Blantika : Multidisciplinary Jornal
Volume 1 Number 2, February, 2023
p- ISSN xxxx-xxxx e-ISSN 2985-4199

ANALISIS MODEL *DIGITAL FORENSIC READINESS INDEX* (DiFRI) UNTUK MENCEGAH *CYBERCRIME*

Erine Dheanda[1], Tata Sutabri[2]
Fakultas Ilmu Komputer Pasca Sarjana, Universitas Bina Darma Palembang, Indonesia[12]
E-mail: erinpramuka@gmail.com[1], tatasutabri@binadarma.ac.id[2]

INFO ARTIKEL
Diterima: 15 Februari 2023
Direvisi: 20 Februari 2023
Disetujui: 25 Februari 2023

ABSTRAK

Kejahatan dunia maya sedang meningkat. Namun, tidak banyak bukti peningkatan kejahatan dunia maya. Ini menunjukkan bahwa kejahatan dunia maya dan forensik digital tidak dipahami. Kesediaan untuk menghadapi kejahatan dunia maya ini dikenal sebagai kesiapan forensik digital. Berdasarkan kajian indikator dan kajian sebelumnya, dapat dirumuskan bahwa indikator kesiapan forensik digital ini meliputi strategi, kebijakan dan prosedur, teknologi dan keamanan, respon forensik digital, pengendalian dan risiko serta legalitas. Berbagai indikator tersebut dapat digunakan untuk membuat indikator yang nantinya dapat digunakan untuk mencegah atau mengendalikan kejahatan dunia maya. Faktor dan indikator tersebut menghasilkan suatu nilai yang disebut Digital Forensics Readiness Index (DiFRI). DiFRI dapat digunakan untuk mengukur kesiapan lembaga dalam mencegah dan menangani kejahatan dunia maya.

Kata Kunci: Kesiapan Forensik Digital; Indexs Kesiapan Forensik Digital (DiEFRI); Cybercrime

ABSTRACT

Cybercrime is on the rise. However, there is not much evidence of an increase in cybercrime. This suggests that cybercrime and digital forensics are not understood. This willingness to deal with cybercrime is known as digital forensic readiness. Based on the study of indicators and previous studies, it can be formulated that these digital forensic readiness indicators include strategies, policies and procedures, technology and security, digital forensic response, control and risk and legality. These indicators can be used to create indicators that can later be used to prevent or control cybercrime. These factors and indicators produce a value called the Digital Forensics Readiness Index (DiFRI). DiFRI can be used to measure an agency's readiness to prevent and address cybercrime.

Keyword; Digital Forensics Readiness; Digital Forensic Readiness Indexes (DiEFRI); Cybercrime

This work is licensed under a Creative Commons Attribution-ShareAlike 4.0 International

PENDAHULUAN

Diperkirakan 556 juta orang menjadi korban kejahatan dunia maya setiap tahun, selain malware, virus, spam, peretasan, dan penipuan atau pencurian, kerugian diperkirakan mencapai 21 miliar dolar AS, bahkan Tiongkok menderita kerugian sekitar 46 miliar dolar (Symantec, 2012).

Selain itu, empat dari sepuluh pengguna situs web Indica mengatakan mereka mengalami atau mengetahui serangan situs web Indica. Data tersebut juga menunjukkan bahwa satu dari enam orang mengakui bahwa akun mereka disusupi dan 10% lainnya mengatakan bahwa mereka telah ditipu menggunakan teknik penipuan online atau dengan mengklik tautan di situs web indeks mereka (Symantec, 2012).

Tim Tanggap Darurat Komputer Indonesia (IDCERT) melaporkan bahwa pada semester pertama tahun 2011 terdapat 78.238 kejahatan dunia maya. Menurut Alkazimy Jumlah kejahatan dunia maya bahkan meningkat menjadi 144.284 pada kuartal kelima tahun 2011 (Widodo, 2016).

Berdasarkan berbagai penelitian yang telah disebutkan di atas, terlihat bahwa kejahatan dunia maya terus meningkat. Sayangnya, jumlah kejahatan tidak sesuai dengan jumlah bukti yang tersedia. Muhammad Nuh Al-Azhar (2013), Ketua Tim *Digital Forensic Analyst* (DFAT) (Nasiroh & Romahon, 2021).

Laboratorium Ilmu Forensik Mabes Polri menyebutkan dari tahun ke tahun bukti digital masih sangat terbatas dan tidak bisa dibandingkan dengan kejahatan dunia maya. Kurangnya tampilan digital juga menunjukkan kurangnya kesiapan forensik digital dari berbagai institusi dan tempat kerja, sekolah dan masyarakat. Penelitian terkait *Digital Forensic Readiness* masih sangat jarang, bahkan peneliti sulit menemukan penelitian sebelumnya tentang *Digital Forensic Readiness* di Indonesia, sehingga penelitian ini sangat penting dan bermanfaat bagi berbagai institusi dan individu.

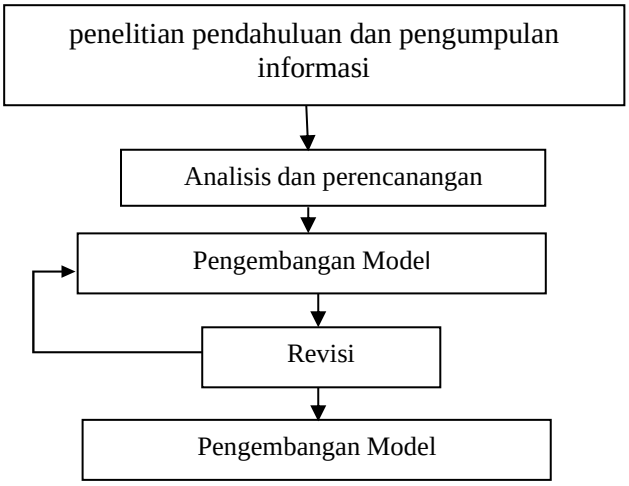
Konsep Dasar *Digital Forensic Readiness*

Berdasarkan penelusuran literatur dan review dari beberapa penelitian sebelumnya. John Tan memaparkan antara lain komponen kesiapan forensik digital yaitu. prosedur, keamanan dan kepatuhan hukum (Tan, 2001). Selain itu, Robert Rowlingson menyebutkan elemen kesiapan forensik digital, termasuk strategi, sumber daya, bukti digital, prosedur, kontrol, keterampilan manusia, dokumentasi, dan penilaian forensik (Rowlingson, 2004). CP Grobler dan CP Lowrens menjelaskan bahwa kesiapsiagaan forensik digital adalah komponen keamanan (Grobler & Louwrens, 2007) dan Barske, Stander dan Jordaan berpendapat bahwa komponen kesiapsiagaan forensik digital adalah strategi, kebijakan, prosedur,

teknologi, respons dan pengukuran forensik digital meliputi manajemen. Kesiapan Forensik Digital (Barske, Stander, & Jordaan, 2010).

METODE PENELITIAN

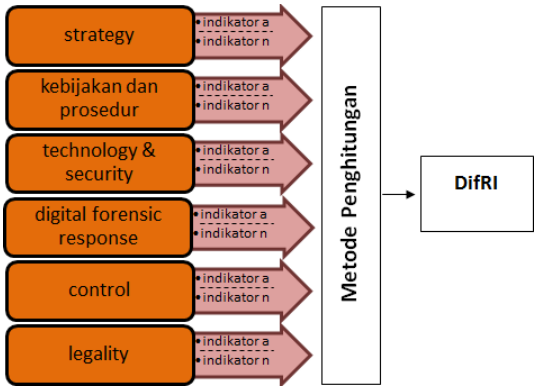
Pada penelitian ini dikembangkan model *Digital Forensic Readiness Index* (DiFRI) berdasarkan penelusuran pustaka. Adapun tahapan penelitiannya adalah sebagai berikut :



Gambar 1. Tahapan Penelitian

HASIL DAN PEMBAHASAN

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



Gambar 2. Model DiFri

Selain itu, setiap komponen dirumuskan menjadi beberapa indikator yang memberikan informasi/representasi yang lebih komprehensif dari kriteria / komponen terpenting. Indikator rinci untuk masing-masing komponen tersebut adalah :

1. **Komponen *Strategy***
   Adapun sub indikator strategi, yaitu:
   a. Program persiapan forensik digital
   b. Aturan, peraturan dan tugas untuk menyimpan dokumen, file dan arsip (CCTV, log, dokumen)
   c. Reservasi saat acara membutuhkan tampilan digital
   d. Mengidentifikasi sumber dan jenis bukti digital organisasi
   e. Identifikasi teknologi dan sumber daya manusia untuk memastikan kesiapan forensik digital
   f. Memastikan tersedianya dana untuk mengimplementasikan dan memelihara program Digital Forensic Readiness
2. **Komponen *Kebijakan dan Prosedur***
   Indikator kebijakan dan prosedur meliputi:
   a. Kebijakan dan prosedur untuk memandu tindakan dan aktivitas anggota organisasi yang menggunakan TIK
   b. Hukuman atas pelanggaran kebijakan dan prosedur kesiapsiagaan forensik digital
   c. Praktik bahwa semua informasi dan sumber daya informasi dimiliki oleh organisasi
   d. Praktikkan kondisi di mana bukti digital dapat diamankan
   e. Kebijakan untuk melindungi bukti digital
   f. Kebijakan yang menentukan cara dan situasi di mana bukti yang ditangkap oleh organisasi dapat dibagikan dengan pihak di luar organisasi, termasuk kapan harus diteruskan ke penegakan hukum nasional
   g. Kebijakan untuk menetapkan wewenang, tugas, dan tanggung jawab untuk pengumpulan, pemeliharaan, dan peninjauan bukti digital
3. **Komponen *Teknologi dan keamanan***
   Indikator untuk komponen teknologi dan keamanan adalah:
   a. Jaminan pengelolaan log, pemeliharaan dan pengelolaan setiap indica
   b. Pengelolaan sumber daya penyimpanan (CD, hard disk, dummy disk) dari masing-masing cato dan server
   c. Ketersediaan alat preservasi dan analisis bukti digital, baik perangkat keras (perlindungan penulisan, dll.) maupun perangkat lunak (alat analisis)
   d. Memastikan keamanan bukti baik online maupun offline melalui pencitraan dan penyalinan fisik
   e. Ketersediaan peralatan pendukung forensik digital seperti CCTV, sidik jari dan autentikasi Indic
   f. Ketersediaan perangkat keamanan Indica seperti firewall, antivirus
   g. Ketersediaan perangkat untuk mendukung keamanan data seperti enkripsi dan kriptografi
4. **Komponen *Digital forensic Response***
   Indikator dari komponen Digital Forensic Response adalah:
   a. Tersedianya SOP (Standard Operating Procedure) untuk menangani insiden dan prosedur forensik digital
   b. Ketersediaan staf dengan sertifikasi/keahlian forensik digital

c. Respon kejahatan dunia maya dan tim respons forensik digital
d. Pelatihan SDM tentang manajemen kejahatan dunia maya dan forensik digital
e. Petunjuk Teknis Pengaduan dan Pelaporan Insiden
f. Alat peraga, petunjuk dan kebijakan terkait cybercrime berupa poster, spanduk dan alat peraga lainnya
g. Ketersediaan indikator pengaduan, informasi dan pelaporan kejahatan dunia maya

5. **Komponen *Control* & Risk**

Angka utama dari komponen kontrol dan risiko adalah:

a. Tinjauan Program Kesiapan Forensik Digital
b. Evaluasi berkala terhadap Program Kesiapan Forensik Digital
c. Distribusi perangkat lunak forensik digital kepada anggota organisasi
d. Memahami anggota dari setiap proses hukum digital dan risiko kegagalan dalam setiap proses
e. Pembaruan alat, alat, dan dica secara berkala
f. Pembahasan hasil ujian dan komunikasi hasil ujian kepada kepala departemen/sudin

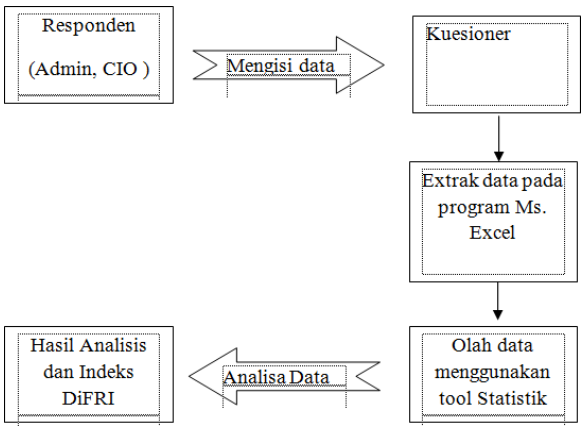
6. **Legalitas**

Indikator komponen legalitas adalah:

a. Berlatih untuk meninjau aspek Ndic dari setiap proses investigasi forensik dan insiden digital
b. Pencantuman indikator, ahli, inspektur dan indikator dalam evaluasi forensik digital atau Kejahatan dunia maya dalam organisasi
c. Setiap insan lembaga pendidikan memahami undang-undang yang mengatur transaksi elektronik dan data digital
d. Penyebaran peraturan dan undang-undang yang terkait dengan transaksi elektronik dan data digital
e. Pelatihan manajemen kejahatan dunia maya dan proses Ndic Identifikasi praktik untuk memastikan pengumpulan bukti sesuai dengan hukum Ndic.

Metode Pengumpulan Data

Dalam penelitian ini, informasi dikumpulkan melalui kuesioner. Kuesioner adalah model DiFRI yang dirancang. Setiap direktur/CIO, manajer dan responden mengisi kuesioner yang tersedia dan kemudian menganalisis data. Proses akuisisi data dapat dilihat pada Gambar 2.



Gambar 3. Alur Pengumpulan Data

A. Metode Penghitungan Data

Survei tersebut menggunakan skala Guttman, yaitu skala pengukuran dengan jawaban pasti "ya dan tidak". Selain itu, dari enam komponen di atas, aspek DiFRI dievaluasi secara keseluruhan untuk menentukan Digital Forensic Readiness Index organisasi. Untuk contoh kuesioner pengukuran DiFRI, lihat ndic 1 (Novita & Yuliani, 2019).

Tabel 1. Rancangan kuesioner

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

Kuesioner Pengukuran DiFRI Komponen No	Indikator	Jawaban	
1	Xxx	Ada	Tidak

Kuesioner Ndic 3.1 kemudian dihitung untuk jawaban "ya" dan "tidak" dan kemudian diberi skor untuk setiap area menggunakan rumus. Hasil evaluasi masing-masing komponen tersebut dan DiFRI disajikan pada bagian 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 diperkirakan berdasarkan nilai setiap komponen untuk sampai pada rumus DiFRI, yaitu:

DiFRI = 1/6 indeks komponen strategis
+ 1/6 Indeks Komponen Kebijakan dan Prosedur
+ 1/6 indeks komponen teknologi dan keamanan informasi
+ 1/6 indeks komponen respon forensik digital
+ 1/6 indeks komponen kontrol
+ 1/6 indeks komponen legal

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

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

IA adalah indeks dari masing-masing aspek, kemudian A adalah jumlah indikator dengan nilai "ada" dan nA adalah jumlah indikator untuk komponen tersebut. Karena nilai eksak dari indeks selalu $0 \leq \mathrm{IA} \leq 1$, digunakan perkalian dengan 10, yang tujuannya adalah untuk mendapatkan skala 0–10.

KESIMPULAN

Berdasarkan tinjauan pustaka dari beberapa penelitian sebelumnya, dapat disimpulkan bahwa: Model DiFRI terdiri dari beberapa komponen yaitu strategi, kebijakan dan prosedur, teknologi dan keamanan, respon forensik digital, kontrol dan hukum. Model DiFRI memberikan output berupa indeks
Indeks DiFRI menunjukkan kesiapan institusi untuk mencegah dan memerangi kejahatan dunia maya

DAFTAR PUSTAKA

Barske, David, Stander, Adrie, & Jordaan, Jason. (2010). A digital forensic readiness framework for South African SME's. *2010 Information Security for South Africa*, 1–6. IEEE.

Grobler, Cornelia P., & Louwrens, C. P. (2007). Digital forensic readiness as a component of information security best practice. *New Approaches for Security, Privacy and Trust in Complex Environments: Proceedings of the IFIP TC-11 22 Nd International Information Security Conference (SEC 2007), 14–16 May 2007, Sandton, South Africa 22*, 13–24. Springer.

Nasiroh, Siti, & Romahon, Rizki Akbar. (2021). Analysis Of Digital Forensic Readiness Index (DIFRI) On Cybercrime Response Using Statistical Methods. *Perwira Journal of Science & Engineering*, *1*(1), 34–41.

Novita, Diana, & Yuliani, Nafisah. (2019). Analisis Customer Satisfaction Pada Transportasi Online Berbasis Android Dengan Menggunakan Metode BLACKBOX Customer. *Ikraith-Informatika*, *3*(2), 76–89.

Rowlingson, Robert. (2004). A ten step process for forensic readiness. *International*

Journal of Digital Evidence, *2*(3), 1–28.
Symantec, Norton. (2012). *2012 Norton Cybercrime Report*. Retrieved from https://biz-file.com/f/1311/2012_Norton_Cybercrime_Report_.pdf
Tan, John. (2001). Forensic readiness. *Cambridge, MA:@ Stake*, *1*.
Widodo, Tri. (2016). Pengembangan Model Digital Forensic Readiness Index (DiFRI) Untuk Mencegah Kejahatan Dunia Maya. *JISKA (Jurnal Informatika Sunan Kalijaga)*, *1*(1), 41–46.