CyberSecurity dan Forensik Digital e-ISSN: 2615-8442
Vol. 4, No. 1, Mei 2021, hlm. 18-23

DIGITAL FORENSIC READINES INDEX (DiFRI) UNTUK MENGUKUR KESIAPAN PENANGGULANGAN CYBERCRIME PADA KANTOR WILAYAH KEMENTERIAN HUKUM DAN HAM DIY

Taufiq Effendy Wijatmoko

Kantor Wilayah Kementerian Hukum dan HAM Daerah Istimewa Yogyakarta
Email: taufiq.ew@gmail.ac.id

(Naskah masuk: 14 Desember 2020, diterima untuk diterbitkan: 31 Mei 2021)

Abstrak

Kantor Wilayah Kementerian Hukum dan HAM DIY dalam pelaksanaan tugas pemerintahannya dibantu dengan Teknologi Informasi dalam bingkai *e-government* berdasarkan suatu tata kelola pemerintahan yang baik (*Good Corporate Governance*). Pengelolaan informasi, termasuk kualitas dan keamanan pengelolaan informasi , merupakan salah satu aspek dalam *Good Corporate Governance*. Pemanfaatan teknologi informasi pada instansi pemerintah (*e-Government*) ibarat dua sisi mata uang. Pada satu sisi memberikan manfaat luar biasa bagi akselerasi tugas pemerintahan, namun pada sisi lain dapat menimbulkan potensi *cybercrime*. Kurangnya pemahaman masyarakat terhadap *cybercrime* dan barang bukti digital terindikasi pada minimnya kesadaran akan laporan tindak kejahatan internet dan barang bukti digital. Dengan kata lain ini menunjukkan rendahnya kesiapan dari berbagai instansi dalam mengantisipasi dan mendokumentasikan pada instansi pemerintah dalam menghadapi *cybercrime* atau yang sering disebut disebut dengan *digital forensic readiness*. Penelitian ini memiliki tujuan untuk mengetahui kesiapan Kantor Wilayah Kementerian Hukum dan Hak Asasi Manusia DIY dalam menanggulangi kejahatan pada dunia masya *cybercrime* dan diharapkan dapat melakukan perbaikan yang fokus dan tepat pada sasaran. Hasil penelitian ini diperoleh melalui data kuisioner pada Kantor Wilayah Kementerian Hukum dan Hak Asasi Manusia DIY yang kemudian di analisis dengan metode statistik. Hasil penelitian memberikan informasi bahwa pada aspek *Strategy* mendapatkan indeks sebesar 5,00 (Cukup Siap), aspek *Policy & Procedure* memperoleh indeks sebesar 5,93 (Cukup Siap), aspek *Technology & Security* sebesar 7,62 (Siap), aspek *Digital Forensic Response* sebesar 4,44 (Cukup Siap), dan aspek *Control* sebesar 3,65 (Kurang Siap). Maka indeks keseluruhan DiFRI pada Kantor Wilayah Kementerian Hukum dan HAM DIY yaitu 5,33 dengan kata lain Kanwil Kemenkumham DIY cukup siap dalam menghadapi *cybercrime* dan direkomendasikan untuk terus melakukan perbaikan dan pembaharuan untuk mengurangi dampak cybercrime dalam rangka melindungsi aset data dan informasi instansi pemerintah.

Kata kunci: *Forensika digital, DiFRI, Cyber Security, e-government.*

DIGITAL FORENSIC READINES INDEX (DiFRI) TO MEASURE READINESS TO TREAT CYBERCRIME IN THE MINISTRY OF LAW AND HUMAN RIGHT DIY

Abstract

The Regional Office of the Ministry of Law and Human Rights in Yogyakarta in carrying out its governmental duties is assisted by Information Technology in the framework of e-government based on a good governance (Good Corporate Governance). Information management, including quality and information management, is one aspect of Good Corporate Governance. The use of information technology in government agencies (e-Government) is like two sides of a coin. On the one hand, it provides tremendous benefits for government acceleration, but on the other hand it can create the potential for cybercrime. The lack of public understanding of cybercrime and digital evidence is indicated by the lack of awareness of internet crime reports and digital evidence. In other words, this shows the low readiness of various agencies in anticipating and documenting government agencies in dealing with cyber crime or what is often referred to as digital forensic readiness. This study aims to see the readiness of the Yogyakarta Regional Office of the Ministry of Law and Human Rights in tackling crimes in the world of cybercrime and is expected to make improvements that are focused and on target. The results of the study were obtained through a data questionnaire at the Yogyakarta Regional Office of the Ministry of Law and Human Rights which was then analyzed by statistical methods. The results provide information that the Strategy aspect gets an index of 5.00 (Quite Ready), the Policy & Procedure aspect gets an index of 5.93 (Quite Ready), the Technology & Security aspect is 7.62 (Ready), the Digital Forensic Response

aspect amounting to 4.44 (Quite Ready), and the Control aspect of 3.65 (Not Ready). So the overall index of DiFRI at the Ministry of Law and Human Rights DIY is 5.33, in other words the Ministry of Law and Human Rights DIY is quite ready to face cybercrime and it is recommended to make improvements and updates to reduce the impact of cybercrime in order to protect data and information assets of government agencies.

Keywords: *Digital Forensics, DiFRI, Cyber Security, e-government*

1. PENDAHULUAN

Kemajuan Teknologi Informasi dan Komputer (TIK) telah mengalami peningkatan yang sangat pesat, khususnya setelah ditemukannya teknologi *networking* yang menghubungkan antar komputer melalui Internet. Berbagai kemajuan TIK tersebut diikuti pula dengan berkembangnya sisi lain dari teknologi yang mengarah pada *cybercrime*. *Cybercrime* dapat diartikan sebagai penggunaan komputer sebagai alat untuk melakukan berbagai modus kejahatan.

Berbagai permasalahan dan dampak negatif telah timbul akibat oleh penggunaan komputer untuk kepentingan berbagai modus kejahatan. Dampak yang muncul secara makro yang berdampak pada wilayah komunal, publik, serta memiliki efek domino yang luas maupun secara mikro yang dampaknya hanya pada tingkatan personal/perseorangan. Pada beberapa negara telah dibentuk unit khusus yang bertugas menindak kejahatan khususnya yang terkait dengan permasalahan *cybercrime*.

Sebuah Organisasi harus siap secara Forensik Digital untuk memaksimalkan potensi mereka dalam merespon peristiwa Cyber Crime dan dapat dengan tepat menunjukkan identifikasi faktor-faktor yang berkontribusi terhadap kesiapan Forensik Digital serta bagaimana faktor-faktor ini bekerja bersama untuk mencapai kesiapan Forensik Digital dalam suatu organisasi.

Diperlukan adanya suatu standar yang sistemik untuk menentukan seberapa siap suatu instansi pemerintah dalam melakukan Forensik Digital, meskipun Digital Forensik telah berkembang saat ini dalam menyelesaikan kasus-kasus Cyber Crime seperti carding, hacking, cracking, defacing, phising, spamming serta kejahatan lainnya yang berbasis digital.

Penelitian berkaitan tentang kesiapan suatu instansi pemerintah masih sangat jarang. Oleh karen itu perlu untuk dilakukan suatu penelitian supaya bisa mengidentifikasi faktor-faktor yang berkontribusi terhadap kesiapan Forensik Digital yang bisa diukur dan setelah dihitung akan menghasilkan sebuah nilai yang disebut Digital Forensic Readiness Index (DiFRI).

2. TINJAUAN PUSTAKA

2.1. Digital Forensic

Digital forensic dapat diartikan sebagai penggunaan ilmu dan metode untuk menemukan, pengumpulkan, mengamankan, menganalisis, menginterpretasi dan mempresentasikan barang bukti digital dalam rangka kepentingan rekontruksi kejadian serta memastikan keabsahan pada proses peradilan (Prayudi and Ashari, 2015). *Digital forensic* mencakup pengujian terhadap bukti digital dengan analisis forensik yang dilakukan oleh Law Enforcement Agencies (LEA). Tujuan utama dari digital forensic adalah menemukan bukti-bukti digital yang akan digunakan oleh pengacara, LEA, dan kantor kejaksaan untuk dipresentasikan di pengadilan. (Kebande, Karie and Venter, 2016)

Forensik Digital merupakan rangkaian metode dari teknik dan prosedur untuk mendapatkan barang bukti digital dari peralatan komputer, berbagai media penyimpanan *storage* dan media digital yang dapat dipresentasikan saat proses di pengadilan dengan format yang dapat dipahami serta memiliki makna.

2.2. Digital Forensic Readiness (DFR)

Digital forensic readiness adalah kemampuan sebuah organisasi untuk memaksimalkan potensi instansi pemerintah dalam menggunakan barang bukti digital dan meminimalisir biaya investigasi yang dikeluarkan instansi. Digital Forensic Readiness memiliki tujuan, yaitu untuk memaksimalkan penggunaan data sebagai barang bukti ketika terjadi insiden dan meminimalisir biaya investigasi ketika merespon insiden.

Digital forensic readiness memiliki tujuan adalah :

a. Agar instansi pemerintah bisa memperoleh barang bukti secara legal tanpa mengganggu proses bisnis dari instansi.
b. Untuk memperoleh barang bukti yang mengarah pada tindak kriminal yang memiliki potensi memunculkan perselisihan.
c. Untuk melanjutkan proporsi pada insiden dengan mengijinkan investigasi computer forensic.
d. Untuk meminimalisir intrupsi pada bisnis dari berbagai investigasi
e. Untuk menjamin bahwa barang bukti memiliki dampak positif ketika dihasilkan dari berbagai aksi legal.

2.3. Model Digital Forensic Readiness

Lima komponen utama digital forensic readiness dalam model digital forensic readiness

menurut Barske et al dapat terlihat pada Gambar berikut :

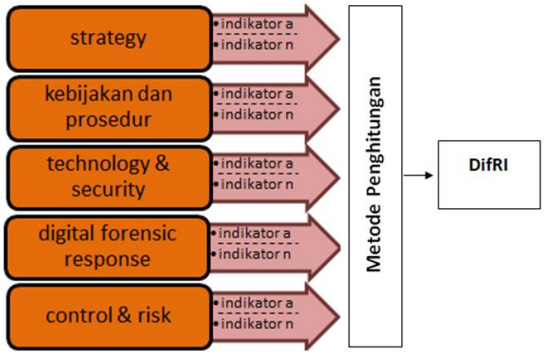
Gambar 1. Model Digital Forensic Readiness

Komponen-komponen tersebut Menurut Barske dkk adalah (Barske, Stander and Jordaan, 2010):

a. Strategi
   Merupakan keputusan untuk mengimplementasikan program *digital forensic readiness* harus menjadikan sebuah keputusan strategis bagi sebuah instansi pemerintah, dan harus dapat dipastikan bahwa *digital forensic readiness* adalah salah satu strategi penting yang berhubungan langsung bagi tujuan organisasi.
b. Kebijakan dan prosedur
   Sebuah instansi pemerintah memerlukan standar operasional prosedur dan kebijakan sebagai pedoman bagi pegawaii berkenaan pelaksanaan tugas sehari-hari. Dalam upaya memastikan *digital forensic readiness* berjalan baik dalam sebuah instansi, harus disiapkan kebijakan dan prosedur untuk memastikan pelaksanaanya.
c. Teknologi
   Instansi pemerintah dalam mengimplementasikan *digital forensic readiness* memerlukan implementasi software atau hardware sebagai pendukung proses *digital forensic*, seperti memperoleh barang bukti digital dan melakukan pengujian terhadap barang bukti digital tersebut.
d. Respon digital forensic
   Dalam upaya menangani dan menindak berbagai isu terkait tindakan *Cybercrime*, investigasi kriminal, perbaikan insiden keamanan komputer dan mendukung setiap proses *digital forensic* dibutuhkan *Digital Forensic Response.*
e. Pelaksanaan dan pengawasan
   Monitoring dan pengawasan program *digital forensic readiness* harus selalu dilaksanakan dengan kontinu dan terus-menerus. Instansi diharapkan mampu menangani resiko ketika terjadi *failure* program *digital forensic readiness*. Semua dapat tercapai ketika semua pegawai dalam sebuah instansi pemerintah memiliki pengetahuan akan kebijakan-kebijakan dan prosedur yang dilaksanakan sesuai peraturan yang berlaku.

2.4. Model Digital Forensic Readiness Index

Dilakukan pendalaman lebih lanjut untuk merumuskan model Digital Forensic Readiness Index (DiFRI) berdasarkan komponen-komponen yang telah dirumuskan.



Gambar 2. Model DiFRI

Selanjutnya masing-masing komponen dipecah menjadi beberapa indikator yang memberikan informasi/ deskripsi lebih detil dari komponen utama. Adapun detail indikator masing-masing komponen tersebut adalah

a. Komponen Strategi
   Indikator Komponen Strategi yaitu :
   - Identifikasi teknologi dan Sumber Daya manusia untuk menjamin Digital Forensic Readiness
   - Jaminan ketersediaan biaya dan anggaran untuk mengimplenetasikan dan *maintenance* program Digital Forensic Readiness
   - Identifikasi sumber-sumber dan tipe-tipe yang berbeda dari barang bukti digital organisasi
   - Aturan, regulasi dan kewajiban menyimpan dokumen, file dan rekaman (CCTV, Log, dokumen)
   - Program-program Digital Forensic Readiness
   - Ketentuan ketika terjadi peristiwa yang membutuhkan barang bukti digital
b. Komponen Policy & Procedure
   Indikator komponen Policy & Procedure antara lain :
   - Kebijakan dalam keadaan bagaimanakah barang bukti digital dapat diamankan
   - Kebijakan pembagian wewenang, tugas dan tanggungjawab terkait pengumpulan barang bukti digital, pemeliharaan dan pemeriksaanya
   - Sanksi/ hukuman bagi pelanggar kebijakan dan prosedur Digital Forensic Readiness

- Kebijakan bahwa semua sumber daya informasi dan data merupakan milik organisasi
- Kebijakan barang bukti digital apa saja yang harus diamankan
- Kebijakan dan prosedur sebagai petunjuk aktifitas dan kegiatan anggota organisasi yang mengunakan TIK
- Kebijakan yang menyatakan cara dan situasi ketika bukti-bukti yang telah diamankan oleh organisasi dapat dilepaskan kepada pihak di luar instansi, termasuk ketika harus dirujuk ke penegak hukum

c. Komponen Technology & Security
Indikator komponen Technoloy & Security antara lain :
- Ketersediaan perangkat pendukung keamanan seperti enkripsi dan kriptografi
- Jaminan keamanan barang bukti, baik secara online maupun offline, melalui imaging maupun penggandaan fisik
- Ketersediaan perangkat akuisisi dan analisis barang bukti digital, baik berupa hardware (write block protector, dll) maupun software (*analisys tool*)
- Manajemen media penyimpanan (CD, hardisk, falshdisk) dari masing-masing komputer dan server
- Ketersediaan perangkat pendukung digital forensic seperti cctv, finger print, dan autentikasi sistem
- Jaminan manajemen log dari masing-masing sistem, pemeliharaan, dan pengelolaan
- Ketersediaan perangkat pengamanan sistem seperti firewall, anti virus

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

e. Komponen Control & Risk
Indikator komponen Control & Risk antara lain :
- Sosialisasi program digital forensic kepada anggota organisasi
- Pembaharuan perangkat, tool, dan sistem secara berkala
- Pengawasan program Digital Forensic Readiness
- Evaluasi secara berkala program Digital Forensic Readiness
- Pemahaman pada anggota setiap proses digital forensic dan resiko kegagalan setiap proses
- Pembahasan hasil investigasi maupun publikasi hasil investigasi kepada kepala-kepala departemen/sub bagian

3. METODOLOGI PENELITIAN

Penelitian ini masuk dalam jenis penelitian evaluatif yang memuat tentang kesiapan instansi pemerintah dalam penerapan tata kelola keamanan informasi dengan menggunakan metode penelitian kualitatif. Penelitian ini memiliki tujuan untuk menghasilkan sebuah rekomendasi terkait dengan tata kelola keamanan informasi pada Kantor Wilayah kementerian Hukum dan HAM DIY.

Berikut adalah gambaran penjelasan masing-masing langkah penelitian secara sistematis sebagai berikut:

- Langkah pertama, mendefinisikan rumusan masalah serta tinjauan literatur. Langkah ini termasuk di dalamnya mempelajari berbagai teori terkait termasuk di dalamnya adalah teori untuk menelaah kesiapan instansi Kantor Wilayah Kementerian Hukum dan HAM DIY dalam menanggulangi *cybercrime*.
- Langkah kedua, pengumpulan data dan analisa data. Setelah didapatkan model pengkajian yang sesuai, selanjutnya adalah dilakukan pengumpulan data berikut analisa data untuk memperoleh informasi yang valid tentang kesiapan tata kelola keamanan informasi pada Kanwil Kemenkumham DIY.

Dalam melaksanakan penelitian ini, untuk mendapatkan data dilakukan melalui penyebaran kuesioner. Kuesioner tersebut merupakan model Digital Forensic Readiness Index (DiFRI) yang telah disusun sebelumnya. Setiap pegawai yang berkaitan dengan Teknologi Informasi akan mengisi kuesioner DiFRI yang telah disusun, langkah selanjutnya adalah dilakukan analisis pada data hasil kuisioner tersebut. Dalam penelitian ini populasi yang digunakan adalah sebanyak 9 (sembilan) orang pegawai Kantor Wilayah Kementerian Hukum dan HAM DIY yang terdiri dari Pelaksana, Pejabat Fungsional Pranata Komputer, Pejabat Pengawas, dan Pejabat Administrator bidang Teknologi Informasi.

Metode analisis data dan interpretasi data yang digunakan adalah metode analisis kualitatif. Pendekatan logika induktif digunakan dalam teknik

analisis ini, di mana penarikan kesimpulan disusun berdasarkan pada hal-hal tertentu atau data di lapangan yang menghasilkan pada kesimpulan-kesimpulan umum. Analisis data kualitatif merupakan langkah yang dilakukan dengan cara mengorganisasikan data dengan memilah-milahnya menjadi satuan yang dapat dikelola kemudian mensintesanya (Bogdan & Biklen, 1982). Selanjutnya berdasarkan hasil dari proses tersebut, akan didapatkan informasi apa yang penting dan informasi apa yang dapat dipelajari untuk menunjang pengambilan keputusan. Penelitian ini dilakukan di Kantor Wilayah Kementerian Hukum dan HAM D.I. Yogyakarta.

3.1. Metode Penghitungan Data

Skala yang digunakan pada kuisioner adalah skala Guttman, yang merupakan skala pengukuran dengan jawaban yang tegas, antara "ada" dan "tidak". Selanjutnya, *Digital Forensic Readiness Index* Kanwil Kemenkumham DIY dapat diketahui setelah dilakukan *scoring* untuk menilai aspek DiFRI secara keseluruhan pada lima komponen.

Dilakukan penghitungan atas jawaban "Ada" dan "Tidak" dari hasil kuisioner, selanjutnya pada masing-masing aspek dilakukan scoring dengan menggunakan rumus :

$$I_A = \frac{\sum_{k=1}^{n} A}{n_A} . 10 \quad (1)$$

I_A adalah indeks dari masing-masing aspek, selanjutnya A adalah jumlah indikator yang bernilai "ada", dan nA merupakan total dari indikator pada aspek tersebut, sedangkan perkalian 10, diharapkan agar didapatkan skala dari 0 sampai dengan 10.

Scoring keseluruhan dari Digital Forensic Readiness Index yaitu dengan menggunakan rumus :

$$I_{el} = \frac{\sum_{k=1}^{n} Ael}{n_{el}} . 10 \quad (2)$$

Indeks dari seluruh komponen disimbolkan dengan I_{el}, selanjutnya A*el* adalah jumlah indikator yang bernilai "ada", dan n_{el} adalah total dari seluruh indikator, sedangkan perkalian 10, dimaksudkan untuk mendapatkan skala dari 0 sampai dengan 10. Dapat juga dipakai rumus :

$$I_{total} = \frac{\sum_{k=1}^{n} I_A}{n_{I_A}} \quad (3)$$

Indeks DiFRI keseluruhan komponen disimbolkan dengan I_{total}, sedangkan I_A adalah indeks masing-masing komponen, dan banyaknya komponen menjadi pembaginya.

3.2. Skala Tingkat DiFRI

Skala dan status untuk masing-masing nilai DiFRI (i) digunakan untuk memberikan rekomendasi dan kejelasan status instansi. Peneliti menyusun lima kriteria berdasarkan skala tertentu, seperti yang ditampilkan pada Tabel berikut :

Tabel 1. Tabel Skala Kesiapan Instansi DiFRI

No	Range/ Skala	Status
1.	$8 < i \leq 10$	Sangat Siap
2.	$6 < i \leq 8$	Siap
3.	$4 < i \leq 6$	Cukup Siap
4.	$2 < i \leq 4$	Kurang Siap
5.	$0 \leq i \leq 2$	Tidak Siap

4. HASIL DAN PEMBAHASAN

4.1. Hasil Perhitungan DiFRI

Digital Forensic Readiness Index bisa dihitung melalui masing-masing variabel, tetapi bisa juga dihitung secara keseluruhan/ secara langsung dari semua variabel. Berikut merupakan rincian DiFRI :

Tabel 2. Tabel Skala Kesiapan Instansi DiFRI

No	Komponen	Indeks
1.	Strategy	5,00
2.	Policy & Procedure	5,93
3.	Technology & Security	7,62
4.	Digital Forensic Response	4,44
5.	Control & Risk	3,65
DiFRI		5,33

Berdasarkan hasil penghitungan rumus dari persamaan (1), untuk variabel *Strategy* diperoleh DiFRI yaitu 5,00. Sehingga dari sisi Strategy Kanwil Kementerian Hukum dan HAM DIY dapat dikatakan Cukup Siap.

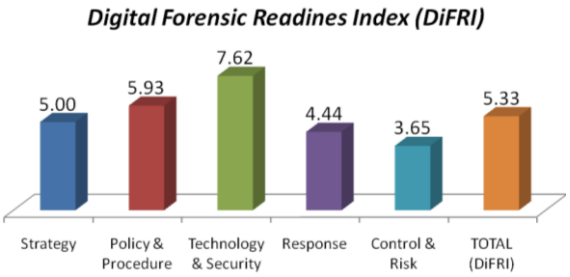
Langkah selanjutnya, dengan menggunakan persamaan (1), untuk variabel *Policy & Procedure* diperoleh DiFRI yaitu 5,93. Sehingga secara Policy & Procedure Kanwil Kementerian Hukum dan HAM DIY dapat dikatakan Cukup Siap.

Kemudian, dengan menggunakan persamaan (1), untuk variabel *Technology & Security* diperoleh DiFRI yaitu 7,62. Sehingga dari segi Technology & Security Kanwil Kementerian Hukum dan HAM DIY dapat dikatakan Siap.

Sedangkan untuk variabel *Response* didapatkan DiFRI 4,44. Sehingga secara dari segi respon terhadap forensik digital pada Kanwil Kementerian Hukum dan HAM DIY dapat dikatakan Cukup Siap.

Hasil penghitungan menggunakan persamaan (1) didapat indeks untuk *Control & Risk* yaitu 3,65. Dapat dimaknai bahwa dari segi Pengawasan dan Manajemen Risiko Kanwil Kementerian Hukum dan HAM DIY Kurang Siap

Hasil penghitungan dengan persamaan diatas, nilai indeks DiFRI yang diperoleh dari keseluruhan komponen-komponen utama pada model ini yaitu 5,33. Maka, dengan indeks tersebut dapat dikatakan bahwa Kanwil Kementerian Hukum dan HAM DIY Cukup Siap dalam menghadapi digital forensic.



Gambar 3. Nilai Indeks DiFRI

4.2. Analisa Model DiFRI

Berdasarkan kompilasi beberapa penelitian, penerapan dan pembahasan tentang model DiFRI serta pengembangan dari model DiFRI yang dikemukakan (Widodo and Prayudi, 2013), diperoleh beberapa hal yang dapat dicermati dan dianalisa dari pengembangan model DiFRI pada implementasi e-government :

- Untuk dapat menerapkan e-government secara optimal instansi pemerintah memerlukan suatu kebijakan mengenai *handling incident* terkait kejadian *digital forensic*, agar aktifitas kerja serta layanan publik yang berjalan tidak terhambat maupun menyebabkan kerugian bagi organisasi, stakeholder terkait serta bagi para pengguna layanan publik.
- Suatu instansi pemerintah memerlukan suatu alat (teknologi) beserta sumber daya manusia (SDM) yang kompeten terkait pencegahan maupun penanganan kejadian *forensic digital* agar file maupun data yang akan dijadikan sebagai barang digital dapat aman dan dapat secara legal dijadikan bukti yang sah di depan hukum.

5. KESIMPULAN

Berdasarkan penelitian yang dilakukan, kesimpulan yang dapat diperoleh terkait penilaian kesiapan menghadapi *cyber crime* di Kantor Wilayah kementerian Hukum dan HAM DIY dengan menggunakan Indeks DiFRI adalah sebagai berikut:

a. Komponen/ variabel yang bisa dipakai guna mengembangkan *Digital Forensic Readiness Index* (DiFRI) terdiri atas lima komponen/ variabel, sebagai berikut :
   - Control & Risk
   - Policy & Procedure
   - Digital Forensic Response
   - Strategy
   - Technology & Security

b. Pada implementasi DiFRI di Kanwil Kementerian Hukum dan HAM D.I. Yogyakarta. Hasilnya Kanwil Kemenkumham DIY pada komponen Strategy mendapatkan indeks sebesar 5,00 (Cukup Siap), komponen Policy & Procedure memperoleh indeks sebesar 5,93 (Cukup Siap), variabel Technology & Security sebesar 7,62 (Siap), aspek Digital Forensic Response sebesar 4,44 (Cukup Siap), variabel Control sebesar 3,65 (Kurang Siap). Maka indeks keseluruhan DiFRI pada Kantor Wilayah Kementerian Hukum dan HAM DIY yaitu 5,33 (Cukup Siap).

c. Dengan memanfatkan Digital Forensic readiness Index (DiFRI), Kanwil Kemenkumham DIY bisa mempersiapkan instansi guna mengantisipasi, menangani dan menindaklanjuti Cyber Crime. Selain itu DiFRI juga bisa meningkatkan aspek kompetensi dan kapasitas Sumber Daya Manusia Teknologi Informasi sehingga akan berdampak pada peningkatan keamanan komputer dan Sistem Informasi serta meningktkanya ketersediaan dan jumlah barang bukti digital.

DAFTAR PUSTAKA

BARSKE, D., STANDER, A. and JORDAAN, J. (2010) ‘A digital forensic readiness framework for South African SME’s’, *Proceedings of the 2010 Information Security for South Africa Conference, ISSA 2010*, (September 2010). doi: 10.1109/ISSA.2010.5588281.

KEBANDE, V. R., KARIE, N. M. and VENTER, H. S. (2016) ‘A generic Digital Forensic Readiness model for BYOD using honeypot technology’, *2016 IST-Africa Conference, IST-Africa 2016*, (September 2018). doi: 10.1109/ISTAFRICA.2016.7530590.

PRAYUDI, Y. and ASHARI, A. (2015) ‘A Study on Secure Communication for Digital Forensics Environment’, *International Journal of Scientific and Engineering Research*, 6(1), pp. 1036–1043. doi: 10.14299/ijser.2015.01.010.

WIDODO, T. and PRAYUDI, Y. (2013) ‘MODEL DIGITAL FORENSIC READINESS INDEX (DiFRI) UNTUK MENGUKUR TIGKAT KESIAPAN INSTITUSI Magister Teknik Informatika Universitas Islam Indonesia (UII)’.