Perwira Journal of Science and Engineering (PJSE)
E-ISSN : 2775-8486
Volume 1 Nomor 1
Februari 2021

ANALYSIS OF DIGITAL FORENSIC READINESS INDEX (DIFRI) ON CYBERCRIME RESPONSE USING STATISTICAL METHODS

Siti Nasiroh[1], Rizki Akbar Romahon[2]
Universitas Perwira Purbalingga[1,2]
nasiroh.pwt@gmail.com

Abstrak

Semakin berkembangnya peralatan teknologi informasi maupun elektronik karena meningkatnya kejahatan *cybercrime*, tapi tidak diimbangi dengan jumlah barang bukti yang tersedia. Kurangnya kesadaran akan laporan tindak kejahatan internet dan barang bukti digital, mengindikasikan kurangnya pemahaman masyarakat akan *cybercrime* dan barang bukti digital dan minimnya barang bukti digital mengindikasikan kurangnya kesiapan dari berbagai lembaga atau instansi dalam mengantisipasi dan mendokumentasikan pada instansi/lembaga dalam menghadapi *cybercrime* disebut dengan *digital forensic readiness*. Tujuan penelitian ini untuk mengetahui kesiapan institusi/lembaga dalam menghadapi *cybercrime* dan diharapkan dapat melakukan perbaikan dan pembenahan tepat sasaran. Penelitian ini diperoleh melalui data kuisioner pada instansi pemerintah yang kemudian di analisis dengan metode statistik. Hasil pengujian kuisioner dilakukan dengan uji validitas dan uji reabilitas. Hasil penelitian menunjukkan instansi pemerintah *belum siap* menghadapi *cybercrime* dan diharapkan melakukan pembenahan dan perbaikan secara tepat sasaran agar dimasa mendatang sudah siap dalam menghadapi tindak kejahatan dunia maya yang disebabkan perkembangan teknologi yang semakin canggih.

Kata kunci : *cybercrime, Digital Forensic Readines Index (DiFRI), SPSS*

Abstract

The development of information and electronic technology equipment is growing due to the increasing crime of cybercrime, but it's not balanced with the amount of evidence available. Lack of awareness of reports of internet crime and digital evidence, indicating a lack of public understanding of cybercrime and digital evidence and the lack of digital evidence indicates a lack of readiness from various institutions or agencies in anticipating and documenting agencies / institutions in dealing with cybercrime called digital forensic readiness. The purpose of this study is to determine the readiness of institutions / institutions in dealing with cybercrime and are expected to be able to make improvements and improvements on target. This research was obtained through questionnaire data on government agencies which were then analyzed by statistical methods. The results of questionnaire testing were carried out with validity and reliability tests. The results of the study show that government agencies are not ready to face cybercrime and are expected to make improvements and correct targets so that in the future they are ready to deal with cyber crime caused by increasingly sophisticated technological developments.

Keywords : cybercrime, Digital Forensic Readines Index (DiFRI), SPSS

1. PENDAHULUAN

Kejahatan saat ini semakin canggih karena melibatkan teknologi informasi maupun peralatan elektronik. Setiap tahun diperkirakan 556 juta orang korban kejahatan internet pencurian/penipuan dan *hacking* (Symantec 2012). Dari sumber yang sama juga disebutkan bahwa motif kejahatan dunia maya yang dilakukan adalah 40% kejahatan dunia maya murni,

50% kejahatan dunia maya untuk tujuan tertentu seperti politik (ujaran kebencian), 3% perang cyber dan 7% mata-mata data informasi. Meningkatnya tindak kejahatan internet terlihat dari Pemaparandiatas, tingkat kejahatan tersebut tidak diimbangi dengan jumlah barang bukti yang tersedia. Muhammad Nuh Al Azhar, ketua Digital Forensic Analyst Team (DFAT) hadfex expo (Al Azhar. M.Nuh 2013) Laboratorium Forensik POLRI menyampaikan minimnya barang bukti digital dari tahun ke tahun, tidak sebanding dengan tindak kejahatan internet. Dilaporkanya tindak kejahatan internet dan barang bukti digital yang sangat minim, mengindikasikankurangnya pemahaman masyarakat akan *cybercrime* dan barang bukti digital. Selain itu, dalam mendokumentasikan setiap kejadian maupun kejahatan internet serta minimnya barang bukti digital mengindikasikan kurangnya kesiapan dari berbagai lembaga dalam hal ini instansi pemerintahan dalam mengantisipasi *cybercrime*.

Digital Forensic Readiness Index (DiFRI) adalah kesiapan institusi dalam hal digital forensic. Adapun komponen dari digital forensik readiness meliputi *strategi* yang merupakan keputusan strategis dalam mengimplementasikan digital forensic, *Policy dan procedure* merupakan kebijakan dan prosedur bagi petunjuk organisasi, *teknologi dan security* adalah penggunaan software dan hardware sebagai petunjuk digital forensik, dalam menangani dan menindak terkait *cybercrime* dibutuhkan *digital forensic response, control* dan *risk* serta *legality* yang kemudian dibuat indikator-indikator untuk menghasilkan nilai yang disebut *Digital Forensic Readiness Index (DiFRI).* Pada era modern dan berjalannya penegakan hukum seperti sekarang, sudah saatnya instansi pemerintahan tidak hanya bersikap pasif, tetapi juga aktif untuk menindak dan melaporkan pelaku kejahatan di lingkungan pemerintahan. Tindakan aktif ini berupa perhatian akan pentingnya barang bukti digital, sehingga sebisa mungkin setiap aktivitas dunia maya dan transaksi elektronik terdokumentasikan dan tercatat dengan baik. Dengan adanya *digital forensic readiness*, suatu instansi pemerintahan akan lebih siap ketika tertimpa insiden, proses investigasi akan lebih cepat, diterima oleh hukum dan adanya barang bukti yang cukup untuk menjerat pelaku kejahatan ke pengadilan.

Berdasarkan penelitian sebelumnya yang dilakukan oleh : (Mouhtaropoulos et al. 2014) bahwa kemampuan organisasi untuk memaksimalkan penggunaan bukti digital dan mengantisipasi litigasi. Ketidakcukupan penelitian teknis dan peraturan perundang-undangan dan kebutuhan yang terus meningkat mekanisme pengawetan bukti telah membawa kebutuhan akan kesiapan forensic dan pembuatan kebijakan di masa depan, untuk mengungkap kesenjangan yang perlu dijembatani. Memvalidasi dan memperbaiki kerangka kesiapan forensik digitalmelalui serangkaian kelompok fokus ahli. Menggambar pada pertimbangan para ahli dikelompok fokus, kami membahas masalah kritis yang dihadapi praktisi dalam mencapai digitalkesiapan forensik.(Elyas et al. 2015)

Implementasi digital forensic readiness atau cara menghitung digital forensic readiness indeks untuk mencegah & menindak lanjuti kejahatan dunia maya, sehingga penelitian ini sangat penting dan bermanfaat sekali untuk diterapkan dan dianalisa bagi instansi Pemerintah yang membahas tentang penyusunan indicator. (Widodo 2016). Langkah-langkah konsentrasi proaktif berbeda yang dapat dianut oleh organisasi sebagai cara untuk meningkatkan kemampuan untuk menanggapi insiden keamanan dan menciptakan lingkungan siap-forensik digital. (Karie & Karume 2018). Forensik digital / komputer forensik adalah disiplin turunan dari keamanan komputer yang membahas temuan bukti digital setelah suatu peristiwa terjadi. Aktivitas forensik komputer itu sendiri adalah suatu proses untuk mengidentifikasi, melestarikan, menganalisis, dan menggunakan bukti digital berdasarkan hukum yang berlaku. Forensik digital / komputer forensik adalah disiplin turunan dari keamanan komputer yang membahas temuan bukti digital setelah suatu peristiwa terjadi. Aktivitas forensik komputer itu sendiri adalah suatu proses untuk mengidentifikasi, melestarikan, menganalisis, dan menggunakan bukti digital berdasarkan hukum yang berlaku.(Kohar et al. 2015)

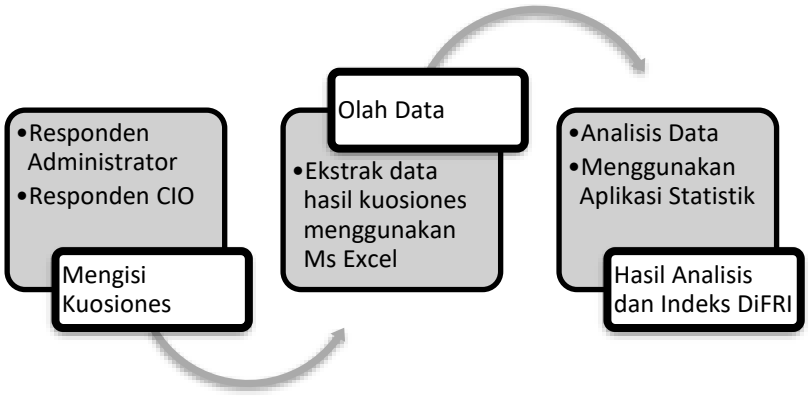
Menyelidiki bukti digital pada file log aplikasi web kemas yang dijalankan pada sistem cluster yang dibangun oleh Docker Swarm. Investigasi ini dilakukan dengan menggunakan kerangka kerja Grr Rapid Response (GRR). (Sunardi et al. 2019). Forensik adalah kegiatan untuk menyelidiki dan menentukan fakta yang terkait dengan pidana kasus dan masalah hukum lainnya. Forensik digital adalah bagian dari ilmu forensik yang mencakup penemuan dan investigasi bahan (data) yang dapat ditemukan di perangkat digital (komputer, ponsel, tablet, PDA, perangkat yang berfungsi baik, penyimpanan, dll.) (Febriansyah & Riadi 2018)

Cybercrime adalah sebagai bentuk hukum gugatan yang dibuat menggunakan internet berdasarkan kecanggihan teknologi komputer dan telekomunikasi. (Hariani & Riadi 2017). Identifikasi aktivitas cybercrime adalah identifikasi jenis serangan yang mengarah ke cybercrime melalui jaringan Wi-Fi. (Susila et al. 2017)

Berdasarkan penjelasan dan uraian diatas akan diterapkan penelitian dari widodo yang melakukan penghitungan digital forensic readness indek untuk mengetahui kesiapan instansi pemerintah dalam menghadapi cybercrime dengan tujuan dapat melakukan pembenahan dan perbaikan secara tepat sasaran agar dimasa mendatang sudah siap dalam menghadapi aktivitas cybercrime yang disebabkan perkembangan teknologi yang semakin maju

2. METODE PENELITIAN

Data penelitian dilakukan dengan cara membagi kuisioner ke instansi pemerintah.kuisi melalui kuesioner. Kuesioner tersebut merupakan model DiFRI yang telah dirancang oleh peneliti sebelumnya. Penelitian ini dilakukan pada 30 instansi, yang meliputi instansi pemerintahan dan teknik pengambilan sampel yang digunakan adalah sampling jenuh, yaitu teknik penentuan sampel yang dilakukan bila jumlah populasi relatif kecil, ada 30 sampel dari 30 instansi pemerintah atau penelitian yang ingin membuat generalisasi dengan kesalahan yang sangat kecil (Sugiyono 2012). Artinya pada penelitian ini sampel adalah seluruh anggota populasi, sehingga jumlah sampel adalah 30 di instansi pemerintahan
Adapun alur proses pengumpulan data seperti terlihat pada gambar 1.



Gambar 1. Alur Pengisian Data

2.1 Pengisian kuisioner

Kuisioner dilakukan melalui 2 (dua) cara yaitu secara online dan offline, kuisioner tersebut terdiri dari 6 komponen DiFRI yaitu strategi, Policy dan procedure, teknologi dan security, digital forensic response, control dan risk serta legality dan tiap komponen terdiri dari beberapa indicatoryang diisi sesuai dengan kondisi instansi pemerintahan tersebut , sedangkan untuk pertanyaan pada kuisioner hanya membutuhkan jawaban antara ada dan tidak

.

2.2.Olah Data

Penelitian ini bersifat evaluatif. diharapkan menjadi model evaluasi DiFRI dari instansi / organisasi dengan menggunakan analisis statistik yang sesuai. Pada data kuisioner skala yang digunakan adalah skala Guttman, yaitu skala pengukuran dengan jawaban tegas, antara "ya-tidak". dipilih skala Guttman karena digunakan untuk membandingkan antara model DiFRI yang dirancang dengan realita yang ada atau terjadi pada suatu organisasi, sehingga organisasi dapat melakukan pembenahan dan perbaikan secara tepat sasaran. 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. Hasil Kuosioner Indikator

Komponen Strategy

Nama :.Dinas Perhubungan
Jabatan : Kasubag Umum

No.	Indikator	Kode	Ada(√) /tidak (×)
1.	Program-program *digital forensic readiness*	S1	×
2.	Aturan, regulasi dan kewajiban menyimpan dokumen, file danrekaman (cctv,log, dokumen)	S2	×
3.	Ketentuan ketika terjadi peristiwa yang membutuhkan barang bukti digital	S3	√
4.	Identifikasi sumber-sumber dan tipe- tipe yang berbeda dari barang bukti digital organisasi	S4	√
5.	Identifikasi teknologi dan sumber daya manusia untuk menjamin *digital forensicreadiness*	S5	×
6.	Jaminan ketersediaan dana untuk menjalankan dan merawat program digital forensik readiness	S6	×

Tahap selanjutnya 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 2.

Tabel 2. Penentuan Skor DiFRI Instansi Pemerintah

NO.	INSTANSI	S1	S2	S3	S4	S5	S6	TOTAL
1	Instansi 1	0	1	1	1	1	0	4
2	Instansi 2	1	1	1	1	1	1	6
3	Instansi 3	0	1	0	0	0	0	1
4	Instansi 4	1	0	1	0	0	0	2
5	Instansi 5	1	0	0	0	1	1	3
6	Instansi 6	0	0	0	0	0	0	0
7	Instansi 7	0	0	0	0	0	0	0
8	Instansi 8	0	1	0	0	0	0	1
9	Instansi 9	0	1	0	0	0	0	1

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
+ 1/6 indeks komponen digital forensic response (1)
+ 1/6 indeks komponen control
+ 1/6 indeks komponen legality

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

$$I_A = \frac{\sum_{k=1}^{n} A}{n_A} . 10 \quad (2)$$

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

2.3 Skala Tingkat DiFRI

Berdasarkan pemberikan rekomendasi dan kejelasan status instansi, maka peneliti sebelumnya skala dan status untuk masing-masing nilai DiFRI (i), ada tiga kriteria berdasarkan skala tertentu, seperti terlihat pada Tabel 3.

Tabel 3. Skala Kesiapan Instansi Pemerintahan berdasarkan DiFRI

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

Berdasarkan skala tersebut mencerminkan keadaan dan status suatu institusi dari segi digital forensic readiness. Adapun detail penjabaran masing-masing status adalah :

1. *Siap*. Status ini merupakan nilai tertinggi bagi istitusi dalam hal *digital forensic readiness*, dari status ini dapat diketahui bahwa sebuah institusi memiliki keenam komponen yang menjadi kriteria *digital forensic readiness* dan mengimplementasikan indikator-indikatornya secara optimal.
2. *Kurang Siap*. Status ini memberikan gambaran bahwa institusi belum memiliki beberapa komponen/kriteria dari komponen *digital forensic readiness* dan belum mengimplementasikan banyak indikator dari komponen yang ada
3. *Tidak siap*. Pada status ini, institusi hanya memiliki satu atau dua komponen *digital forensic readiness*, itupun hanya dengan beberapa indikator saja. Dalam keadaan seperti ini, institusi akan rentan terkena *cybercrime*, selain itu institusi juga tidak mampu menghadapi ataupun menindak lanjuti tindakan *cybercrime*.

3. HASIL DAN PEMBAHASAN

Dalam mengambil suatu keputusan analisis dapat dilakukan menguji kuisioner itu valid atau tidak dengan cara :

1. Uji Validitas yaitu membandingan nilai r_{tabel} dengan r_{hitung}

Apabila $r_{tabel} > r_{hitung}$ tidakvalid
Apabila $r_{tabel} < r_{hitung}$ valid dari *degree of freedom* (df) ((Ghozali 2017)Besar df = n-2, dimana n adalah jumlah sample. Pada penelitian ini besar sampel adalah 30, sehingga df=28, sehingga besar r table untuk df=28 dan alpha=0,05 didapat r table=0,3610 (lihat r table produk moment. Sedangkan r_{hitung} dapat dihitung menggunakan spss pada analisa statistik, dan untuk tiap komponen mempunyai nilai diatas 0.3610 sehingga dinyatakan valid.

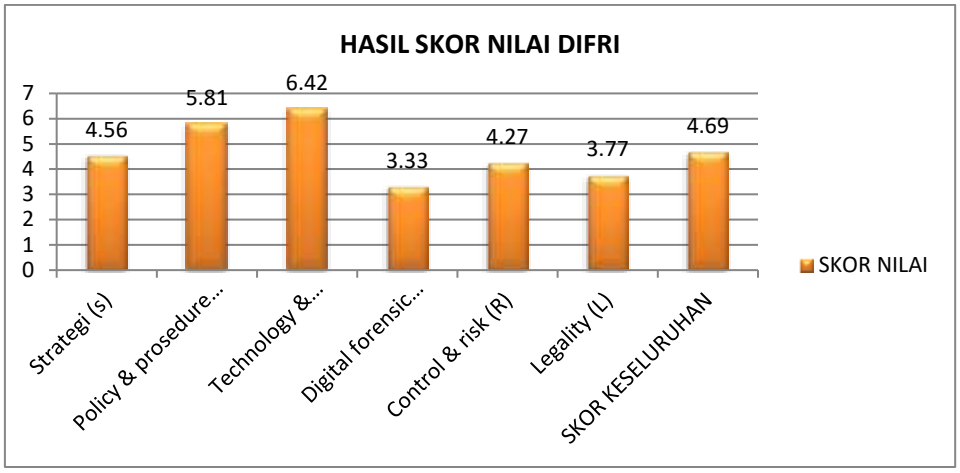
2. Uji reabilitas
   Uji reabilitas diketahui dalam suatu variabel, dapat gunakan Cronbach Alpha (α). Suatu Konstruksi atau variabel dikatakan *reliabel* jika memberikan nilai Cronbach Alpha > 0,70 ((Ghozali 2017). Adapaun hasil uji reliabilitas Variabel dapat dilihat pada Tabel 4.

Tabel 4. Hasil Uji Realibilitas

No.	Variabel	Alpha	Keterangan
1.	*Strategy* (S)	0,772	reliabel
2.	*Policy* &*prosedure* (K)	0,898	reliabel
3.	*Technology* &*security* (T)	0,869	reliabel
4.	*Digital forensic response* (P)	0,604	reliabel
5.	*Control* &*risk* (R)	0,798	reliabel
6.	*Legality* (L)	0,603	reliabel

Menghitung DiFRI keseluruhan variabel, dapat digunakan persamaan (1). Berdasarkan persamaan (1), maka diperoleh DiFRI sebesar 4,69 atau instansi pemerintahan kurang siap Status ini memberikan gambaran bahwa instansi belum memiliki beberapa komponen/kriteria dari komponen *digital forensic readiness* dan belum mengimplementasikan banyak indikator dari komponen yang ada. Pada kondisi seperti ini, institusi akan sangat mudah menjadi korban *cybercrime* dan akan kesulitan mendapatkan barang bukti digital ketika terkena serangan *cybercrime*. Dalam status ini, institansi direkomendasikan untuk melakukan evaluasi dan pembenahan secara intens terhadap komponen dan indikator yang belum dimiliki.

Detail perbandingan antara nilai DiFRI keseluruhan variabel dengan masing- masing variabel dapat terlihat pada gambar 2.



Gambar 2. Alur Pengisian Data

Perbandingan indeks pada masing-masing variabel menunjukan, indeks tertinggi terletak pada variabel *Teknologi Security* yaitu sebesar 6,42. Hal itu menunjukan instansi pemerintahan siap akan menjadikan institusi lebih baik dalam hal keamanan sistem informasi dan jaringan, dalam pemanfaatan TIK, peningkatan barang bukti digital, dan mudah dalam menindak *cybercrime*, dari sisi waktu penindakan lebih cepat dan tepat, dari sisi biaya akan lebih efisien dan hemat.

Indeks policy & prosedur 5,81 ini menandakan kurang siap ada beberapa kebijakan dan prosedur belum ada pada instansi pemerintahan serta belum adanya pembagian wewenang, tugas dan tanggung jawab terkait barang bukti

Pada instansi pemerintahan indek strategi nilai menunjukan 4,55 ini menunjukan kurang siap untuk program–program *digital forensic readiness* artinya instansi pemerintah belum secara khusus dibuat aturan atau program *digital forensic readnes.* Pada pengawasan dan resiko nilai indek 4,27 menunjukan belum siap, sebab dibeberapa instansi belum adanya pengawasan dan manajemen resiko sehingga perlu penanganan dan pembenahan lebih intensif.

Indeks legality pada instansi pemerintahan menunjukan nilai 3,77 ini menandakan kurang siap dalam hal penanganan *cybercrime* dan proses hukum sehingga perlu dibenahi dari sisi legalitas pada aspek hukum pada setiap proses investigasi *digital forensic* dan insiden Indeks terendah 3,33 pada variable digital forensic respon menunjukan instansi pemerintah kurang siap dalam hal sumber daya manusia yang mempunyai sertifikat digital forensic dan diadakan pelatihan – pelatihan mengenai penaganan cybercrime dan *digital forensic* agar instansi pemerintah tidak dijadikan sebagai target *cybercrime*.

KESIMPULAN

Indikator-indikator didapatkan dari penelitian-penelitian sebelumnya yang dirumuskan dari aspek-aspek yang dinilai pada komponen tersebut. Selanjutnya dari aspek-aspek tersebut dianalisa menggunakan metode statistic. Pada perhitungan DiFRI Pemerintahan pada aspek *strategy* memperoleh indeks sebesar 4,56 (kurang siap), aspek *policy & procedure* memperoleh indeks sebesar 5,81 (kurang siap), komponen *technology & security* sebesar 6,42 (siap), komponen *digital forensic response* sebesar 3,33 (kurang siap), komponen *control* sebesar 4,27(kurang siap), komponen *legality* sebesar 3,77 (kurang siap). sehingga indeks keseluruhan DiFRI adalah 4,69 (kurang siap).

secara keseluruhan instansi pemerintah *belum siap* menghadapi *cybercrime* dan diharapkan melakukan pembenahan dan perbaikan secara tepat sasaran agar dimasa mendatang sudah siap dalam menghadapi tindak kejahatan dunia maya yang disebabkan perkembangan teknologi yang semakin canggih.

.

DAFTAR PUSTAKA

(Ghozali, 2011), 2017. Pengaruh Reward (Penghargaan) Terhadap Kinerja Dengan Komitmen Organisasi Sebagai Variabel Moderasi. *Protein Science*, 16(4), pp.733–743.

Al Azhar. M.Nuh, 2013. Mobile Forensic Investigation. Hacking and DigitalForensic Expo (Hadfex).

Elyas, M. et al., 2015. Digital forensic readiness: Expert perspectives on a theoretical framework. *Computers and Security*, 52, pp.70–89. Available at: http://dx.doi.org/10.1016/j.cose.2015.04.003.

Febriansyah, L. & Riadi, I., 2018. Analysis on predicting cyberterrorism using ahp (Analytical hierarchy process) method. *Journal of Theoretical and Applied Information Technology*, 96(22), pp.7563–7575.

Hariani & Riadi, I., 2017. Detection Of Cyberbullying On Social Media Using Data Mining Techniques. *IJCSIS*, 15(3), pp.244–250.

Karie, N. & Karume, S., 2018. Digital Forensic Readiness in Organizations: Issues and Challenges. *The Journal of Digital Forensics, Security and Law*, 12(4).

Kohar, A., Riadi, I. & Lutfi, A., 2015. Analysis of Smartphone Users Awareness Activities Cybercrime. *International Journal of Computer Applications*, 129(2), pp.1–6.

Mouhtaropoulos, A., Li, C. & Grobler, M., 2014. Digital Forensic Readiness: Are We There Yet?: UMUC Library OneSearch. *Joournal of International Commercial Law and Technology*, 9(3), pp.173–179. Available at: http://eds.b.ebscohost.com.ezproxy.umuc.edu/eds/pdfviewer/pdfviewer?sid=a09eede2-dac3-4941-89cb-18d587bda568@sessionmgr101&vid=1&hid=111.

Sugiyono, 2012. Metode Penelitian Kuantitatif, Kualitatif dan R & D.Bandung:Alfabeta. *Metode Penelitian Kuantitatif, Kualitatif dan R & D.Bandung:Alfabeta.*, p.117.

Sunardi, Riadi, I. & Sugandi, A., 2019. Forensic Analysis of Docker Swarm Cluster using Grr Rapid Response Framework. *International Journal of Advanced Computer Science and Applications*, 10(2).

Susila, A., Riadi, I. & Prayudi, Y., 2017. Wi-Fi Security Level Analysis for Minimizing Cybercrime. *International Journal of Computer Applications*, 164(7), pp.35–39.

Symantec, 2012. 2012 Norton Cybercrime Report. *Norton Cybercrime Report*, pp.1–27.

Widodo, T., 2016. Pengembangan Model Digital Forensic Readiness Index (DiFRI) Untuk Mencegah Kejahatan Dunia Maya. *Jurnal Informatika Sunan Kalijaga*, 1(1), pp.41–46.