SAFFA-NG
SISTEM ARISTEKTUR MANAJEMEN KASUS FORENSIK

I Made Wiryana[(1)], A.B. Mutiara[(2)], Andreas Vangerow[(3)]
[(1), (2)] Jurusan Teknik Informatika Gunadarma University, Jakarta, Indonesia
[(3)]P3 Consulting and Software GmbH – Frankfurt Germany

SAFFA-NG
SYSTEM ARCHITECTURE FOR FORENSIC ANALYSIS

Abstract: Cybercrime has been known as side effects of the use of the International Policy Institute for Counter-Terrorism (ICT). The character of digital evidences which are very specific, require special handling methods. Nowadays, there are many forensics tools which are either proprietary or open source. However, most of them are low level tools which are used to gather the uncover data from the storage or computing devices. A better forensic case management which support the root cause analysis based on a formal method will assist the work of investigator. SAFFA-NG is a freely available workflow system which is designed to assist the work of forensic and investigator by guiding the forensic work according to forensic guidelines. System Architecture For Forensic Analysis (SAFFA-NG) is developed using many Open Source Software components which ensure the thorough auditing of the system. It is designed based on technical and forensic requirements. This is a collaboration projects between Gunadarma University, I Made Wiryana (Rechnernetze und Verteilte Systeme (RVS) Arbeitsgruppe – Bielefeld University) and Andreas Vangerow (P3 Consulting GmbH). During the development of system some feedbacks and assistance are provided by Landes Kriminal Alamtes (LKA) Niedersachsen, Komisi Pemberantasan Korupsi (KPK) and Indonesia Police Department.

Keywords: System Architecture For Forensic Analysis (SAFFA-NG), Computer Forensic, Case management, Open Source.

Makin penting dan luas pemanfaatan *ICT*, juga memiliki dampak negatif, yaitu mulai tumbuh dan makin meningkatnya kejahatan *cyber*. Kejahatan *cyber* memiliki barang bukti yang bersifat elektronis dan membutuhkan metode pengelolaan yang khusus, sehingga dapat memenuhi persyaratan forensik untuk digunakan sebagai barang bukti. Saat ini, memang telah terdapat beberapa perangkat lunak yang lazim digunakan para penegak hukum untuk melakukan pekerjaan forensik, misalnya *Encase*, *FTK*, *Autopsy*, *tct*, dan sebagainya (Schweitzer, 2003). Tetapi, penegak hukum harus menyatukan bukti-bukti itu dan me-

Alamat Korespondensi:
Jurusan Teknik Informatika Universitas Gunadarma, Jl. Margonda Raya No. 100, Depok, Jakarta 16464
Telp: 021-78881112 ex: 308, Email: amutiara@staff.gunadarma.ac.id

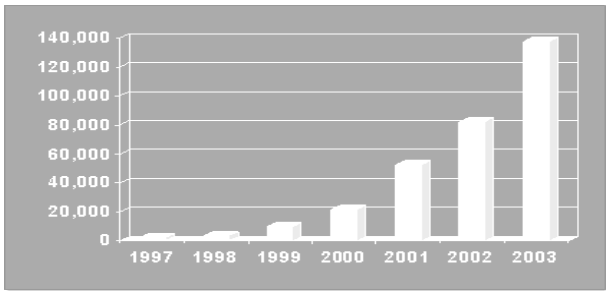
runutnya secara manual agar dapat digunakan sebagai pembuktian. Penulisan laporan forensik harus dilakukan secara manual. Padahal tahapan-tahapan forensik harus dilakukan secara berurutan dengan urutan sesuai bakuan forensik yang diterima pengadilan.

Untuk mendukung pekerjaan itu, dibutuhkan perangkat Manajemen Kasus Forensik yang dapat membantu penegak hukum dalam melakukan tugas forensik. Perangkat lunak ini akan membantu petugas melakukan langkah demi langkah forensik. Di samping itu, juga membantu melakukan analisis dengan menerapkan analisis *Causal Factor* yang menerapkan metode *Why Because Analysis* (*WBA*) yang dikembangkan oleh Prof Peter B. Ladkin PhD (Univ. Bielefeld) yang telah banyak digunakan untuk menganalisis kecelakaan sistem berbasis komputer (Ladkin, 2001). Juga telah digunakan dalam menganalisis kasus sekuriti (Wiryana, 2003). Di samping harus memenuhi tahapan forensik, metode penyimpanan bukti digital dengan menjaga integritas data harus pula dipenuhi oleh sistem ini.

Dengan memanfaatkan infrastruktur perangkat lunak *Open Source* seperti *GNU/Linux, Java*, *Tomcat, Graphviz* dan basis data *Extensible Markup Language* (*XML*), dan ditambah aplikasi khusus yang dikembangkan untuk mendukung sistem *workflow* untuk mendukung pekerjaan forensik, sistem *SAFFA-NG* ini dibangun untuk membantu penegak hukum memerangi kejahatan komputer.

Cyber Crime

Cyber crime didefinisikan sebagai "*crime related to technology, computers, and the internet* "mengalami peningkatan akhir-akhir ini (*CERT*, www.cert.org). Kejahatan komputer secara luas dapat didefinisikan sebagai kegiatan kriminal yang meliputi infrastruktur teknologi informasi, termasuk akses tak berhak (*unauthorized access*), intersepsi ilegal, gangguan data termasuk pengaksesan data secara ilegal yang bersifat merusak, penghapusan data, kerusakan data, perubahan data atau penyembunyian data pada komputer, interferensi sistem, penyalahgunaan *device*, pemalsuan (pencurian ID), serta penipuan secara elektronik. Pada Gambar 1, tampak *trend* kejahatan komputer makin lama semakin meningkat.



Gambar 1 Trend Kejadian Kejahatan Komputer (sumber: *CERT*/CC, www.cert.org)

Ketika suatu kejahatan komputer terjadi, maka pihak pengelola sistem akan melakukan tahapan penanganan kasus (*incident handling*). Proses yang sering melibatkan tim yang disebut *Computer Emergency Response Team* (*CERT*) dilakukan dengan tahapan berikut (*CERT*, www.cert.org): (1) identifikasi yaitu mendeteksi permasalahan atau serangan, (2) koordinasi, yaitu memperkirakan kerusakan yang terjadi, (3) mitigasi yaitu mengendalikan kerusakan, (4) investigasi yaitu memeriksa kerusakan, (5) edukasi yaitu mempelajari kasus yang terjadi untuk perbaikan sistem.

Menghadapi kejahatan dengan kompleksitas yang tinggi ini membutuhkan waktu yang lama dan teknik khusus agar dapat membawanya ke

pengadilan. Sejak dimulainya tahapan pertama di atas, maka metode pengelolaan barang bukti yang tepat harus dilakukan. Analisis forensik merupakan suatu langkah penting dalam penanganan kejahatan komputer. Terutama ketika ingin membawanya menjadi suatu kasus di pengadilan. Komputer dan datanya sebagai barang bukti tidak dapat ditangani tanpa suatu pertimbangan dan aturan yang ketat.

METODE

Forensik dalam Dunia *ICT*

Forensik komputer merupakan bidang yang luas dan diterapkan pada penanganan kejahatan yang berkaitan dengan teknologi informasi. Definisi forensik komputer menurut Noblett adalah proses mengambil, menjaga, mengembalikan, dan menyajikan data yang telah diproses secara elektronik dan disimpan di media komputer (Noblett, 2000). Tujuan forensik komputer adalah untuk mengamankan dan menganalisis bukti digital. McKemmish (1999) mendefinisikan forensik komputer adalah proses mengidentifikasi, menjaga, menganalisis, dan menyajikan bukti digital (*digital evidence*) dalam tata cara yang diterima secara hukum. Kedua definisi tersebut berprioritas pada pemulihan (*recovery*) dan analisis data.

Bukti digital sangat berkaitan dengan forensik komputer. Istilah ini digunakan untuk menghindari keterbatasan yang ada pada istilah bukti elektronik. Termasuk di dalam bukti digital adalah (Turner, 2005): (1) komputer desktop, dapat menyimpan data catatan kegiatan pengguna,email, dan lain-lain, (2) s*erver* sistem, menyimpan data seperti komputer desktop tetapi untuk semua pengguna, dan *file log* lainnya, (3) peralatan komunikasi, *router* atau modem, yang dapat mengandung: *IP Address*, nomor, dan telepon, (4) peralatan komunikasi, *router* atau modem, yang dapat mengandung *IP Address*, nomor, dan lain-lain, (5) *Embedded devices*, sistem komputer kecil yang menjadi bagian dari sistem yang lebih besar, (6) telepon bergerak, yang dapat menyimpan data seperti nomor telepon, *Short Message Service* (*SMS*), *call history*, gambar, dan video.

Prosedur forensik komputer yang perlu dilakukan dengan tahapan sebagai berikut (Stephenson, 2003): (1) membuat salinan dari keseluruhan *log data*, berkas-berkas, dan lain-lain yang dianggap perlu pada suatu media yang terpisah, (2) membuat *fingerprint* dari data secara matematis (contoh: Hashing Algorithm, MD5), (3) membuat *fingerprint* dari salinan secara matematis, (4) membuat suatu *Hashes Masterlist*, (5) dokumentasi yang baik dari segala sesuatu yang telah dikerjakan.

Dalam menindaklanjuti kasus kejahatan komputer, selain masalah pengumpulan dan menyajikan bukti-bukti yang diperlukan penyidik, terdapat juga permasalahan lain yaitu dokumentasi hasil uji forensik komputer. Hal-hal yang didokumentasikan ini adalah segala hal yang berhubungan dengan kejahatan termasuk bagaimana proses penanganan barang bukti tersebut. Artinya harus tercatat rapi siapa, apa, dan bagaimana suatu bukti digital dikelola dan diproses, sehingga sah digunakan sebagai bukti di pengadilan.

Kesulitan-kesulitan yang dihadapi dalam mengelola bukti digital: (1) banyak dan beragamnya sumber bukti digital, dari komputer, *Personal Digital Assistant* (*PDA*), telpon genggam dan sebagainya, (2) membuat salinan dari keseluruhan *log data*, berkas-berkas, dan lain-lain yang dianggap perlu ada, dan terkadang susah untuk dipahami manusia, (3) masalah kuantitas, jumlah data yang harus dianalisis

mungkin saja besar. Teknik reduksi data digunakan untuk memecahkan masalah ini, (4) bukti digital dapat berubah secara mudah, data komputer dapat berubah setiap saat di dalam komputer dan sepanjang jalur transmisi, tanpa meninggalkan jejak nyata.

Memperhatikan beberapa kesulitan di atas, sehingga dalam persidangan, bukti digital adalah hal yang sangat kompleks bagi para hakim. Sangat kecil kemungkinan hakim memiliki pengetahuan komputer yang mendalam. Merupakan tugas seorang spesialis forensik komputer untuk membuatnya menjadi lebih sederhana tanpa mengurangi fakta. Kompleksitas permasalahan komputer dalam persidangan dijelaskan dalam istilah yang mudah dipahami dan jelas.

Data yang ditangani dalam dokumentasi hasil uji forensik merupakan informasi yang besar dan kompleks. Seringkali kesaksian diberikan dalam beberapa bulan bahkan beberapa tahun setelah bukti digital diproses. Karena hal tersebut, dibutuhkan suatu sistem pengelolaan dan dokumentasi hasil analisis uji forensik komputer atau *digital evidence* yang diperoleh dari semua barang bukti yang dapat dipertanggungjawabkan dan dipahami sesuai dengan aturan hukum yang berlaku dari suatu kasus tertentu.

Dokumentasi yang baik, dan tersusun dalam metode pemrosesan yang diterapkan secara konsisten, bertindak sebagai pengingat bagi spesialis komputer juga dapat menjadi kunci penting dalam kesuksesan atau kegagalan suatu persidangan kejahatan komputer. Dokumentasi itu harus lengkap, detil, akurat, dan komprehensif. Tanpa kemampuan untuk rekonstruksi secara akurat terhadap apa yang telah terjadi, bukti penting dapat dipertanyakan. Langkah-langkah analisis dalam dokumentasi harus sesuai dengan pedoman-pedoman yang dipergunakan secara nasional maupun internasional.

Kelangkaan Sumber Daya Manusia (SDM) penegak hukum dalam bidang forensik, menjadikan tahapan forensik dan dokumentasinya menjadi beban berat bagi para petugas dan penyidik. Sehingga, dibutuhkan suatu sistem manajemen kasus forensik yang akan meringankan kerja petugas untuk melakukan tahapan-tahapan forensik yang benar, menghasilkan laporan forensik yang merunut bukti-bukti tersebut secara logis, dan membantu menarik kesimpulan dan menyajikannya sebagai suatu bukti di pengadilan.

HASIL DAN PEMBAHASAN

SAFFA-NG

Untuk mengatasi kebutuhan penegak hukum dalam melakukan analisis forensik, melakukan dokumentasi, serta menarik kesimpulan secara sistematis dan logis, maka dikembangkan suatu solusi Sistem Manajemen Kasus Forensik. Sistem yang dikembangkan ini dibuat merupakan pengembangan dari *SAFFA*.

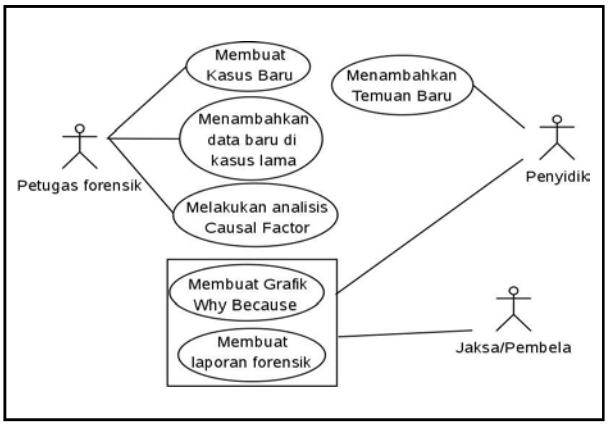
SAFFA yang awalnya dikembangkan sebagai proyek riset oleh Andreas Vangerow – Universitas Bielefeld – Jerman dibawah bimbingan Prof Peter Ladkin PhD dan I Made Wiryana SSi, SKom, MSc, merupakan aplikasi *workflow* yang membantu dokumentasi analisis hasil uji forensik komputer (Vengeron, 2006). *SAFFA* juga membantu menarik kesimpulan penyelidikan dengan menerapkan metode *WBA* yang telah banyak digunakan untuk analisis kecelakaan. *SAFFA* difokuskan untuk analisis forensik *server* dan *desktop Personal Computer* (*PC*).

Sistem yang dikembangkan ini disebut *SAFFA-NG* karena merupakan pengembangan lebih lanjut dan perubahan secara mendasar arsitektur *SAFFA* dengan menggunakan komponen *Open Source* untuk menggantikan komponen *proprietary* yang tadinya digunakan *SAFFA*. Hanya konsep dan pendekatan *SAFFA* saja yang tetap masih digunakan. *SAFFA-NG* ini merupakan kerjasama riset antara Universitas Gunadarma, peneliti *RVS* Arbeitsgrupe-Bielefeld University, dan Andreas Vangerow (*P3 Consulting GmbH*), dengan masukan dari Kepolisian Negara bagian Niedersachsen (*LKA* Niedersachsen) serta kerja sama dengan badan pemerintahan Indonesia seperti KPK, dan Kepolisian Indonesia.

Mekanisne Penggunaan Sistem

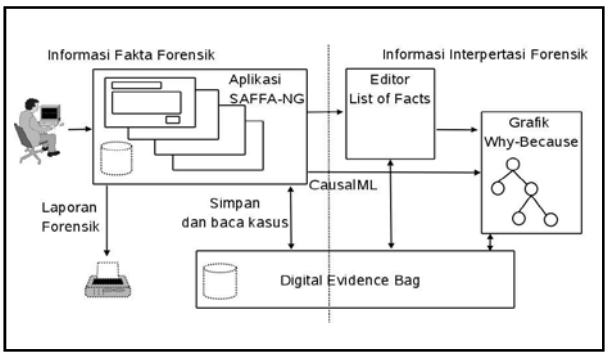
Penggunaan *SAFFA-NG* ini disajikan pada Gambar 2. Pada dasarnya pengguna sistem ini akan terbagi menjadi 3 jenis aktor yaitu: (1) petugas forensik, petugas ini yang melakukan pencarian bukti-bukti digital pada perangkat yang digunakan sebagai bukti, (2) penyidik, yang melakukan penyidikan dengan menggunakan data hasil forensik. Penyidik akan menganalisis kasus dari bukti forensik, secara logis, dan sistematis dengan bantuan *SAFFA-NG,* dalam penyidikan, dapat saja penyidik menemukan suatu bukti baru yang akan diberikan kepada petugas forensik, (3) jaksa/pembela, memperoleh keluaran berupa laporan forensik untuk digunakan di pengadilan.

SAFFA mendokumentasikan hasil analisis uji forensik komputer dengan menggunakan aliran kerja yang terdiri dari tahapan-tahapan sesuai dengan bakuan kerja forensik. Pada tiap tahapan petugas mengisikan formulir yang berbeda. Pada formulir tersebut, informasi dari hasil analisis dapat disimpan



Gambar 2 Diagram *Use-Case SAFFA-NG*

dan jika analisis tersebut dibuka lagi penyelidik dapat memprosesnya lebih lanjut tetapi tanpa merusak informasi pada analisis sebelumnya. Semua *text field* diperuntukkan bagi pertanyaan atau butir tertentu yang berhubungan dengan analisis forensik dan sesuai dengan pedoman/*guideline* yang digunakan. Butir-butir tersebut diistilahkan sebagai indeks *SAFFA*. *SAFFA* terdiri dari 5 Indeks dan beberapa subindeks. Alur kerja SAFFA dapat dilihat pada Gambar 3.



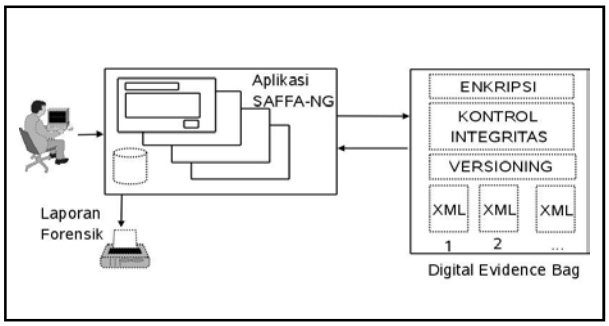
Gambar 3 Alur kerja *SAFFA* (*SAFFA Workflow*)

Hasil analisis perangkat lunak lain dapat dijadikan sebagai lampiran untuk pertanyaan atau butir dari indeks yang berhubungan yang digunakan di dalam analisis faktor kejahatan. Semua

dokumentasi akan digabungkan dalam satu digital *evidence bag* untuk setiap *ID* kasus. Hasil analisis yang telah dimasukkan akan disimpan pada sebuah berkas *XML* dengan nama sesuai dengan kasus yang bersangkutan. *Digital Evidence Bag* berupa sebuah suatu obyek penyimpanan untuk setiap kasus.

Untuk laporan forensik, *SAFFA-NG* dapat mengubah berkas *XML* menjadi berkas *HTML* atau berkas *Doc*, *OpenOffice*, dan lainnya. Berkas laporan ini disimpan di dalam folder *Digital Evidence Bag* dan dapat dicetak serta diedit pada aplikasi Ms Word atau *OpenOffice*. Selain itu dalam *Digital Evidence Bag* disimpan juga folder untuk CausalML. Format CausalML ini digunakan untuk menghasilkan *Why Because Graph* yang akan mempermudah dalam menganalisis kasus.

Sedikit berbeda dengan sistem basis data atau *workflow*, maka *SAFFA* ini harus memiliki beberapa fitur di dalam sistem basis data yang digunakan sebagai *Digital Evidence Bag*. Fitur tersebut adalah: (1) mendukung enkripsi, (2) mendukung *versioning,* (3) mendukung kontrol integritas. Desain Basis Data *SAFFA*.



Gambar 4 Desain Basis Data *SAFFA*

SAFFA memungkinkan pengguna (dalam hal ini penyelidik) untuk membuat suatu interpretasi dengan dukungan metode formal untuk *Causal Analysis* yaitu *WBA*. Penyelidik dapat memasukkan analisis *WBA* untuk setiap butir analisis. Bagian kanan tampilan halaman analisis *SAFFA* diperuntukkan untuk analisis sistem kausal. Dari analisis ini dapat dibuat sebuah "*list of facts*".

List of facts digunakan untuk membuat suatu grafik *WBA*, grafik ini menunjukkan hubungan kausal dalam bentuk diagram. Sebuah "*fact*" berisikan data mengenai indeks dan deskripsinya, daftar *Necessary Causal Factor* (*NCF*), jenisnya, dan lain-lain. Hasil analisis *WBA* inilah yang disimpan pada folder *CausalML*. Proses analisis *WBA* memungkinkan pengguna untuk mendapatkan suatu interpretasi metode *WBA* dari setiap kasus.

Pertimbangan Khusus

Walau pada dasarnya sistem ini merupakan sistem *workflow*, tetapi karena digunakan sebagai tugas forensik untuk memenuhi kebutuhan penegak hukum maka membutuhkan beberapa pertimbangan khusus. Pertimbangan tersebut meliputi: (1) sekuriti pada umumnya, karena sistem ini digunakan untuk mengelola bukti digital, maka prinsip sekuriti seperti kerahasiaan (*secrecy*) akan dijaga, penggunaan teknik enkripsi merupakan suatu kewajiban, (2) *accountabilit*y, artinya setiap perubahan data akan dapat dirunut, siapa, dan kapan dilakukannya, (3) *chain of custody*, setiap perubahan akan selalu tercatat, sehingga dapat diikuti rantai bukti yang disajikan, (4) *integrity*, setiap data yang disimpan akan dijaga integritasnya, sehingga perubahan yang dilakukan secara tidak sah akan dapat dideteksi, (5) *interoperability*, diharapkan *SAFFA-NG* ini dapat mendapatkan masukan dari program forensik lainnya.

Berdasarkan pertimbangan tersebut, maka *SAFFA-NG* dikembangkan agar dapat digunakan pada lingkungan/komunitas yang lebih luas. Pengembangan tersebut meliputi dukungan *SAFFA* untuk berbagai bahasa, termasuk: bahasa Indonesia, Inggris, dan Jerman.

Penyusunan tahapan kerja forensik pada *SAFFA-NG* mengacu pada beberapa pedoman/ *guideline*, yaitu:

- A-SIT, *Secure Information Technology Center* (Austria), *Austrian Federal Ministry of the Interior* (Austria), *National Specialist Law Enforcement Centre* (UK), *Federal Ministry of the Interior represented by the LKA Niedersachsen* (Germany), *O.I.P.C.-INTERPOL Sécrearíat général*, EUROPOL, *National Criminal Investigation Department* (Sweden); *Seizure of e-evidence. Deliverable V1.01. 15.12. 2003*. (rekomendasi dari *state offices of criminal investigation Niedersachsen*, Jerman.)
- *U.S Department of Justice. Office of Justice Programms. NIJ Special Report – Forensic Examination of Digital Evidence: A Guide for Law Enforcement.* 1999
- ENFSI; *Guidelines For Best Practice in The Forensic Examination of Digital Technology*.2003. (rekomendasi dari *state offices of criminal investigation Niedersachsen*, Jerman.)
- *Alexander Geschonneck*; *Computer-Forensik*; *dpunkt Verlag*. ISBN: 3-89864-253-4. 2004. Rekomendasi dari *state offices of criminal investigation Niedersachsen*, Jerman, diberikan oleh *Erster kriminalhauptkommisar Christian Foerster*, *Head of Department 56, IT-Forensics*.

Arsitektur Sistem

Pada dasarnya sistem *SAFFA-NG* yang dibangun akan terdiri dari 3 bagian utama:

- *Storage manager* yang bersifat: *archive system*, *versioning*, dengan *integrity* dan fungsi enkripsi. Sehingga, pada model ini suatu berkas tidak pernah diedit tetapi perubahan dari berkas analisis akan selalu tercatat dari waktu ke waktu. Dengan demikian, dapat dengan mudah untuk ditelusuri apa saja yang terjadi. Untuk *storage manager* ini digunakan suatu basis data *XML* yang diberi tambahan suatu aras (*layer*) yang menyajikan metode penyimpanan secara pengarsipan, *versioning*, dan metode penjagaan integritas dan kerahasiaan data dengan menggunakan metode enkripsi.
- *Interface system*, baik ke pengguna, dokumen atau program lain. Sistem ini akan menerima masukan baik dari orang (petugas forensik), ataupun dari keluaran program forensik lainnya. Sebagai keluaran, di samping berbentuk hasil tercetak, dapat juga diberikan ke program pengolah kata atau pengolah grafik.
- *Sistem workflow*. Karena pada dasarnya sistem ini menyajikan benang merah tahapan-tahapan, maka dibutuhkan dukungan *workflow*. Agar fleksibel, misal menghadapi perubahan panduan forensik, maka diterapkan sistem *workflow* yang fleksibel.

Software Terkait

SAFFA merupakan perangkat lunak pertama yang tersedia secara bebas yang digunakan untuk sistem pengelolaan bukti digital dan pengelolaan data forensik. Memang telah ada beberapa perangkat lunak forensik seperti:

- *Encase* (http://www.guidancesoftware.com/)
- X-*Ways* (http://www.x-ways.net)
- *Autopsy* (http://www.sleuthkit.org/autopsy/)
- PyFLAG (http://www.pyflag.net/)
- TimeCoronerToolkit (http://www.porcupine.org/forensics/tct.html)

Tetapi, perangkat lunak tersebut berdiri sendiri dan relatif merupakan forensik aras bawah, yang belum mendukung ke pengambilan runutan kesimpulan. *SAFFA-NG* dapat memanfaatkan keluaran dari perangkat lunak aras bawah tersebut, sebagai masukan pengolaan bukti digital. Sehingga, *SAFFA-NG* dapat merangkum hasil perolehan berbagai perangkat bantu tersebut. *SAFFA-NG* ini menggunakan berbagai komponen perangkat lunak *Open Source* yaitu:

- *GNU/Linux*
- Tomcat *Server*, sebagai *server* untuk aplikasi Saffa *JSP*
- Basis data *XML*
- *OpenOffice* sebagai *converter* berbagai dokumen yang dijalankan dalam modus *server*

Perangkat lunak yang hampir mirip dengan fungsi *SAFFA* ini adalah *Open Computer Forensic Architecture* (*OSCA*) dari kepolisian Belanda (http://ocfa.sourceforge.net). Tetapi *OSCA* tersebut lebih pada program untuk membangun *framework server* yang akan digunakan untuk melakukan pekerjaan forensik, bukan memberikan panduan tahapan forensik seperti halnya *SAFFA*. Dari sisi *User Interface*, *SAFFA* memiliki pendekatan lebih ke arah pengguna, jadi pengguna lebih dilibatkan dalam menentukan *User Interface*. Untuk penggunaan di Indoensia, tim pengembang *SAFFA* banyak mendapat masukan dari pihak KPK, serta dicobakan juga di Kepolisian Republik Indonesia.

SIMPULAN

Dengan menggunakan *SAFFA-NG* maka penyidik dan penegak hukum dapat melakukan analisis forensik secara lebih efisien, terarah, serta mengikuti suatu panduan yang formal. Juga memungkinkan adanya pertukaran informasi antar institusi investigasi internasional. Pengembangan sistem ini juga bertujuan untuk menghasilkan sebuah laporan hasil analisis uji forensik komputer dalam bahasa yang berbeda-beda agar dapat digunakan oleh berbagai institusi investigasi internasional.

RUJUKAN

Schweitzer, D, 2003, *Incident Response: Computer Forensics Toolkits*, Indianapolis: Wiley Publs.

Ladkin, PB, 2001, *Causal System Analysis. Formal Reasoning About Safety and Failure*, Heidelberg and London: Springer-Verlag.

Wiryana, IM, 2003, *Analyzing DNS Incident*, Bieleschweig I, Bielefeld – Germany.

CERT, *Historical Statistic*, _____, (online) (http://www.cert.org/stats/historical.html)

Noblett, MG, and Pollit, MM, 2000, Recovering and Examining Computer Forensic Evidence, *Forensic Science Communications*, 2 (4)

McKemmish, R. 1999. What is forensic computing. *Trends & Issues in Crime and Criminal Justice*, No. 118, Canberra: Australia Instute of Criminology

Turner, P. 2005. *Unification of Digital Evidence from Disparate Source (Digital Evidence Bags)*. Digital Forensic Workshop (DFRWS)

Stephenson, P, 2003, Modelling of Post-Incident Root Cause Analysis, *International Journal of Digital Evidence*, Vol 3 (2)

Vangerow, A, 2006, *Entwicklung einer Systemarchitektur fuer forensische Analysen*, Diplomarbeit, Bielefeld University.