CyberSecurity dan Forensik Digital e-ISSN: 2615-8442
Vol. 3, No. 2, November 2020, hlm. 1-5

PEMBUATAN MODEL *DIGITAL FORENSIC READINESS INDEX (DiFRI)* TERHADAP SERANGAN *MALWARE*

Yogi Pratama[1], **Imam Riadi**[2], **Yudi Prayudi**[3]

[1,3]Program Studi Teknik Informatika, [2]Program Studi Sistem Informasi
[1,3]Universitas Islam Indonesia, [2]Universitas Ahmad Dahlan
Yogyakarta, Indonesia,
Email: [1]pratama.yogi09@gmail.com, [2]imam.riadi@is.uad.ac.id, [3]prayudi@uii.ac.id

(Naskah masuk: 02 Juli 2020, diterima untuk diterbitkan: 23 November 2020)

Abstrak

Semakin banyaknya jumlah *malware* yang tersebar di dunia saat ini, maka akan semakin banyak membuka peluang untuk melakukan tindak kejahatan, maka dibutuhkan kesiapan / *readiness* bagi setiap pengguna *internet* dalam menghadapi tindak kejahatan tersebut. Kesiapan menangani tindak kejahatan ini disebut *digital forensic readiness*. Oleh karena itu dibutuhkan sebuah model *digital forensic readiness* yang spesifik untuk mengukur tingkat kesiapan pengguna *internet* atau institusi dalam menghapai serangan *malware*. Model ini memiliki komponen utama yang digunakan untuk mengetahui atau menghitung tingkat kesiapan dari pengguna internet atau institusi, komponen utama tersebut adalah komponen *strategy*, komponen *policy & procedure*, komponen *technology & security*, komponen *digital forensic response*, komponen *control & legality*. Metode penghitungan yang digunakan dalam penelitian ini adalah Skala *Likert*, dengan metode ini maka akan diperoleh hasil yang lebih mendekati dengan keadaan sesungguhnya. Nilai / indeks tingkat kesiapan yang diperoleh akan memberikan rekomendasi-rekomendasi kepada pengguna internet dan rekomendasi-rekomendasi ini dapat digunakan untuk melakukan pembenahan secara baik dan tepat sasaran.

Kata kunci: *Malware, Digital Forensic, Digital Forensic Readiness, Digital Forensic Readiness Index*

MAKING OF DIGITAL FORENSIC READINESS INDEX (DiFRI) MODELS TO MALWARE ATTACKS

Abstract

The increasing number of malware spread in the world today, then there will be more opportunities to commit crime, so readiness is needed for every internet user in dealing with these crimes. The readiness to handle crime is called digital forensic readiness. Therefore, we need a specific digital forensic readiness model to measure the level of readiness of internet users or institutions in achieving malware attacks. This model has the main components used to determine or calculate the level of readiness of internet users or institutions, the main components are the strategy component, the policy & procedure component, the technology & security component, the digital forensic response component, the control & legality component. The calculation method used in this study is a Likert Scale, with this method the results will be obtained that are closer to the real situation. The value / index of readiness level obtained will provide recommendations to internet users and these recommendations can be used to make improvements properly and on target.

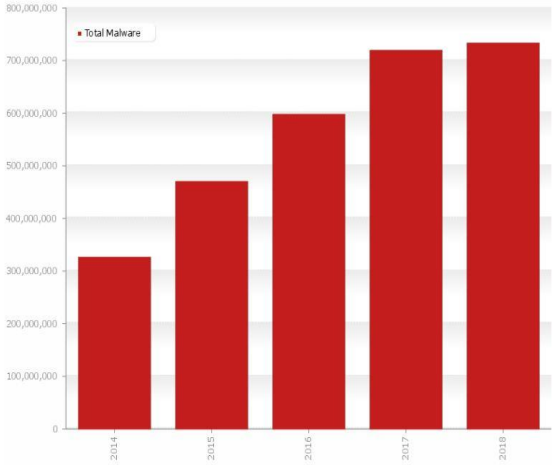
Keywords: *Malware, Digital Forensic, Digital Forensic Readiness, Digital Forensic Readiness Index*

1. PENDAHULUAN

Kejahatan yang terjadi saat ini makin meningkat pesat, berbagai cara dan modus operasi yang dilakukan oleh pelaku tindak kejahatan sangat bervariasi dan tidak mengenal para korbannya, hal ini dilakukan hanya berdasarkan pola kebiasaan masyarakat dan perkembangan tekonologi informasi yang terjadi di masyarakat itu sendiri. Kejahatan yang terjadi saat ini tidak lagi tentang perampokan, pencurian barang ataupun penipuan uang atau barang yang biasa dilakukan dengan kontak fisik atau kekerasan, melainkan dilakukan dengan memanfaatkan perkembangan yang sangat pesat di dunia teknologi informasi serta peralatan-peralatan elektronik yang memanfaatkan kemajuan teknologi

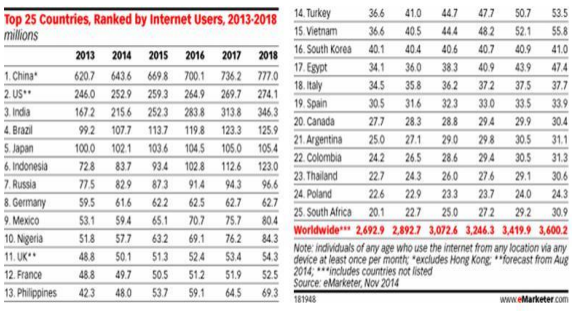
informasi, seperti *malware*, *virus*, *spam*, *hacking* dan penipuan atau pencurian lainnya.

Hal ini dapat dilihat berdasarkan penelitian yang dilakukan oleh AV-TEST (The Independent IT-Security Institute) tentang jumlah *malware* yang tersebar di seluruh dunia dalam 5 tahun terakhir dan menariknya jumlah *malware* tersebut setiap tahunnya meningkat. Data jumlah *malware* yang tersebar di seluruh dunia itu dapat di lihat pada Gambar 1



Gambar 1 Jumlah *Malware* dalam 5 tahun terakhir.
(Sumber : www.av-test.org, 2018)

Pada Gambar 1 menunjukkan bahwa dalam 5 tahun terjadi peningkatan yang sangat jelas dan signifikan jumlah *malware* yang tersebar di dunia teknologi informasi. Ini sangat jelas berbanding lurus dengan jumlah pengguna internet di Indonesia yang makin meningkat. Jumlah pengguna internet di Indonesia menurut survey yang dilakukan lembaga riset pasar e-Marketer yang dikutip dari website Kementerian Komunikasi dan Informatika Republik Indonesia berada di posisi nomor 6 dunia, dimana jumlah pengguna internet pada tahun 2017 mencapai 112,6 juta pengguna dan diperkirakan pada tahun 2018 mencapai 123 juta pengguna. Peningkatan tersebut dapat terlihat dari Gambar 2



Top 25 Countries, Ranked by Internet Users, 2013-2018
millions

	2013	2014	2015	2016	2017	2018
1. China*	620.7	643.6	669.8	700.1	736.2	777.0
2. US**	246.0	252.9	259.3	264.9	269.7	274.1
3. India	167.2	215.6	252.3	283.8	313.8	346.3
4. Brazil	99.2	107.7	113.7	119.8	123.3	125.9
5. Japan	100.0	102.1	103.6	104.5	105.0	105.4
6. Indonesia	72.8	83.7	93.4	102.8	112.6	123.0
7. Russia	77.5	82.9	87.3	91.4	94.3	96.6
8. Germany	59.5	61.6	62.2	62.5	62.7	62.7
9. Mexico	53.1	59.4	65.1	70.7	75.7	80.4
10. Nigeria	51.8	57.7	63.2	69.1	76.2	84.3
11. UK**	48.8	50.1	51.3	52.4	53.4	54.3
12. France	48.8	49.7	50.5	51.2	51.9	52.5
13. Philippines	42.3	48.0	53.7	59.1	64.5	69.3
14. Turkey	36.6	41.0	44.7	47.7	50.7	53.5
15. Vietnam	36.6	40.5	44.4	48.2	52.1	55.8
16. South Korea	40.1	40.4	40.6	40.7	40.9	41.0
17. Egypt	34.1	36.0	38.3	40.9	43.9	47.4
18. Italy	34.5	35.8	36.2	37.2	37.5	37.7
19. Spain	30.5	31.6	32.3	33.0	33.5	33.9
20. Canada	27.7	28.3	28.8	29.4	29.9	30.4
21. Argentina	25.0	27.1	29.0	29.8	30.5	31.1
22. Colombia	24.2	26.5	28.6	29.4	30.5	31.3
23. Thailand	22.7	24.3	26.0	27.6	29.1	30.6
24. Poland	22.6	22.9	23.3	23.7	24.0	24.3
25. South Africa	20.1	22.7	25.0	27.2	29.2	30.9
Worldwide* **	**2,692.9**	**2,892.7**	**3,072.6**	**3,246.3**	**3,419.9**	**3,600.2**

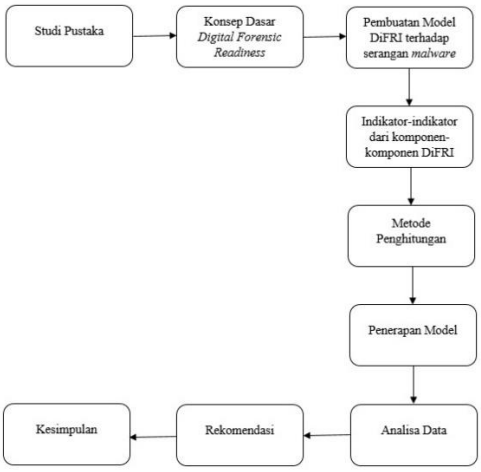
Note: individuals of any age who use the internet from any location via any device at least once per month; *excludes Hong Kong; **forecast from Aug 2014; ***includes countries not listed
Source: eMarketer, Nov 2014
181948
www.eMarketer.com

Gambar 2 Peringkat Jumlah Pengguna Internet di dunia.
(Sumber: www.kominfo.go.id).

Dengan semakin banyaknya jumlah *malware* yang tersebar di dunia saat ini, maka akan semakin banyak membuka peluang untuk melakukan tindak kejahatan, maka dibutuhkan kesiapan / *readiness* bagi setiap pengguna *internet* dalam menghadapi tindak kejahatan tersebut. Melihat fenomena tersebut dan berdasarkan penelitian-penelitian yang berkaitan dengan *readiness* / kesiapan atau dalam hal ini berkaitan dengan *digital forensic readiness* yang telah ditelaah, terutama seperti yang dipaparkan oleh (Widodo, 2016) dalam penelitiannya yang berjudul *Pengembangan Model Digital Forensic Readiness Index (DiFRI) untuk Mencegah Kejahatan Dunia Maya* yang mengukur kesiapan pengguna internet dalam hal ini sebuah institusi dalam menanggulangi *Cyber Crime* masih mencakup hal yang sangat luas dari kejahatan dunia maya dan tidak ditemukannya sebuah model *Digital Forensic Readiness Index (DiFRI)* yang spesifik atau khusus menangani serangan *malware*. Maka dibutuhkan sebuah pembuatan model *Digital Forensic Readiness Index (DiFRI)* yang lebih spesifik terhadap serangan *malware* berdasarkan model-model yang telah ada. Model ini nantinya akan diterapkan pada sebuah institusi untuk mengetahui tingkat kesiapan institusi tersebut dalam menghadapi serangan *malware*.

2. METODE PENELITIAN

Berdasarkan latar belakang yang sudah dituliskan pada bagian pendahuluan dan untuk menyelesaikan penelitian ini diperlukan beberapa metode, langkah atau tahapan. Bagian ini akan menjelaskan metode-metode yang dilakukan sehingga diketahui dengan jelas dan rinci tentang urutan langkah-langkah yang dibuat secara sistematis dan dapat dijadikan pedoman yang jelas dalam menyelesaikan penelitian ini, membuat analisis terhadap hasil penelitian, serta kesulitan-kesulitan yang dihadapi. Untuk lebih mudah dipahami, langkah-langkah tersebut telah diuraikan dan dapat dilihat pada Gambar 3**.**



Gambar 3. Metodologi Penelitian

Pada Gambar 3 terlihat penelitian ini diselesaikan melalui 6 tahapan, yaitu (1) Studi Pustaka; (2) Konsep Dasar *Digital Forensic Readiness* (DFR); (3)

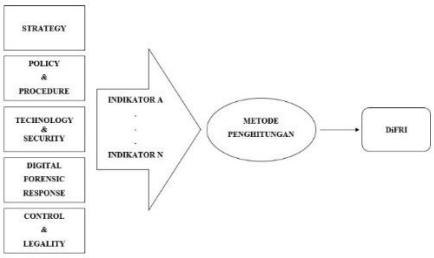
Pembuatan Model DiFRI terhadap serangan *Malware*; (4) Indikator-indikator dari komponen DiFRI; (5) Metode Penghitungan; (6) Penerapan Model; (7) Analisis Data; (8) Rekomendasi; (9) Kesimpulan.

3. KONSEP DASAR *DIGITAL FORENSIC READINESS*

Selanjutnya berdasarkan penelitian-penelitian sebelumnya dilakukan pengembangan terhadap model DiFRI agar sesuai untuk model DiFRI terhadap serangan *malware*. Hasil dari pengembangan model DiFRI terlihat dari komponen utama yang dimiliki. Pada model DiFRI terhadap serangan *malware* ini ada komponen utama yang digabung, yaitu komponen *control* dan *legality* karena komponen ini merupakan komponen yang sejalan dan saling terkait dan tak bisa dipisahkan, terutama untuk kasus serangan *malware*. Pada kasus serangan malware dibutuhkan pengawasan (*control*) atas resiko yang akan timbul sehingga pencegahan dan penanganan dapat berjalan dengan baik (Robert, 2004) (Barske dkk., 2010), dan juga dibutuhkan payung hukum yang jelas, agar dalam penanganan setiap data digital yang diperoleh bisa digunakan secara sah (*legality*) di mata hukum sebagai barang bukti (Robert, 2004) (Mouhtaropoulos & Li, 2014). Hal ini berdasarkan pengertian dari *malware* itu sendiri, yaitu sebuah program yang sengaja dibuat untuk membahayakan dan merugikan sistem operasi atau data pada komputer tanpa persetujuan pemilik komputer (Siddiqui dkk., 2008).

4. HASIL

Hasil dari penelitian ini adalah sebuah model *Digital Forensic Readiness Index (DiFRI)* terhadap serangan *malware* seperti yang dapat dilihat pada gambar 4.



Gambar 4. Model DiFRI terhadap serangan *malware.*

Kemudian dari setiap komponen-komponen utama dirumuskan menjadi indikator-indokator yang akan memberi gambaran / informasi lengkap dari komponen-komponen utamanya.

a. Komponen *Strategy*

Indikator-indikator dari komponen *strategy* adalah:

1. Program *digital forensic readiness.*
2. Aturan, regulasi dan kewajiban menyimpan dokumen dan rekaman (log, dokumen).
3. Ketentuan ketika terjadi peristiwa yang membutuhkan barang bukti digital.
4. Identifikasi sumber yang berbeda dari barang bukti digital.
5. Identifikasi teknologi dan sumber daya manusia untuk menjamin *digital forensic readiness*.

b. Komponen *Policy & Procedure*

Indikator-indikator dari komponen *policy & procedure* adalah:

1. Petunjuk atau prosedur aktifitas pegawai instansi dalam menggunakan TIK.
2. Mengetahui sangsi jika melanggar aturan dan prosedur dari *digital forensic readiness.*

c. Komponen *Technology & Security*

Indikator-indikator dari komponen *technology & security* adalah:

1. Jaminan manajemen log.
2. Manajemen media penyimpanan dari perangkat komputer.
3. Ketersediaan perangkat akuisisi analisis barang bukti digital, baik berupa *hardware* maupun *software*.
4. Jaminan keamanan barang bukti, baik secara *online* maupun *offline*.
5. Perangkat pendukung *digital forensic*.
6. Ketersediaan perangkat pengamanan sistem.
7. Ketersediaan perangkat pendukung keamanan.

d. Komponen *Digital Forensic Response*

Indikator-indikator dari komponen *digital forensic response* adalah:

1. SOP dalam penanganan insiden atau tindakan *digital forensic.*
2. Pegawai instansi yang memiliki sertifikasi/keahlian di bidang *digital forensic*.
3. Pelatihan-pelatihan bagi pegawai instansi mengenai penanganan serangan *malware* dan *digital forensic*.
4. Tim penanganan *malware* dan *digital forensic.*
5. Petunjuk teknis pengaduan maupun pelaporan insiden.
6. Pegawai instansi memiliki pengetahuan tentang bahaya *malware.*
7. Alat peraga, petunjuk dan arahan mengenai *malware* berupa poster, banner dan alat peraga lainnya.

e. Komponen *Control & Legality*

Indikator-indikator dari komponen *control & legality* adalah:

1. Sosialisasi tentang *digital forensic* kepada pegawai instansi.
2. Sosialisasi tentang bahaya *malware* kepada pegawai instansi.
3. Pengawasan program *digital forensic readiness*.
4. Pemahaman kepada setiap pegawai mengenai setiap proses *digital forensic* dan resiko kegagalan setiap prosesnya.
5. Pembaharuan perangkat, *tool* dan sistem secara berkala.
6. Kebijakan aspek hukum setiap proses investigasi *digital forensic*.
7. Pemahaman setiap pegawai instansi akan undang-undang ITE.
8. Sosialisasi peraturan dan undang-undang ITE.
9. Pelatihan penanganan terhadap serangan *malware* dan proses hukumnya.

4.1 METODE PENGHITUNGAN DATA

Pada penelitian ini data diperoleh dari kuesioner yang dibagikan dan dihitung menggunakan skala *likert*. Skala *likert* adalah skala yang bisa digunakan untuk mengukur persepsi atau pendapat seseorang mengenai sebuah peristiwa atau fenomena sosial. Skala ini dipilih karena memiliki interval dalam penilaiannya, hal ini akan membuat nilai yang diperoleh lebih mendekati dengan keadaan sesungguhnya sehingga pengguna internet dapat melakukan pembenahan dan perbaikan secara baik dan tepat sasaran. Berikut rancangan kuesioner pengukuran DiFRI seperti yang dapat dilihat pada tabel 1.

Tabel 1. Rancangan Kuesioner

Nama Institusi : …….
Jabatan : …….

1. Komponen *x*

No.	Indikator	SS	S	RG	TS	STS
1						
n						

Berdasarkan tabel 1 akan dilakukan penghitungan atas jawaban-jawaban yang diberikan, kemudian dilakukan *scoring* / penilaian pada setiap komponen dengan menggunakan skala *likert.* Hasil *scoring* / penilaian dapat dilihat pada tabel 2.

Tabel 2 *Scoring* setiap komponen

No	Indikator	Total Skor					Jumlah Total Skor	Indeks (%)
		SS	S	RG	TS	STS		
1								
n								
Indeks (%) Komponen								

Total skor untuk setiap jawaban dapat dihitung dengan rumus:

$$Total\ Skor = T \times Pn \quad (1)$$

Keterangan:
T : Jumlah responden.
Pn : Skor pilihan.

Jumlah Total Skor untuk setiap indikator dapat dihitung dengan rumus:

$$Jumlah\ Total\ Skor = \sum\ Total\ Skor\ Setiap\ Pilihan \quad (2)$$

Indeks (%) untuk setiao indikator dapat dihitung dengan rumus:

$$Indeks\ (\%)\ Indikator = \frac{Jumlah\ Total\ Skor}{Skor\ Maksimum} \times 100 \quad (3)$$

Keterangan:
Skor Maksimum : Nilai tertinggi pilihan dikali jumlah responden.

Indeks (%) setiap komponen dapat dihitung dengan rumus:

$$Indeks\ (\%)\ Komponen\ = \frac{\sum Indeks\ Indikator}{Jumlah\ Indikator} \quad (4)$$

Tabel 3. *Scoring* DiFRI

No.	Komponen	Indeks (%)
1		
n		
Nilai DiFRI (%)		

DiFRI akan dihitung berdasarkan besar nilai dari setiap komponen-komponen yang dimiliki, sehingga dapat dirumuskan:

$$DiFRI = \frac{Jumlah\ Indeks\ Semua\ Komponen}{Jumlah\ Komponen} \quad (5)$$

Selanjutnya peneliti membuat skala dan status dari hasil nilai DiFRI (d) yang diperoleh. Hal ini untuk memperjelas hasil dari kesiapan para penggunan *internet*. Peneliti membuat 3 kriteria berdasarkan skala tertentu seperti dapat dilihat pada tabel 4.

Tabel 4. Skala Kesiapan berdasarkan DIFRI

No.	Skala	Status
1.	0% < d ≤ 30%	Tidak Siap
2.	31% < d ≤ 60%	Kurang Siap
3.	61% < d ≤ 100%	Siap

5. KESIMPULAN

Berdasarkan studi pustaka dari beberapa penelitian terdahulu, dapat disimpulkan jika model DiFRI terhadap serangan *malware* ini memiliki 5 komponen utama, yaitu komponen *strategy*, komponen *policy & procedure*, komponen *technology & security*, komponen *digital forensic*

response, komponen *control & legality*. Model DiFRI ini menghasilkan nilai / indeks yang mencerminkan tingkat kesiapan dari pengguna internet atau institusi dalam menghadapai serangan *malware* dan memberikan rekomendasi - rekomendasi kepada penggunan internet atau institusi untuk melakukan pembenahan secara baik dan tepat sasaran.

DAFTAR PUSTAKA

ALAMSYAH, R. (2009). Teknik Forensik Meneliti Bukti Digital. Retrieved March 5, 2018, from http://www.perspektifbaru.com/wawancara/708 pada 16 Oktober 2009.05

BARSKE, D., STANDER, A., & 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*. https://doi.org/10.1109/ISSA.2010.5588281

ELYAS, M., AHMAD, A., MAYNARD, S. B., & LONIE, A. (2015). Digital forensic readiness: Expert perspectives on a theoretical framework. *Computers and Security*, *52*, 70–89. https://doi.org/10.1016/j.cose.2015.04.003

GROBLER B., T. AND L. (2007). Digital Forensic Readiness as a Component of Information Security Best Practice. *IFIP International Federation for Information Processing*, *232*, 13.

MARCELLA, A. J., & GREENFIELD, R. S. (2002). "Cyber Forensics a field manual for collecting, examining and preserving evidence of computer crimes", by CRC Press LLC, United States of America.

MOUHTAROPOULOS, A., & LI, C. (2014). Digital Forensic Readiness : Are We There Yet ?, *1*(3), 173–179.

PALMER, G. (2001). the first Digital Forensic Research Workshop. *The First Digital Forensic Research Workshop (DFRWS)*, (1), 15–18. https://doi.org/10.1111/j.1365-2656.2005.01025.x

REAVIS, J. (2012). The Ongoing Malware Threat: How Malware Infects Websites and Harms Businesses — and What You Can Do to Stop It. *Symantec*, 11. Retrieved from https://www.geotrust.com/anti-malware-scan/malware-threat-white-paper.pdf

ROWLINGSON, R. (2004). A Ten Step Process for Forensic Readiness. International Journal of Digital Evidence, Volume 2, Issue 3. https://www.utica.edu/academic/institutes/ecii/publications/articles/A0B13342-B4E0-1F6A-156F501C49CF5F51.pdf

ONYEMAUCHE, U.C. NWOSU, Q.N. & MBANUSI, C.E. (2015). A Conceptual Framework on Digital Forensics Readiness for Criminals Tracking: Data Reduction Modalities. http://www.ijritcc.org

KEBANDE, V.R. KARIE, N.M. & VENTER, H.S. (2016). Generic Digital Forensic Readiness Model for BYOD using Honeypot Technology.

PARK, S. KIM, Y. PARK, G. NA, O. & CHANG, H. (2018). Research on Digital Forensic Readiness Design in a Cloud Computing-Based Smart Work Environment.

SIDDIQUI, M., C., MORGAN WANG A. (2008). Data Mining Methods For Malware Detection. *Electronic Theses and Dissertations, 2004-2019*. 3709. https://stars.library.ucf.edu/etd/3709