ANALISIS *DATA RECOVERY* MENGGUNAKAN *SOFTWARE FORENSIC*: WINHEX AND X-WAYS FORENSIC

Vidila Rosalina[1] , Andri Suhendarsah[2,] M. Natsir[3]
FTI Universitas Serang Raya Jl. Raya Serang-Cilegon Taman Kopasus
[1)]vidila.suhendarsah@gmail.com, [2)]andris@lottechem.com[3)]natsir.Singa@gmail.com

Abstrak - Segala bentuk kejahatan baik di dunia nyata maupun di dunia maya, sering meninggalkan jejak yang tersembunyi ataupun terlihat. Jejak tersebut yang kemudian dapat meningkat statusnya menjadi bukti, menjadi salah satu perangkat/entitas hukum.Data recovery merupakan bagian dari analisa forensik di mana hal ini merupakan komponen penting di dalam mengetahui apa yang telah terjadi, rekaman data, korespondensi, dan petunjuk lannya. Banyak orang tidak menggunakan informasi yang berasal dari data recovery karena dianggap tidak murni/asli/orisinil. Setiap sistem operasi bekerja dalam arah yang unik, berbeda satu sama lain (walaupun berplatform sistem operasi yang sama). Untuk melihat seberapa jauh data sudah dihapus atau belum, perlu memperhatikan segala sesuatu yang ada dalam raw disk. Jika data yang digunakan untuk kejahatan ternyata masih ada, maka cara yang termudah adalah menguji data dengan pemanfaatan tool yang ada pada standar UNIX, seperti strings, grep, text pagers, dan sebagainya. Sayangnya, tools yang ada tidak menunjukkan data tersebut dialokasikan di mana.Artikel ini akan membahas software forensic: winhex and x-ways forensic yang dapat melakukan data recovery dengan lebih sempurna.

Kata Kunci: *Data Recovery, Digital Forensic, Wihex, X-Way Forensic*

I. PENDAHULUAN

Dengan dibentuknya Asosiasi Forensik Digital Indonesia (AFDI) oleh Kementrian Komunikasi dan Informatika pada tanggal 17 November 2015 yang lalu hal ini membuktikan bahwa Digital Forensik merupakan bidang ilmu baru dalam dunia komputer yang berkembang pesat akhir-akhir ini dengan makin maraknya kejahatan di bidang komputer serta semakin banyaknya buku-buku yang mengupas mengenai digital forensik, sehingga semakin menambah refrensi pengetahuan bagi peneliti-peneliti muda. Dengan lahirnya Undang-undang Informasi Transaksi Elektronik nomor 11 Tahun 2008, maka semakin membuat bidang ilmu ini menjadi perangkat wajib untuk membongkar kejahatan yang melibatkan dunia komputer, karena pada umumnya kejahatan komputer ini meninggalkan jejak digital, maka perlu adanya seorang ahli komputer forensik yang akan mengamankan barang bukti digital atau biasa disebut digital evidence. Komputer Forensik tentu memerlukan suatu standart operational procedure (SOP) dalam mengambil bukti-bukti digital agar tidak terkontaminasi pada saat data di ambil dari digital evidence sehingga sangat memudahkan para ahli komputer forensik untuk melakukan pemulihan sistem pasca kerusakan (Rosalina, 2015).

Konsep Awal Pada kondisi sebenarnya, dalam proses delete itu tidak menghapus data secara permanen dari media penyimpanan (disk, dsb), tapi memberitahukan kepada komputer bahwa ruang yang ditempati data tersebut tersedia untuk ditimpa/diisi/di-overwrite oleh data yang lain. File ini dapat dengan mudah dikembalikan ke bentuk semula, bila belum tertimpa file lain dengan menggunakan Norton Utility atau Lost & Found dari PowerQuest. Pada Windows 9x/NT bahkan disediakan Recycle Bin sehinnga dapat mengembalikan file yang secara tidak sengaja terhapus. Kapasitas penyimpanan (harddisk) yang semakin besar saat ini, memungkinkan orang untuk menggunakan seluruh ruang harddisk, dan overwrite hanya dilakukan ketika melakukan proses format. Sekalipun file dihapus, potongan-potongan file tersebut masih selamat/tersimpan. Jika sebuah dokumen berada pada disk dalam bentuk yang di-compress, maka dokumen tersebut tetap dalam bentuk ter-compress saat dihapus, dengan demikian pencarian di disk untuk sebuah kata kunci yang hanya ada di dalam file yang dihapus tidak akan membuahkan hasil. File yang sedikit terfragmentasi (terpecah-pecah) akan lebih memudahkan untuk dipulihkan / di-recover, tetapi penempatan file system yang baik memiliki lebih banyak manfaat, antara lain memungkinkan informasi yang terhapus dapat bertahan lebih lama daripada yang kita duga. Dengan semakin berkembangnya sistem enkripsi, seorang penyusup selalu berusaha untuk mendapatkan berbagai informasi, dimanapun dan bagaimanapun bentuk informasi tersebut, bahkan walaupun informasi tersebut sudah dihilangkan. Dengan menggunakan peralatan canggih seperti magnetic force microscopy (MFM) informasi yang berbentuk file yang disimpan pada media magnetic dan telah dihapus serta ditimpa berulang kali dapat diperoleh kembali. Agar dapat menghapus file dan tidak dapat dikembalikan lagi terutama penghapusan yang aman pada media magnetik, dikenal meetoda lama yang dikenal dengan metoda standar DoD (Department of Defense). Metoda DoD ini adalah dengan menimpa data dengan sebuah pola kemudian ditimpa lagi dengan komplemen pola pertama dan ketiga ditimpa lagi dengan pola lain. Misalnya sebuah data ditimpa oleh pola 1 (satu) semua, kemudian ditimpa oleh komplemennya yaitu 0 (nol) semua dan terakhir dengan pola 10 (satu nol). Tetapi Bruce Schneier menyarankan menghapus file sebanyak tujuh kali. Pertama dengan pola 1 (satu) kemudian dengan pola 0 (nol) sebanyak lima kali dan terakhir dengan pola pseudo-random yang aman secara kriptografi. Tetapi cara ini pun tidak aman setelah dikembangkannya electron-tunneling microscopes. Cara penghapusan

yang aman pada media magnetik adalah seperti yang dikembangkan oleh Peter Gutmann dari Universitas Auckland. Pada metoda ini Peter Gutmann mengembangkan pola tertentu yang disesuaikan dengan cara pengkodean pada harddisk seperti RLL, MFM, dan PRLM. Konsep dengan cara overwrite ini adalah dengan membalik bidang magnetik pada disk bolak-balik sebanyak mungkin tanpa menulis pola yang sama berturut-turut.Rumusan masalah pada artikel ilmiah ini adalah bagaimana data recoverymenggunakan software forensic: winhex and x-ways forensic?

II. METODE PENELITIAN

2.1. *The Chain of Custody*

Satu hal terpenting yang perlu dilakukan investigator untuk melindungi bukti adalah the chain of custody.Maksud istilah tersebut adalah pemeliharaan dengan meminimalisir kerusakan yang diakibatkan karena investigasi.Barang bukti harus benarbenar asli atau jika sudah tersentuh investigator, pesan-pesan yang ditimbulkan dari bukti tersebut tidak hilang. Tujuan dari the chain of custody adalah :

1. Bukti itu benar-benar masih asli/orisinil
2. Pada saat persidangan, bukti masih bisa dikatakan seperti pada saat ditemukan. (biasanya jarak antara penyidikan dan persidangan relatif lama).

Beberapa pertanyaan yang dapat membantu the chain of custody ini adalah :

1. Siapa yang mengumpulkan bukti ?
2. Bagaimana dan di mana ?
3. Siapa yang memiliki bukti tersebut ?
4. Bagaimana penyimpanan dan pemeliharaan selama penyimpanan bukti itu ?
5. Siapa yang mengambil dari penyimpanan dan mengapa ?

Untuk menjaga bukti itu dalam mekanisme the chain of custody ini, dilakukan beberapa cara : 1. Gunakan catatan yang lengkap mengenai keluar-masuk bukti dari penyimpanan

2. Simpan di tempat yang dianggap aman.
3. Akses yang terbatas dalam tempat penyimpanan.
4. Catat siapa saja yang dapat mengakses bukti tersebut.

Gambar 1. Chain Of Custody (CoC)

2.2. *Rules of Evidence*

Manajemen bukti kejahatan komputer juga mengenal istilah "Peraturan Barang Bukti" atau Rules of Evidence. Arti istilah ini adalah barang bukti harus memiliki hubungan yang relevan dengan kasus yang ada. Dalam rules of evidence, terdapat empat persyaratan yang harus dipenuhi, antara lain :

1. Dapat Diterima (Admissible) Harus mampu diterima dan digunakan demi hukum, mulai dari kepentingan penyidikan sampai dengan kepentingan pengadilan.
2. Asli (Authentic) Bukti tersebut harus berhubungan dengan kejadian/kasus yang terjadi dan bukan rekayasa.
3. Lengkap (Complete) Bukti bisa dikatakan bagus dan lengkap jika di dalamnya terdapat banyak petunjuk yang dapat membantu proses investigasi.
4. Dapat Dipercaya (Believable & Reliable) Bukti dapat mengatakan hal yang terjadi di belakangnya. Jika bukti tersebut dapat dipercaya, maka proses investigasi akan lebih mudah. Walau relatif, dapat dipercaya ini merupakan suatu keharusan dalam penanganan perkara.

2.3. *Metodologi Forensik*

Teknologi Informasi Metodologi yang digunakan dalam menginvestigasi kejahatan dalam teknologi informasi dibagi menjadi dua :

1. *Search & Seizure*. Investigator harus terjun langsung ke dalam kasus yang dihadapi, dalam hal ini kasus teknologi informasi.Diharapkan investigator mampu mengidentifikasi, menganalisa, dan memproses bukti yang berupa fisik. Investigator juga berwenang untuk melakukan penyitaan terhadap bukti yang dapat membantu proses penyidikan, tentunya di bawah koridor hukum yang berlaku.
2. *Pencarian Informasi*. Beberapa tahapan dalam pencarian informasi khususnya dalam bidang teknologi informasi :
   a. Menemukan lokasi tempat kejadian perkara
   b. Investigator menggali informasi dari aktivitas yang tercatat dalam log di komputer.
   c. Penyitaan media penyimpanan data (data storages) yang dianggap dapat membantu proses penyidikan

Walaupun terlihat sangat mudah, tetapi dalam praktek di lapangan, ketiga tahapan tersebut sangat sulit dilakukan.Investigator yang lebih biasa ditempatkan pada kasus kriminal non-teknis, lebih terkesan terburu-buru mengambil barang bukti dan terkadang barang bukti yang dianggap penting ditinggalkan begitu saja.Dalam menggali informasi yang berkaitan dengan kasus teknologi informasi, peran investigator dituntut lebih cakap dan teliti dalam menyidik kasus tersebut.Celah yang banyak tersedia di media komputer menjadikan investigator harus mengerti trik-trik kasus teknologi informasi.Kedua metodologi di atas setidaknya menjadi acuan pihak yang berwenang dalam menyidik kasus kejahatan dalam bidang teknologi informasi.

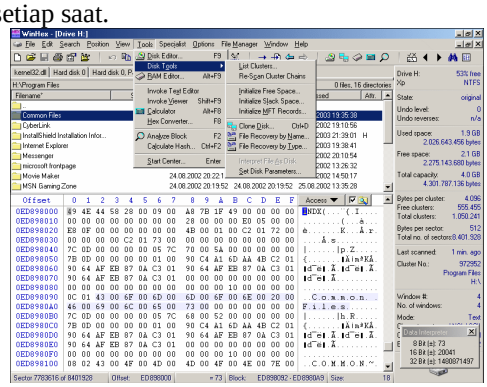
III. HASIL DAN PEMBAHASAN

Data recovery merupakan bagian dari analisa forensik di mana hal ini merupakan komponen penting di dalam mengetahui apa yang telah terjadi, rekaman data, korespondensi, dan petunjuk lannya. Banyak orang tidak menggunakan informasi yang berasal dari data recovery karena dianggap tidak murni/asli/orisinil. Setiap sistem operasi bekerja

dalam arah yang unik, berbeda satu sama lain (walaupun berplatform sistem operasi yang sama). Untuk melihat seberapa jauh data sudah dihapus atau belum, perlu memperhatikan segala sesuatu yang ada dalam raw disk. Jika data yang digunakan untuk kejahatan ternyata masih ada, maka cara yang termudah adalah menguji data dengan pemanfaatan tool yang ada pada standar UNIX, seperti strings, grep, text pagers, dan sebagainya. Sayangnya, tools yang ada tidak menunjukkan data tersebut dialokasikan di mana. Contohnya, intruder menghapus seluruh system log files (dimulai dari bulan, hari, dan waktu) dari minggu pertama Januari, seharusnya ditulis untuk melihat syslog tersebut: Melalui investigasi dari sistem yang dirusak oleh intruder, sistem files UNIX yang modern tidak menyebar contents dari suatu file secara acak dalam disk. Sebagai gantinya, sistem files dapat mencegah fragmentasi file, meskipun setelah digunakan beberapa tahun. File content dengan sedikit fragmentasi akan lebih mudah untuk proses recover dari pada file content yang menyebar dalam disk (media penyimpanan). Tetapi sistem file yang baik memiliki beberapa keuntungan lain, salah satunya mampu untuk menghapus informasi untuk bertahan lebih lama dari yang diharapkan. Dalam kasus Linux, sistem file extension tidak akan menghapus lokasi dari urutan pertama 12 blok data yang tersimpan dalam inode jika file sudah dipindah/dihapus. Hal ini berarti menghapus data dapat dikembalikan langsung dengan menggunakan icat dalam inode yang terwakilkan. Seperti metode data recovery lainnya, tidak akan menjamin jika data tetap ada di tempat semula. Jika file dihapus dalam sistem operasi Linux, inode's time akan terupdate. Dengan menggunakan informasi tersebut, data dapat dikembalikan dari 20 inode pada sistem file yang dihapus.

Forensic Software WinHex pada intinya adalah editor hexadecimal universal, yang paling utama adalah sangat membantu dalam bidang computer forensics, data recovery, proses data dalam tingkat yang rendah, dan keamanan IT. Sebuah peralatan yang semakin maju setiap harinya dan penggunaan dalam keadaan darurat : memeriksa dan mengedit semua jenis file mengembalikan data yang telah dihapus atau data yang telah hilang dari hard drives system file yang corrupt, atau dari kartu memory digital camera. Berikut adalah beberapa kelebihan dan cara kerja dari WinHex, antara lain :

a. Disk editor untuk hard disk, floppy disk, CD-ROM & DVD, ZIP, Smart Media, Compact Flash. Dukungan untuk FAT, NTFS, Ext2/3, ReiserFS, Reiser4, UFS, CDFS, UDF
b. Memiliki interpretasi untuk sistem RAID dan dynamic disks
c. Berbagai macam teknik pemulihan data
d. RAM editor, menyediakan akses kepada physical RAM, dan proses-proses yang dimiliki virtual memory
e. Penerjemah data, mengetahui 20 jenis type data
f. Mengedit struktur data menggunakan templates (contoh : untuk memperbaiki tabel partisi / boot sector)
g. Menyatukan dan memisahkan file, menyatukan dan membagi kejanggalan dalam bytes/words.
h. Menganalisa dan membandingkan file – file
i. Pencarian yang paling flexibel
j. Mengganti fungsi – fungsi Disk cloning (undr DOS dengan X-Ways Replica)
k. Mengatur gambar dan mengamankannya (menurut pilihan dikecilkan ukuran filenya atau dipisahkan menjadi dokumen- dokumen sebesar 650 MB)
l. Memprogram interface (API) dan menulis program
m. Enkripsi AES 256-bit, pengecekan total, CRC32, hashes (MD5, SHA-1)
n. Menghapus file rahasia dengan aman, membesihkan hard drive demi menjaga privacy
o. Mengimpor semua format clipboard, termasuk ASCII hex
p. Mengkonversi diantara biner, hex ASCII, Intel hex, dan Motorola S
q. Setelan karakter : ANSI ASCII, IBM ASCII, EBCDIC, (Unicode)
r. Pergantian jendela yang cepat. Mencetak. Pembangkit nomor acak
s. Mendukung file dengan ukuran yang lebih dari 4 GB. Sangat cepat.
t. Mudah digunakan. Pertolongan yang selalu ada setiap saat.

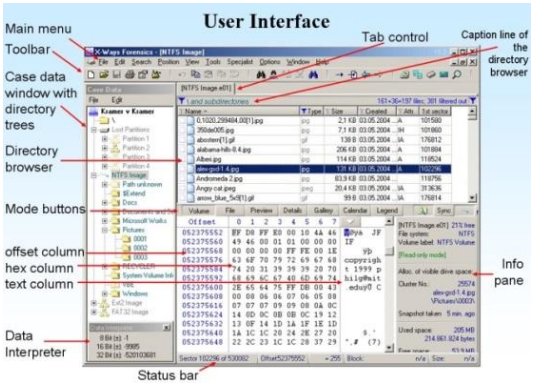


Gambar 2.WinHex

X-Ways Forensik, edisi forensik dari WinHex, adalah lingkungan komputer forensik yang kuat dan mampu dengan sejumlah fitur forensik, menerjemahkannya menjadi perangkat analisis yang kuat : menangkap ruang yang bebas, ruang yang lemah, ruang dalam partisi, dan teks, membuat table yang berisi petunjuk dengan detail yang lengkap dengan segala file yang termasuk dan file yang telah dihapus dan direktori dan bahkan alur data alternative (NTFS), file dengan penomoran yang tertahan, dan banyak lagi. Juga menyediakan sebagai penggambar disk dalam tingkatan rendah dan peralatan cloning yang menciptakan cermin sesungguhnya (termasuk ruang yang lemah) dan membaca sebagian besar format drive dan type media, pendukung – pendukung drive dan file dari ukuran yang pada dasarnya tidak terbatas (bahkan terabytes dari NTFS volumes). X-Ways forensics dan WinHex pada dasarnya mengartikan dan menunjukan struktur direktori pada FAT, NTFS, Ext2/3, Reiser, CDFS, dan media UDF dan file gambar. Itu menunjukan pemulihan yang aman pada hard disk, memory card, flash disks, floppy disks, ZIP, JAZ, CDs, DVDs, dan banyak lagi. X-Ways forensics dan WinHex menyatukan beberapa

mekanisme penyembuhan file yang otomatis dan mengizinkan pemuliha data secara manual. WinHex memberikan kepuasan, pencarian fungsi yang sangat cepat secara simultan yang mungkin anda butuhkan untuk mencari di seluruh media (atau data gambar), termasuk kelemahan, untuk data yang telah dihapus, data yang disembunyikan dan banyak lagi. Melalui akses fisik, hal ini dapat dilakukan meskipun isinya tidak terdeteksi oleh operating system, contohnya yang disebabkan oleh sistem file yang corrupt dan tidak diketahui. Selain fitur-fitu diatas, Winhex juga dapat digunakan untuk:

a. Drive cloning, drive imaging,membuat suatu duplikasi yang bisa menghemat waktu dalam menginstall suatu sistem operasi dan software lainnya untuk beberapa komputer yang sejenis atau agar memungkinkan untuk memperbaiki suatu installasi yang sedang dilakukan apabila ada data yang rusak.
b. RAM editor Untuk menjalankan/memanipulasi program yang sedang berjalan dan dalam permainan komputer khusus.
c. Analyzing files Untuk menentukan jenis recoveri data sebagai bagian rantai yang hilang oleh ScanDisk atau ChkDisk
d. Wiping confidential files or disks Dengan menghapus file rahasia dengan winhex maka tidak satupun dari komputer yang ada bahkan spesialis komputer forensik sekalipun tidak akan bisa mendapatkan file itu lagi.
e. Wiping unused space and slack space . Dengan menghapus ruang kosong yang tidak terpakai maka akan meminimalkan ukuran backup datanya. Pada drive berjenis NTFS, winhex dapat membersihkan semua file $Mft (Master File Table) yang tidak terpakai.
f. ASCII-EBCDIC conversion, memungkinkan untuk bisa merubah kode ASCII ke EBCDIC
g. Binary, Hex ASCII, Intel Hex, and Motorola S conversion, digunakan oleh programmer yang menggunakan (E)PROM
h. Unifying and dividing odd and even bytes/words, digunakan oleh programmer yang menggunakan (E)PROM
i. Conveniently editing data structure, untuk merubah struktur data yang ada dengan baik sesuai dengan apa yang diinginkan.
j. Splitting files that do not fit on a disk Kita bisa menggabungkan atau membagi file yang tidak muat di disk.
k. WinHex as a reconnaissance and learning tool, menemukan program-program lain yang disimpan pada suatu file dan mempelajari file-file yang formatnya tidak diketahui dan bagaimana file tersebut bekerja.
l. Finding interesting values (e.g. the number of lives, ammunition, etc.) in saved game files Menggunakan penggabungan antara pencarian atau menggunakan perbandingan file
m. Manipulating saved game files,untuk permainan di komputer, mengikuti cheat-nya yang ada di internet atau membuat cheat sendiri.
n. Upgrading MP3 jukeboxes and Microsoft Xbox with larger hard drive,untuk meng-upgrade, hard disk baru memerlukan persiapan dan disinilah winhex dipergunakan.
o. Manipulating text,untuk mengubah text di sebuah file berupa binary yang di aplikasi tersebut tidak diizinkan untuk bisa merubahnya.
p. Viewing and manipulating files that usually cannot be edited, untuk mengubah file yang tidak bisa diubah karena dilindungi oleh windows
q. Viewing, editing, and repairing sistem areas,seperti master boot record dengan table pembagiannya dan boot sector.
r. Hiding data or discovering hidden data Winhex secara khusus memungkinkan kita menggunakan bagian yang kelebihan dan tidak digunakan oleh sistem operasi
s. Copy & Paste, dimungkinkan untuk secara bebas untuk mengkopi dari disk dan menuliskannya ke dalam clipboard di disk tanpa perlu melihat batasan bagian/sektor nya
t. Unlimited Undo, mengulang apa yang telah kita ubah atau kerjakan dengan bebas tanpa batasan.
u. Jump back and forward Winhex, menyimpan sejarah/history apa yang telah dikerjakan sehingga bisa kembali ke sebelum atau ke tahap apa yang telah kerjakan dengan mudah seperti pada web browser.
v. Scripting Pengubahan file otomatis menggunakan script. Script bisa dijalankan dari start center atau awal perintahnya. Ketika script dijalankan kita bisa membatalkannya dengan menekan esc.
w. API (Application Programming Interface) Pengguna yang professional (programer) akan memanfaatkan kemampuan winhex dalam program buatan mereka.
x. Data recovery, bisa digunakan pada semua file sistem dan bisa memperbaiki beberapa jenis file pada satu waktu seperti file jpg, png, gif, tif, bmp, dwg, psd, rtf, xml, html, eml, dbx, xls/doc, mdb, wpd, eps/ps, pdf, qdf, pwl, zip, rar, wav, avi, ram, rm, mpg, mpg, mov, asf, mid.
y. Komputer examination/ forensiksWinhex adalah sebuah alat atau software yang sangat berharga bagi seorang spesialis investigasi komputer di sebuah perusahaan pribadi dan untuk penegakkan hukum.
z. Trusted download Dengan winhex akan lebih aman dan dapat dipercaya kebersihannya dari hal-hal yang dapat mengganggu komputer.
aa. 128-bit encryption dengan winhex kita bisa membuat file tidak bisa dibaca oleh orang lain.
bb. Checksum/digest calculation Untuk memastikan file yang ada tidak ada yang rusak dan tidak terubah, atau untuk mengenali file-file yang dikenal.
cc. Generating pseudo-random data Digunakan untuk beberapa tujuan seperti simulasi ilmiah.



Gambar 3, X-Ways Forensic

IV. KESIMPULAN

Dari pembahasan yang sudah dipaparkan, makapeneliti dapat menarik kesimpulan,yaitu :

Penggunaan software forensic: winhex and x-ways forensic memiliki banyak keunggulan dalam data recovery sehingga dapat membantupara penegak hukum dalam melengkapi persyaratan *Rules Of Evidence* dan *Chain of Custody.*

V. DAFTAR PUSTAKA

[1] E. K. Mabuto and H. S. Venter, 2011, "*State of the art of Digital Forensic Techniques*", in Information Security for South Africa (ISSA, pp. 1–7).

[2] F. Dezfoli and A. Dehghantanha, 2013, "*Digital Forensic Trends and Future*", Int. J. Cyber-Sec urity Digit. Forensics, vol. 2, no. 2, pp. 48–76.

[3] Kemmish, R. M., 2012 "*What is Forensic Computer"*. Australian institute of Criminology, Canberra. (http://www.aic.gov.au/ publications/ tandi/ti118.pdf)

[4] Mutiara, A Benny, 2007, Buku: Panduan Komputer Forensik Dalam Penanganan Bukti Digital Pada Personal Digital Assistants (PDA)

[5] N. L. Beebe and J. G. Clark, 2005, "*A hierarchical, objectives-based framework for the digital investigations process*", Digit. Investig., vol. 2, no. 2, pp. 147–167.

[6] Osvalds, G. ,2001. "*Definition of Enterprise Architecture",* – Centric Models for The Systems Engineers, TASC Inc.

[7] P. Čisar and S. M. Čisar, "*Methodological frameworks of digital forensics*", in SISY 2011 - 9th International Symposium on Intelligent Systems and Informatics, Proceedings, 2011, pp. 343–347.

[8] Prayudi, Y., Ashari, A. , 2015 "*Digital Chain of Custody!: State Of The Art*", Int. J. Comput. Appl., vol. 114(5), pp. 1–9.

[9] Rosalina, Vidila, 2015, *Pengembangan Model Tahapan Digital Forensics Untuk Mendukung Serang Sebagai Kota Bebas Cyber Crime*, Proceding SENASSET 2015ISBN 978-602-73672-0-3 : 12 Desember 2015.

[10] *www.winhex.com/winhex/*

[11] *www.worldwidejournals.com*

[12] *www.x-ways.net/forensics/*