Indonesian Journal of Legal and Forensic Sciences 2008; 1(1):40-46 ***Asosiasi Forensik Indonesia***
Diterbitkan di Jakarta

SAFFA-NG
Sistem Aristektur Manajemen Kasus Forensik

I Made Wiryana MSc[1], *Dr. A.B. Mutiara*[1] , *Dr. A. Suhendra*[1], *R. Hadibowo* [1], Andreas Vangerow [2]

[1] Gunadarma University, Jakarta, Indonesia
[2] P3 Consulting and Software GmbH – Frankfurt Germany
{mwiryana|amutiara|adang}@staff.gunadarma.ac.id, andreasvangerow@p3-consulting.de

Abstract

Cybercrime has been known as side effects of the use of 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. 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 (RVS Arbeitsgruppe – Bielefeld University) and Andreas Vangerow (P3 Consulting GmbH). During the development of system some feedbacks and assistance are provided by LKA Niedersachsen, KPK and Indonesia Police Department.

Key words: Computer Forensic, Case management, Open Source.

1. Pendahuluan

Makin pentingnya luasnya pemanfaatan ICT, juga memiliki dampak negatif, yaitu mulai tumbuhnya dan makin meningkatnya kejatahan cyber. Kejahatan cyber memiliki barang bukti yang bersifat elektronis dan membutuhkan metoda pengelolaan yang khusus sehingga dapat memenuhi persyaratan forensik untuk digunakan sebagai barang bukti. Saat ini memang telah ada beberapa perangkat lunak yang lazim digunakan para penegak hukum untuk melakukan pekerjaan forensik, misal Encase, FTK, Autopsy, tct dan lain sebagainya [1]. Tetapi penegak hukum harus menyatukan bukti-bukti itu dan merunutnya 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 itu mendukung pekerjaan itu dibutuhkan perangkat Manajemen Kasus Forensik yang dapat membantu penegak hukum dalam melakukan tugas

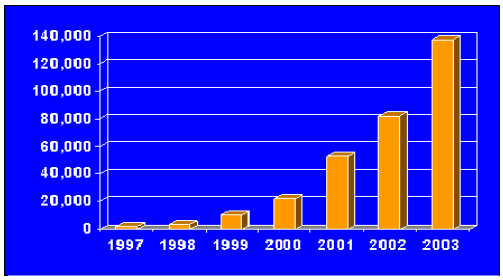
Coressponding Author: [1] Gunadarma University, Jakarta, Indonesia
{mwiryana|amutiara|adang}@staff.gunadarma.ac.id, andreasvangerow@p3-consulting.de

forensik. Perangkat lunak ini akan membantu petugas melakukan langkah demi langkah forensik. Di samping itu membantu melakukan analisis dengan menerapan analisis Causal Faktor yang menerapkan metoda **Why Because Analysis** yang dikembangkan oleh Prof Peter B. Ladkin PhD (Univ. Bielefeld) yang telah banyak digunakan untuk menganalisis kecelakaan sistem berbasis komputer [2]. Juga telah digunakan dalam menganalisis kasus sekuriti [3] Di samping harus memenuhi tahaapan forensik metoda 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 database 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.

2. Latar belakang

Cyber crime yang didefinisikan sebagai "*crime related to technology, computers, and the internet* " mengalami peningkatan akhir-akhir ini [4]. 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 ini makin lama semakin meningkat.



Gambar 1 Trend Kejadian kejahatan Komputer (CERT/CC)

Ketika suatu kejahatan komputer terjadi maka pihak pengelola sistem akan melakukan tahapan penanganan kasus (*incident handling*). Proses yang sering melibatkan tim yang disebut CERT (Computer Emergency Response Team) dilakukan dengan tahapan sebagai berikut [5] :

1. **Identifikasi** : mendeteksi permasalahan atau serangan
2. **Koordinasi** : memperkirakan kerusakan yang terjadi
3. **Mitigasi** : mengendalikan kerusakan
4. **Investigasi** : memeriksa kerusakan
5. **Edukasi** : mempelajari kasus yang terjadi untuk perbaikan sistem

Menghadapi kejahatan dengan kompleksitas yang tinggi ini membutuhkan waktu yang lama dan teknik yang khusus agar dapat membawanya ke pengadilan. Sejak dimulainya tahapan pertama di atas, maka metoda 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.

3. 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 [6]. Tujuan forensik komputer adalah untuk mengamankan dan menganalisis bukti digital. McKemmish mendefinisikan forensik komputer

adalah proses mengidentifikasi, menjaga, menganalisa, dan menyajikan bukti digital (*digital evidence*) dalam tata cara yang diterima secara hukum. Kedua definisi tersebut berprioritas pada pemulihan (*recovery*) dan analisis data [7].

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 [8] :

- Komputer desktop, dapat menyimpan data catatan kegiatan pengguna,email, dll.
- Server sistem, menyimpan data seperti komputer desktop tetapi untuk semua pengguna, dan file log lainnya.
- Peralatan komunikasi, router atau modem, yang dapat mengandung IP Address, nomor, telepon.
- Peralatan komunikasi, router atau modem, yang dapat mengandung IP Address, nomor, dll.
- Embedded devices, sistem komputer kecil yang menjadi bagian dari system yang lebih besar.
- Telpon bergerak, yang dapat menyimpan data seperti nomor telpon, SMS, call history, gambar dan video.

Prosedur forensik komputer yang perlu dilakukan dengan tahapan sebagai berikut [9]:

- Membuat salinan dari keseluruhan log data, files, dan lain lain yang dianggap perlu pada suatu media yang terpisah.
- Membuat fingerprint dari data secara matematis (contoh : Hashing Algorithm, MD5).
- Membuat fingerprint dari salinan secara matematis.
- Membuat suatu Hashes Masterlist.
- Dokumentasi yang baik dari segala sesuatu yang telah dikerjakan.

Dalam menindak-lanjuti 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.

4. Permasalahan

Kesulitan- kesulitan yang dihadapi dalam mengelola bukti digital:

- Banyak dan beragamnya sumber bukti digital, dari komputer, PDA, telfon genggam dan sebagainya
- Membuat salinan dari keseluruhan log data, files, dan lain lain yang dianggap perlu ada, dan terkadang susah untuk dipahami manusia.
- Masalah kuantitas, jumlah data yang harus dianalisis mungkin saja besar. Teknik reduksi data digunakan untuk memecahkan masalah ini.
- Bukti digital dapat berubah secara mudah, data komputer dapat berubah setiap saat di dalam komputer dan sepanjang jalur transmisi, tanpa meninggalkan jejak nyata.

Sehingga dalam persidangan, bukti digital adalah hal yang sangat kompleks bagi para hakim. Sangat kecil kemungkinannya 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 dan dipahami dan jelas.

Data yang ditangani dalam dokumentasi hasil uji forensik merupakan informasi yang besar dan kompleks. Seringkali kesaksian diberikan dalam beberapa bulan bahkan tahun setelah bukti digital diproses. Sehingga dibutuhkan suatu sistem pengelolaan dan dokumentasi hasil analisis uji forensik komputer atau digital evidence yang diperoleh dari semua barang bukti yang dapat di pertanggungjawabkan 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 dan dapat menjadi kunci penting dalam kesuksesan atau kegagalan suatu persidangan kejahatan komputer. Dokumentasi itu harus lengkap, ditail, 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.

Langkanya SDM penegak hukum untuk 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.

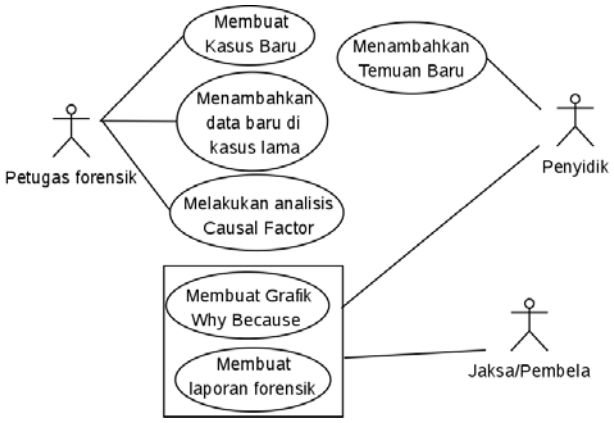
5. SAFFA-NG

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 (*System Architecture For Forensic Analysis*) 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 [10] SAFFA juga membantu menarik kesimpulan penyelidikan dengan menerapkan metoda Why Because Analysis (WBA) yang telah banyak digunakan untuk analisis kecelakaan. SAFFA difokuskan untuk analisis forensik server dan desktop 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 Komisi Pemberantas Korupsi (KPK), dan Kepolisian Indonesia.

5.1. Mekanisne penggunaan sistem



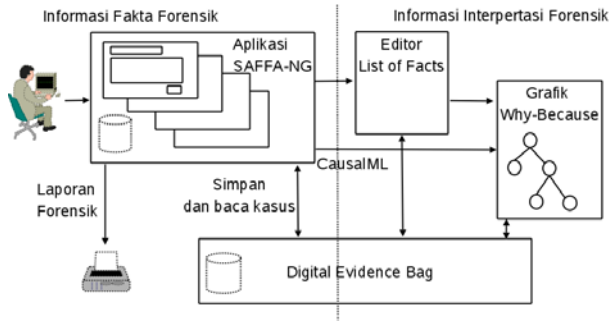
Gambar 2 Diagram Use-Case SAFFA-NG

Penggunaan SAFFA-NG ini disajikan pada gambar 2. Pada dasarnya pengguna sistem ini akan terbagi menjadi 3 jenis aktor yaitu,

- **Petugas forensik**, pada dasarnya petugas ini yang melakukan pencarian bukti-bukti digital pada perangkat yang digunakan sebagai bukti
- **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.
- **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 yang sesuai dengan bakuan kerja forensik. Pada tiap tahapan petugas

mengisikan formulir yang berbeda. Pada formulir tersebut informasi dari hasil analisis dapat disimpan dan jika analisis tersebut dibuka lagi penyelidik dapat memprosesnya lebih lanjut tetapi tanpa merusak informasi pada analsis sebelumnya. Semua text field diperuntukkan bagi pertanyaan atau point tertentu yang berhubungan dengan analisis forensik dan sesuai dengan pedoman/guideline yang digunakan. Point-point tersebut diistilahkan sebagai index SAFFA. SAFFA terdiri dari 5 Index dan beberapa subindex.



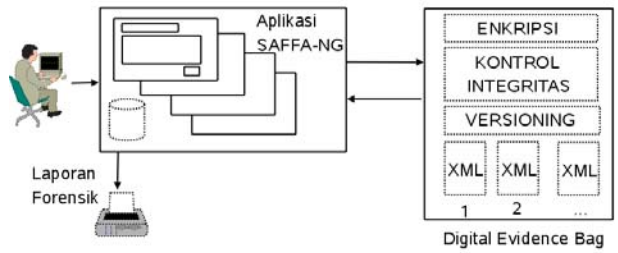
Gambar 3 Alur kerja SAFFA (SAFFA Workflow)

Hasil analisis dari software lain dapat dijadikan sebagai lampiran untuk pertanyaan atau point dari index 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 diinput akan disimpan pada sebuah file 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 file XML menjadi file HTML atau berkas Doc, OpenOffice dan lainnya. Beras report ini 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 database atau workflow, maka SAFFA ini harus memiliki beberapa fitur di dalam sistem database yang digunakan sebagai Digital Evidence Bag. Fitur tersebut adalah :

- Mendukung enkripsi
- Mendukung versioning
- Mendukung kontrol integritas



Gambar 4 Design Database SAFFA

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

List of facts digunakan untuk membuat suatu grafik analisis WB, grafik ini menunjukkan

hubungan causal dalam bentuk diagram. Sebuah "fact" berisikan data mengenai index dan deskripsinya, daftar *Necessary Causal Factor* (NCF), jenisnya, dll. Hasil analisis WBA inilah yang disimpan pada folder CausalML. Proses analisis WBA memungkinkan pengguna untuk mendapatkan suatu interpretasi metode WBA (Why Because Analysis) dari setiap kasus.

5.2. Pertimbangan khusus

Walau pada dasarnya sistem ini merupakan sistem workflow, tetapi karena digunakan untuk tugas forensik untuk memenuhi kebutuhan penegak hukum maka membutuhkan beberapa pertimbangan khusus. Pertimbangan tersebut meliputi

- Security pada umumnya, karena sistem ini digunakan untuk mengelola bukti digital maka prinsip sekurity seperti kerahasiaan (*secrecy*) akan dijaga. Penggunaan teknik enkripsi merupakan suatu kewajiban
- *Accountabilit*y, artinya setiap perubahan data akan dapat dirunut, siapa, kapan dilakukannya
- *Chain of Custody*, setiap perubahan akan selalu tercatat, sehingga dapat diikuti rantai bukti yang disajikan.
- *Integrity*, setiap data yang disimpan akan dijaga integritasnya. Sehingga perubahan yang dilakukan secara tidak sah akan dapat dideteksi.
- *Interoperability*, diharapkan SAFFA-NG ini dapat mendapatkan masukan dari program forensik lainnya.

Berdasarkan pertimbangan tersebut 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 Sécreariat 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.

5.3. 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. Sehingga dapat denga mudah untuk ditelusuri apa saja yang terjadi. Untuk storage manager ini digunakan suatu database XML yang diberi tambahan suatu aras (layer) yang menyajikan metoda penyimpanan secara pengarsipan, *versioning*, dan metoda penjagaan integritas dan kerahasiaan data dengan menggunakan metoda enkripsi.
- **Interface system**, baik ke user, document atau program lain. Sistem ini akan menerima masukan baik dari orang (petugas forensik), ataupun dari output program forensik lainnya. Sebagai keluaran, disamping 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 menghadpai perubahan panduan

forensik, maka diterapkan sistem workflow yang fleksibel.

6. Software terkait

SAFFA merupakan software 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 dari pengolahanan bukti digital. Sehingga SAFFA-NG dapat merangkum hasil perolehan dari 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
- Database XML
- OpenOffice sebagai converter berbagai document yang dijalankan dalam modus server

Perangkat lunak yang hampir mirip dengan fungsi SAFFA ini adalah **Open Computer Forensic Architecture** 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 sis 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.

7. Penutup

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.

8. Daftar Pustaka

[1] Schweitzer, Douglas, *Incident Response: Computer Forensics Toolkits*, Wiley Publs, 2003.

[2] Ladkin, Peter B. *Causal System Analysis. Formal Reasoning About Safety and Failure*, 2001.

[3] Wiryana, I Made, *Analyzing DNS Incident*, Bieleschweig I, Bielefeld - Germany, 2003.

[4] TechTV, TechTV Cybercrime Glossary, 2001.

[5]CERT, *Historical Statistic*, http://www.cert.org/stats/historical.html

[6] Noblett, Michael G, Mark M. Pollit, *Recovering and Examining Computer Forensic Evidence*. Forensic Science Communications, Vol. 2 No. 4, Oktober 2000.

[7] McKemmish, Rodney. *What is forensic computing*. Trends & Issues in Crime and Criminal Justice, No. 118, Australia Instute of Criminology, Canberra, Australia, June 1999.

[8] Turner, Phillip. *Unification of Digital Evidence from Disparate Source (Digital Evidence Bags)*. Digital Forensic Workshop (DFRWS),. 2005.

[9] Stephenson, Peter, *Modelling of Post-Incident Root Cause Analysis*. International Journal of Digital Evidence, Vol 3, No.2 , 2003

[10] Vangerow, Andreas. *Entwicklung einer Systemarchitektur fuer forensische Analysen*, Diplomarbeit, Bielefeld University, 2006.