.x,0,80,4184,404,123,GET,/<Rejected-By-UrlScan>,d/winnt/system32/cmd.exe,219.88.67.33,-,10/11/2016, 0:49:07, W3SVC1, webserver, x.x.x.x,0,96,4184,404,123,GET,/<Rejected-By UrlScan>,~/scripts/..%255c../winnt/system32/cmd.exe,219.88.67.33,- ,10/11/2016,0:49:13, W3SVC1,webserver,x.x.x.x,0,117,4184,404,123,GET,/<Rejected-By-UrlScan>, ~/_vti_bin/..%255c../..%255c../..%255c../winnt/system32/cmd.exe,2016-11-1013:00:19 66.166.205.246 - 66.166.77.164 80 GET /default.ida xx%u9090%u6858%ucbd3%u7801%u9090%u6858%ucbd3%u7801%u9090%u6858%ucbd3%u7801%u9090%u9090%u8190%u00c3%u0003%u8b00%u531b%u53ff %u0078%u0000%u00=a200

Tabel 4. Uji Data e-Mail Dengan IIS Log

AKSI	BUKTI INFORMASI
Siapa	Atas nama Microsoft Team (identitas disembunyikan).
Apa	Mencari korban untuk kepentingan pribadi .
Mengapa	Mendapatkan keuntungan dari pribadi-pribadi yang awam lewat internet.
Kapan	Tgl. 10/11/2016. Jam 00:48:43, 00:48:49,…
Dimana	Di server dengan IP address 219.88.67.33 dengan webserver yang berbeda-beda (rejected).
Bagaimana	Informasi penting disembunyikan dengan enkripsi (u6858%ucbd3%u7801%u….) dst.

Simpulan

Pengembangan uji data digital dengan metode digital forensic ini dapat membuktikan kebenaran data digital secara hampir sempurna sehingga dapat dimanfaatkan untuk:

1. Uji, lacak, ungkap, dan pembuktian penggunaan data atau *file* digital terhadap jaringan Komputer dan *website*.
2. Utilitas uji data digital untuk pembuktian terhadap jaringan Komputer dan website apabila terjadi penetrasi ilegal ataupun untuk kepentingan penyelidikan oleh pihak intelejen untuk kebutuhan tertentu. Utilitas kebutuhan itu berupa *undelete file*, *recovery fil*e, *unformat*, *disk image* atau *disk cloning*, c*hecksum image*, *delete file*, *located file*, *unalocated file*, dan *slack space*, hak akses, URL, dan Basis Data. Sehingga dapat dibuktikan secara ilmiah.

Daftar Pustaka

Casey Eoghan, *Handbook of Computer Crime Investigation.* 20013. Academic Press; 4st edition. Prentice Hall. USA.

Casey Eoghan. *Digital Evidence and Computer Crime*. 2014. Academic Press. 2st edition. Prentice Hall. USA

David Solomon A. and Russinovich Mark E, *Inside Microsoft® Windows®*. 2014, Third Edition Microsoft Press, Redmond, Washington. USA.

M. Alazab. *Effective Digital Forensic Analysis of The NTFS Disk Image*. 2011. University of Ballarat. Autralia. Vol. 20(4):30-70.

Steve Debrota. *Computer Forensics Field Triage Process Model*. 2013. U.S. Attorney Office. Southern Indiana. Vol. 60(10):208-220.

Stephen K. Brannon. *Digital Forensic Analysis Methodology*. 2008. Department of Justice United State. Wasington DC. USA. Vol. 10(5). ch:4-6. pp:20-40.