JISKa, Vol. 1, No. 1, MEI, 2016, Pp. 41 – 46
ISSN 2527-5836

PENGEMBANGAN MODEL *DIGITAL FORENSIC READINESS INDEX* (DiFRI) UNTUK MENCEGAH KEJAHATAN DUNIA MAYA

Tri Widodo [(1)]
Pendidikan Teknologi Informasi
Universitas Teknologi Yogyakarta
e-mail : triwidodo@uty.ac.id

Abstract

Cybercrime is increasing. Unfortunately, the crime rate is not offset by the amount of evidence available. The lack of reports and digital evidences, indicates a lack of understanding of the cybercrime and Forensic Digital, as well as the lack of Digital forensic Readiness of various institutions and the community. Based on the literature study and a review of previous studies, the main component of the Digital forensic Readiness cannot be apart from a few things, such as Strategy, Policy & Procedure, Technology & Security, Digital forensic Response, Control & Risk, and Legality. Further components are broken down into the indicators to assess the Digital forensic Readiness Index (DiFRI) of an institution. With the DiFRI, institutions are expected to be ready in the face of Cybercrime, DiFRI also can increase the amount of evidence and the validity of the evidence.

Key words : Digital forensic, Digital forensic Readiness, Digital forensic Readiness Index(DiFRI), Cyber Crime

Absrak

Kejahatan dunia maya terus meningkat. Namun, peningkatan kejahatan dunia maya, tidak disertai banyaknya barang bukti. Hal ini mengindikasikan kurangnya pemahaman akan kejahatan dunia maya dan juga *digital forensic*. Kesiapan menangani kejahatan dunia maya ini disebut *digital forensic Readiness*. Berdasarkan studi literatur dan penelitian-penelitian sebelumnya, dapat dirumuskan bahwa faktor-faktor *digital forensic Readiness* ini antara lain, *Strategy, Policy & Procedure, Technology & Security, Digital forensic Response*, *Control & Risk, and Legality*. Dari berbagai faktor tersebut dapat dibuat indikator-indikator yang nantinya dapat digunakan untuk mencegah atau menindaklanjuti kejahatan dunia maya. Faktor-faktor dan indikator tersebut akan menghasilkan nilai yang disebut *Digital forensic Readiness Index* (DiFRI). Sehingga kesiapan institusi mencegah dan menangani kejahatan dunia maya dapat diukur dengan menggunakan DiFRI.

Kata Kunci : *Digital forensic*, *Digital forensic Readiness*, *Digital forensic Readiness Index* (DiFRI), Kejahatan dunia maya

1. PENDAHULUAN

Diperkirakan 556 juta orang setiap tahun menjadi korban kejahatan internet, selain itu kerugian di perkirakan mencapai 21 milyar dollar di akibatkan oleh malware, virus, spam, hacking dan penipuan atau pencurian, bahkan masyarakat Cina juga mengalami kerugian sekitar 46 milyar Dollar (Norton, 2012).

Selain itu, empat dari sepuluh orang penguna situs jejaring sosial mengatakan pernah atau mengetahui serangan dari situs jejaring sosial. Data juga menunjukan, satu dari enam orang mengaku akun mereka pernah dibobol, 10% lain mengatakan pernah tertipu dengan teknik penipuan di internet atau meng-*click link* yang tampil di halaman situs jejaring sosial mereka (Norton, 2012).

Indonesia Computer Emergency Response Team (IDCERT) menyatakan pada semester I tahun 2011, terjadi 78.238 tindak Cyber Crime. Tindakan Cyber Crime bahkan meningkat menjadi 144.284 pada dwu-wulan kelima tahun 2011 (Alkazimy, 2011).
Dari berbagai telaah diatas, terlihat bahwa tindak kejahatan internet selalu meningkat. Sayangnya, tingkat kejahatan tersebut tidak diimbangi dengan jumlah barang bukti yang tersedia. Muhammad Nuh Al-Azhar (2013), ketua *Digital forensic Analist Team* (DFAT) dari

Laboratorium Forensik Markas Besar Kopolisian Republik Indonesia menyampaikan dari tahun ke tahun, barang bukti digital masih sangat minim, tidak sebanding dengan tindak kejahatan internet. Minimnya barang bukti digital tersebut juga mengindikasikan kurangnya *Digital forensic Readiness* dari berbagai lembaga dan institusi tempat bekerja, sekolah, maupun lingkungan masyarakat.

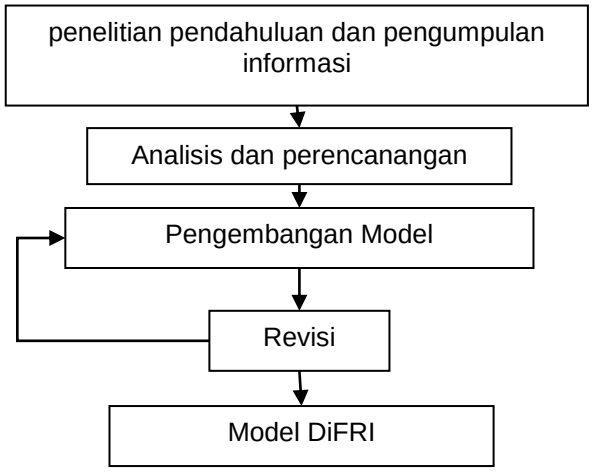
Penelitian terkait *Digital forensic Readiness* masih sangat langka, bahkan peneliti kesulitan menemukan penelitian-penelitian terdahulu mengenai *Digital forensic Readiness* di Indonesia, sehingga penelitian ini sangat penting dan bermanfaat sekali bagi berbagai institusi dan perorangan.

2. KONSEP DASAR *DIGITAL FORENSIC READINESS*

Berdasar studi pustaka dan *review* beberapa penelitian-penelitian sebelumnya. Antara lain, John Tan (2001) menyampaikan komponen digial forensic *Readiness* yaitu *Procedure*, security, dan *Legality* in law. Selanjutnya Robert Rowlingson (2014) menyebutkan unsur *digital forensic Readiness* meliputi *Strategy, resources, digital evidence, procedure, control, human skill, documentation, dan legal review*. CP Grobler dan CP Lowrens (2007) menjelaskan *Digital forensic Readiness* adalah bagian dari *Security,* dan *Barske, Stander,* dan *Jordaan* (2010) menyebutkan komponen *digital forensic Readiness* mencakup *Strategy, policy, procedure, technology*, *digital forensic response*, dan *control* untuk mengukur *Digital forensic Readiness*.

3. METODE PENELITIAN

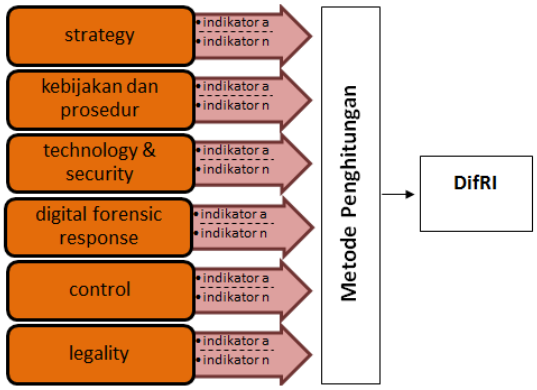
Pada penelitian ini, model *Digital forensic Readiness Index* (DiFRI) dikembangkan berdasarkan penelitian pustaka (library research). Adapaun tahapan penelitian adalah sebagai berikut:



Gambar 1. Tahapan Penelitian

4. HASIL

Pada penelitian ini, hasil penelitian berupa model, yaitu model *Digital forensic Readiness Index* (DiFRI) seperti yang terlihat pada gambar 1.



Gambar 2. Model DiFRI

Selanjutnya dari masing-masing komponen dirumuskan menjadi sejumlah indikator yang memberikan informasi/gambaran lebih lengkap dari kriteria /komponen utama. Adapun detail indikator masing-masing komponen tersebut adalah

a. Komponen *Strategy*

Indikator Komponen *Strategy* yaitu :

- Program-program *Digital forensic Readiness*
- Aturan, regulasi dan kewajiban menyimpan dokumen, file dan rekaman (CCTV, Log, dokumen)
- Ketentuan ketika terjadi peristiwa yang membutuhkan barang bukti digital
- Identifikasi sumber-sumber dan tipe-tipe yang berbeda dari barang bukti digital organisasi
- Identifikasi teknologi dan Sumber Daya manusia untuk menjamin *Digital forensic Readiness*
- Jaminan ketersediaan dana untuk menjalankan dan merawat program *Digital forensic Readiness*

b. Komponen *Policy* & *Procedure*

Indikator komponen *Policy & Procedure* antara lain :

- Kebijakan dan prosedur sebagai petunjuk aktifitas dan kegiatan anggota organisasi yang mengunakan TIK
- Sangsi bagi pelanggar kebijakan dan prosedur *Digital forensic Readiness*
- Kebijakan bahwa semua sumber daya informasi dan data merupakan milik organisasi
- Kebijakan dalam keadaan bagaimanakah barang bukti digital dapat diamankan
- Kebijakan barang bukti digital apa saja yang harus diamankan
- Kebijakan yang menyatakan cara dan situasi ketika bukti-bukti yang telah diamankan oleh organisasi dapat dilepaskan kepada pihak di luar organisasi, termasuk ketika harus dirujuk ke penegak hukum
- Kebijakan pembagian wewenang, tugas dan tanggungjawab terkait pengumpulan barang bukti digital, pemeliharaan dan pemeriksaanya

c. Komponen *Technology* & Security

Indikator komponen *Technoloy & Securit*y antara lain :

- Jaminan manajemen log dari masing-masing sistem, pemeliharaan, dan pengelolaan
- Manajemen media penyimpanan (CD, *hardisk, falshdisk*) dari masing-masing komputer dan server
- Ketersediaan perangkat akuisisi dan analisis barang bukti digital, baik berupa hardware (*write block protector*, dll) maupun *software* (analisys tool)

- Jaminan keamanan barang bukti, baik secara online maupun offline, melalui imaging maupun penggandaan fisik
- Ketersediaan perangkat pendukung *digital forensic* seperti cctv, *finger print*, dan autentikasi sistem
- Ketersediaan perangkat pengamanan sistem seperti *firewall*, anti virus
- Ketersediaan perangkat pendukung keamanan seperti *enkripsi* dan *kriptografi*

d. Komponen *Digital forensic Response*

Indikator komponen *Digital forensic Response* yaitu :

- Ketersediaan SOP (standard operating *procedure*) penanganan insiden maupun tindakan *digital forensic*
- Ketersediaan SDM yang memiliki sertifikasi/keahlian bidang *digital forensic*
- Tim penanganan *cyber crime* dan *digital forensic response*
- Pelatihan-pelatihan SDM mengenai penanganan *cyber crime* dan *digital forensic*
- Petunjuk teknis pengaduan maupun pelaporan insiden
- Alat peraga, petunjuk dan arahan mengenai *cyber crime* berupa poster, banner, dan alat peraga lainya
- Ketersediaan sekretariat pengaduan, informasi dan pelaporan *cyber crime*

e. Komponen *Control* & Risk

Indikator komponen *Control*& Risk antara lain :

- Pengawasan program *Digital forensic Readiness*
- Evaluasi secara berkala program *Digital forensic Readiness*
- Sosialisasi program *digital forensic* kepada anggota organisasi
- Pemahaman pada anggota setiap proses *digital forensic* dan resiko kegagalan setiap proses
- Pembaharuan perangkat, tool, dan sistem secara berkala
- Pembahasan hasil investigasi maupun publikasi hasil investigasi kepada kepala-kepala departemen/sub bagian

f. Legality

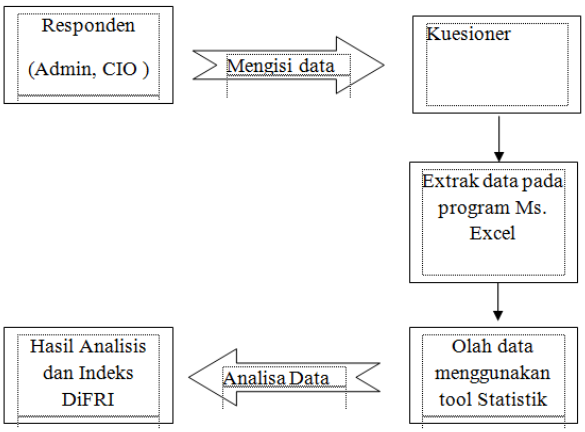
Indikator komponen *Legality* yaitu :

- Kebijakan peninjauan aspek hukum setiap proses investigasi *digital forensic* dan insiden
- Keterlibatan penegak hukum, ahli, auditor profesional dalam evaluasi *digital forensic* atau *cyber crime* pada organisasi
- Pemahaman setiap anggota institusi akan undang-undang transaksi elektronik dan data digital
- Sosialisasi peraturan dan undang-undang transaksi elektronik dan data digital
- Pelatihan penanganan ciber crime dan proses hukum

Identifikasi kebijakan-kebijakan untuk menjamin pengumpulan barang bukti sesuai dengan legalitas hukum yang ada.

4.1 Metode Pengumpulan Data

Pada penelitian ini, data akan didapatkan melalui kuesioner. Kuesioner tersebut merupakan model DiFRI yang telah dirancang. Setiap direktur /CIO, administrator dan responden akan mengisi kuesioner yang telah disediakan, selanjutnya dilakukan analisis pada data tersebut. Adapun alur pengumpulan data seperti terlihat pada Gambar 2.



Gambar 3. Alur Pengumpulan Data

4.2 Metode Penghitungan Data

Pada kuesioner, skala yang digunakan adalah skala *Guttman*, yaitu skala pengukuran dengan jawaban tegas, antara "ada-tidak". Selanjutnya, dari enam komponen di atas akan dilakukan *scoring* untuk menilai aspek DiFRI secara keseluruhan untuk mengetahui *Digital forensic Readiness Index* suatu organisasi. Contoh kuesioner pengukuran DiFRI dapat dilihat pada tabel 1.

Tabel 1. Rancangan kuesioner

Kuesioner Pengukuran DiFRI
Komponen x

Nama Institusi :.....
Nama Responden :……..
Jabatan :.....

No	Indikator	Jawaban	
1	Xxx	Ada	Tidak

Dari kuesioner pada tabel 3.1, kemudian akan dilakukan penghitungan atas jawaban "Ada" dan "Tidak", selanjutnya dilakukan *scoring* pada masing-masing aspek dengan menggunakan rumus. Hasil *scoring* masing-masing komponen tersebut dan DiFRI seperti terlihat pada tabel 3.2.

Tabel 3.3 Penentuan Skor DiFRI Institusi

NO	Nama Institusi	Skor Aspek pada Komponen 1	Skor Aspek pada Komponen 2	Skor Aspek pada Komponen n	Skor keseluruhan DiFRI
1	Institusi A				

DiFRI akan dinilai berdasarkan besar nilai dari masing-masing komponen, sehingga didapatkan rumus DiFRI yaitu :

DiFRI = 1/6 indeks komponen *strategy*
+ 1/6 indeks komponen *policy & procedure*
+ 1/6 indeks komponen *technology & security* (1)
+ 1/6 indeks komponen *digital forensic response*
+ 1/6 indeks komponen *control*
+ 1/6 indeks komponen *legality*

Selanjutnya besar indeks untuk masing-masing komponen dihitung menggunakan rumus :

$$I_{\mathrm{A}} = \frac{\sum_{k=1}^{n} A}{n_A} \cdot 10 \qquad (2)$$

I_A merupakan indeks dari masing-masing aspek, selanjutnya A merupakan jumlah indikator yang bernilai ”ada”, dan nA adalah total dari indikator pada komponen tersebut. Karena nilai indeks pasti akan selalu bernilai $0 \leq IA \leq 1$, maka digunakan perkalian 10, yang dimaksudkan untuk mendapatkan skala dari 0 sampai dengan 10.

5. KESIMPULAN

Berdasarkan studi pustaka dari beberapa penelitian sebelumnya, dapat disimpulkan bahwa

1. Model DiFRI memiliki beberapa komponen, yaitu *Strategy*, *Policy* and *Procedure*, *Technology* and Security, *Digital forensic Response*, *Control*, dan Legality
2. Model DiFRI akan memberikan *output* berupa indeks
3. Indeks DiFRI mencerminkan kesiapan sebuah institusi dalam mencegah dan menangani kejahatan dunia maya

DAFTAR PUSTAKA

Al-Azhar, M. Nuh,. (2013). *Mobile Forensic Investigation*. Hacking and *Digital forensic* Expo (Hadfex). UII Yogyakarta

Alkazimy, Ahmad Khalil. (2011). *Statistik Internet Abuse Indonesia 2011:Laporan Semester-I Tahun 2011*, edisi I. http://www.cert.or.id/media/files/Lap-Abuse-Semester-I-2011.pdf diakses 4 April 2013

Barske, D., Stander, A. & Jordaan, J. (2010), *A Digital forensic Readiness Framework for South African SME's*. IEEE. diakses tanggal 23 januari 2013 dari http://icsa.cs.up.ac.za/issa/2010/Proceedings/Full/30_Paper.pdf

Grobler, CP., Louwrens, CP. (2007), *Digital forensic Readiness as a Component of Information Security Best Practice*. Boston:Springer. diakses tanggal 23 Januari 2013 dari http://www.springer.com/cda/content/document/cda_downloaddocument/9780387723662-c2.pdf

Norton. (2012). *2012 Norton Cyber crime Report*, http://now-static.norton.com/now/en/pu/images/Promotions/2012/*cybercrime*Report/2012_Norton_*Cyber crime*_Report_Master_FINAL_050912.pdf diakses 4 April 2013

Rowlingson, Ph.D., Robert. (2004). *A Ten Step Process for Forensic Readiness, International Journal of Digital Evidence vol 2*. Winter diakses pada 23 Januari 2013 dari http://www.utica.edu/academic/institutes/ecii/publications/articles/A0B13342-B4E0-1F6A-156F501C49CF5F51.pdf

Tan, John. (2001). *Forensic Readiness*. Cambridge, USA. http://isis.poly.edu/kulesh/forensics/forensic_*Readiness*.pdf diakses 23 januari 2013