CyberSecurity dan Forensik Digital e-ISSN: 2615-8442
Vol. 7, No. 2, November 2024, hlm. 81-89

Tinjauan Pustaka Sistematis: Tantangan Dan Faktor-Faktor Pengembangan Kesiapan Forensik Digital

Tri Rochmadi[1,2], Abdul Fadlil[3], Imam Riadi[4]

[1]Program Studi Informatika, Universitas Ahmad Dahlan, Yogyakarta, Indonesia, 55191
[2] Program Studi Sistem Informasi, Universitas Alma Ata, Yogyakarta, Indonesia, 55183
[3] Program Studi Teknik Elektro, Universitas Ahmad Dahlan, Yogyakarta, Indonesia, 55191
[4] Program Studi Sistem Informasi, Universitas Ahmad Dahlan, Yogyakarta, Indonesia, 55191

Email: [1]2437083008@webmail.uad.ac.id, [2]trirochmadi@almaata.ac.id, [3]fadlil@mti.uad.ac.id, [4]imam.riadi@is.uad.ac.id

Abstrak

Teknologi informasi telah mengubah hampir segala lini kehidupan dari konvensional ke digitalisasi. Digitalisasi yang begitu cepat, menimbulkan permasalahan pada serangan siber yang belum diimbangi oleh penanganan insiden siber. Kesiapan forensik digital menjadi hal penting bagi organisasi agar proses penanganan insiden lebih efektif dan efisien. Tujuan penelitian ini adalah mengidentifikasi faktor-faktor dan tantangan terkait topik kesiapan digital forensik. Metode yang digunakan dalam penelitian ini menggunakan metode tinjauan pustaka sistematis. Hasil yang didapatkan pada penelitian ini memberikan informasi jurnal yang paling banyak mempublikasikan topik kesiapan forensik digital, obyek penelitian, metode yang digunakan, standarisasi yang diintegrasikan, faktor-faktor dan tantangan dalam pengembangan kesiapan forensik digital. Penelitian ini bisa menjadi rujukan peneliti akademisi ataupun praktisi pada bidang forensik digital ataupun pengembang aplikasi.

Kata kunci: tinjauan pustaka sistematis, kesiapan forensik digital, ISO/IEC 27043, COBIT.

Systematic Literature Review: Challenges And Factors For Developing Digital Forensic Readiness

Abstract

Information technology has changed almost all lines of life from conventional to digitalization. Rapid digitalization has led to problems with cyber-attacks that the handling of cyber incidents has not matched. Digital forensic readiness is important for organizations to make the incident-handling process more effective and efficient. The purpose of this research is to identify factors and challenges related to the topic of digital forensic readiness. The method used in this research is a systematic literature review. The results obtained in this study provide information on the journals that publish the most digital forensic readiness topics, research objects, methods used, standardization integrated, factors, and challenges in developing digital forensic readiness. This research can be a reference for academic researchers or practitioners in digital forensics or application developers.

Keywords*: systematic literatur review, digital forensic readiness, ISO/IEC 27043, COBIT.*

1. PENDAHULUAN

Peranan teknologi informasi telah mengubah proses bisnis dari konvensional menjadi digitalisasi (Nugroho et al., 2023), (Jupriadi Fakhri et al., 2023). Data digitalisasi di Indonesia menurut (Simon Kemp, 2024) terdapat 185,3 juta pengguna internet pada awal tahun 2024. Dampak digitilasi meningkatkan potensi serangan siber, menurut (Bernadinus Pramudita, 2023) tercatat 7.729.320 serangan terjadi di Indonesia pada periode Q2 2023, dan kebocoran data masih sering terjadi (Riadi et al., 2023). Prediksi dari (Id-SIRTII/CC – BSSN, 2024) serangan siber akan meningkat, sehingga ketahanan siber wajib ditingkatkan (Joe Arton, 2023) karena dampak serangan siber riskan bagi organisasi (Azzam et al., 2023).

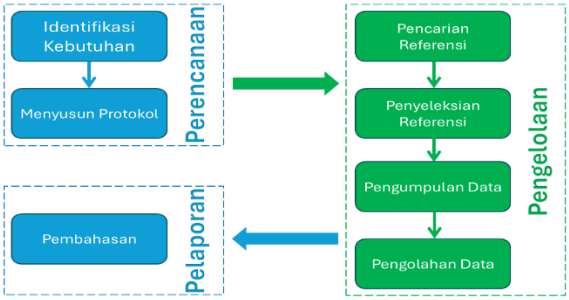
Forensik digital menjadi keharusan untuk mengatasi serangan siber. Forensik digital merupakan ilmu dalam bidang komputer yang menangani masalah serangan siber (Riadi et al., 2022), (Riadi & Ruslan, 2023) atau insiden kejahatan pada perangkat komputer (Rochmadi & Pasa, 2021) untuk mengidentifikasi sumber serangan (Firmansyah et al., 2019). Penerapan forensik digital yang lebih siap atau dikenal dengan *digital forensic*

readines (DFR) belum banyak diterapkan. Ada tantangan dan faktor-faktor utama ataupun pendukung untuk menerapkan DFR ini. DFR bagi organisasi sangat penting karena bukti digital tersebar (Koen & Venter, 2024), sehingga perlu disiapkan agar membantu proses investigasi yang lebih efisien mengurangi biaya investigasi (Garba & Musa Bade, 2019), (Kebande & Venter, 2019b) dan efektif jika terjadi serangan siber (F. M. Alotaibi et al., 2022), (Asante & Amankona, 2021). Kebutuhan DFR dari perspektif keamanan menjadi keharusan untuk memastikan lingkungan atau *environment* penggunana IT terlindungi dan memaksimalkan pengumpulan bukti digital (Kebande & Venter, 2019a). Bukti digital yang didapatkan dari bukti elektronik sangat penting dalam keberhasilan penanganan insiden untuk mendapatkan bukti digital yang relevan (Barske et al., 2010).

Penelitian ini bertujuan untuk menganalisis tantangan dan faktor-faktor yang memengaruhi penerapan kesiapan forensik digital, termasuk pengembangan standar DFR yang relevan, studi kasus terkait, dan metode implementasi yang sesuai. Hasil penelitian ini diharapkan menjadi dasar pengembangan kerangka kerja yang dapat mengisi kesenjangan penelitian di bidang forensik digital.

2. METODOLOGI

Penelitian ini menggunakan metode *Systematic Literatur Review* (SLR) mengadopsi dari penelitian (Wahono, 2015). Tahapan dari metode tersebut terdiri dari tiga (3) tahapan utama yaitu perencanaan, pengelolaan, dan pelaporan. Detail dari tahapan tersebut pada penelitian ini dapat dilihat pada Gambar 1.



Gambar 1. Tahapan *Systematic Literatur Review*

Perencanaan pada tahapan SLR terdiri dari identifikasi kebutuhan dan menyusun protokol. Identifikasi kebutuhan pada penelitian ini adalah menggali informasi dengan topik *Digital Forensic Readiness Framework*. Topik DFR *framework* yang ingin dicari dapat dilihat pada Tabel 1.

Tabel 1. Daftar Pertanyaan pada Literatur Review

ID	Pertanyaan	Tujuan
ID1	Di mana topik DFR paling banyak dipublikasikan?	Mengidentifikasi jurnal untuk menjadi target publikasi penelitian sejenis.
ID2	Apa saja obyek yang telah dilakukan peneliti?	Mengidentifikasi kesenjangan obyek dari penelitian.
ID3	Metode apa saja yang dilakukan oleh peneliti?	Mengidentifikasi metode yang paling banyak digunakan.
ID4	Standarisasi apa yang diintegrasikan dalam DFR?	Mengidentifikasi standarisasi yang paling pernah dilakukan.
ID5	Apa saja hasil dan saran dari penelitian sebelumnya?	Mengidentifikasi tantangan atau faktor pendukung dari DFR dan mengetahui yang belum dikerjakan secara sempurna.

Tabel 1 dapat ditarik kesimpulan bahwa pertanyaan ID1 dapat menjadi rujukan untuk penelitian sejenis dipublikasikan pada jurnal yang paling banyak memuat penelitian serupa. Pertanyaan ID2, ID3 dan ID4 adalah pertanyaan inti yang dapat dijadikan landasan dalam pengembangan penelitian. Pertanyaan ID5 menjadi pendukung dalam penelitian untuk menjadi pertimbangan dalam penelitian berikutnya.

Pengelolaan pada tahapan ini ada beberapa langkah seperti pada Gambar 2, pertama yaitu pencarian literatur dengan memfokuskan pada jurnal dan prosiding internasional bereputasi seperti ScienceDirect, Springer, IEEE, ACM dan *publisher* terindeks scopus. Pencarian referensi menggunakan parameter dengan kata kunci *digital forensic readiness framework* dan 5 tahun terakhir yaitu 2020-2024. Kedua, penyeleksian referensi yaitu pemilihan berdasarkan judul artikel dan beberapa pengecualian seperti artikel sulit didapatkan. Ketiga, pengumpulan data berupa tabulasi untuk mengerucutkan pembagian pertanyaan inti dan pendukung untuk penelitian selanjutnya. Keempat, pengolahan data berupa analisis dan visualisasi agar memudahkan memahami informasi.

Analisis data dilakukan dengan mengorganisasi data untuk mencatata informasi penting. Kriteria data tersebut meliputi informasi dasar berupa judul, penulis, tahun publikasi, dan penerbit. Fokus penelitian berupa metode, *tools*, obyek, dan standarisasi yang digunakan. Metodologi dan hasil penelitian diperlukan untuk mengetahui dan bahan pertimbangan dalam melakukan penelitian selanjutnya. Penelitian ini ekstraksi informasi dari artikel yang dikumpulkan dengan pendekatan manual yaitu membaca artikel dan mencatat ke dalam aplikasi Microsoft Excel.

Gambar 2. Tahapan Pengelolaan SLR

Setelah tahapan pengelolaan selesai, dilanjutkan dengan pelaporan. Pelaporan adalah informasi secara utuh menggambarkan apa yang telah dianalisis sebelumnya pada tahapan pengelolaan. Pelaporan memberikan informasi atau rangkuman dari jawaban yang menjadi pertanyaan pada Tabel 1.

3. HASIL DAN PEMBAHASAN

3.1. HASIL

Hasil dari tinjauan pustaka didapatkan artikel yang berhubungan dengan topik DFR dan sangat relevan sebanyak 42 dari 50 artikel yang dikumpulkan. Data hasil penyeleksian referensi mengikuti ketentuan tahapan yang dilakukan dapat dilihat pada Tabel 2, Tabel 3, Tabel 4, Tabel 5, dan Tabel 6.

Tabel 2. Hasil Seleksi Referensi Tahun 2020

Peneliti	Penerbit	Metode; *Tools*;	Obyek; Standarisasi;
(Munkhondya et al., 2020)	Proquest (International Conference on Cyber Warfare and Security)	Eksperimen; IDS; Snort	*Software-Defined Network*
(Baror et al., 2020)	Taylor & Francis (Australian Journal of Forensic Sciences)	Eksperimen; NLP; Virtualisasi	*Cloud;* ISO/IEC 27043
(Kristyan et al., 2020a)	IEEE (International Conference on Information Technology Systems and Innovation)	Mapping domain framework	*Cloud*
(Bhatia & Malhotra, 2020)	Springer (Innovative Data Communication Technologies and Application)	Mapping domain tool	*Cloud;* ISO/IEC 27050
(Philomin et al., 2020)	Proquest (International Conference on Cyber Warfare and Security)	-	*Smart Home;* IoT; ISO/IEC 27043
(Lagrasse et al., 2020)	Proquest (International Conference on Cyber Warfare and Security)	Eksperimen; IDS; Snort; OpenSwitch	*Software-Defined Network;* ISO/IEC 27043
(Kebande et al., 2020)	Elsevier (Forensic Science International: Reports)	Mapping domain layer IoT	IoT; ISO/IEC 27043
(Gunawan & Yazid, 2020)	IEEE (International Sem inar on Application for Technology of Inform ation and Com m unication)	Mapping domain; Statistik PARETO	*Company*
(Kristyan et al., 2020b)	IEEE (International Conference on Information Technology Systems and Innovation)	Mapping domain; Meta Analisis	
(Sheunesu M. Makura et al., 2020)	IEEE (International Conference on Informatics, IoT, and Enabling Technologies)	Eksperimen; API	*Cloud;* ISO/IEC 27043, ISO/IEC 27037, GDPR
(Daubner et al., 2020)	ACM (Symposium on Applied Computing)	*Design research;*	Sofware

Tabel 2 menunjukkan *publisher* dan jurnal tertinggi yang mempublikasikan topik DFR adalah ProQuest (International Conference on Cyber Warfare and Security) sebanyak 3 artikel. *Publisher* lainnya yang banyak mempublikasikan DFR adalah IEEE namun tersebar ke 4 jurnal. Metode yang digunakan domain mapping sebesar 5 penelitian dan eksperimen 4 penelitian. Obyek paling banyak adalah *cloud* sebanyak 5 dan standarisasi paling banyak diintegrasikan adalah ISO/IEC 27043.

Tabel 3. Hasil Seleksi Referensi Tahun 2021

Peneliti	*Publisher*	Metode; *Tools*;	Obyek; Standarisasi;
(Nik Zulkipli & Wills, 2021)	Elsevier (Procedia Computer Scienc)	Mixed method; FGD	IoT
(Jayaraman & Stanislaus Panneerselvam, 2021)	Springer (Journal of Ambient Intelligence and Humanized Computing)	Eksperiment; Swift	Industri Kesehatan; *Cloud*
(Mudau et al., 2021)	Springer (International Conference on Emerging Applications and Technologies for Industry 4.0)	Domain mapping tool	IoT; ISO/IEC 27043
(Forfot & Østby, 2021)	Springer (Intelligent Technologies and Applications)	*Design research;*	IoT; ISO/IEC 27037, ISO/IEC 10118-2
(Asante & Amankona, 2021)	Journal of Digital Forensics, Security and Law	Mapping domain BYOD; *Design research*	BYoD; ISO/IEC 27043
(Kebande & Choo, 2021)	Wiley (Security Privacy)	-	*Cloud*
(Makura et al., 2021)	Wiley (Security Privacy)	Eksperimen; PDE; Openstack	*Cloud;* ISO/IEC 27043
(Kebande et al., 2021)	Wiley (Security Privacy)	*Design research*;	*Cloud;* ISO/IEC 27043
(Alexakos et al., 2021)	Elsevier (Transportation	Simulasi	Automotiv; IoT;

Peneliti	*Publisher*	Metode; *Tools*;	Obyek; Standarisasi;
	Research Procedia)		GDPR
(Ariffin & Ahmad, 2021)	Elsevier (Computers & Security)	SLR	Industri; CMMI, COBIT
(Lee & Kim, 2021)	IEEE Access	-	Keuangan; ISO/IEC 27043, CMMI
(Ali & Kaur, 2021)	Hindawi (Security and Communication Networks)	Eksperimen; Firewall; IPS, IDS; Anti Virus	*BYoD*
(Sadineni et al., 2021)	IEEE (World Forum on Internet of Things)	Eksperimen; Contiki	IoT

Data pada tahun 2021 seperti Tabel 3, *publisher* dan jurnal tertinggi adalah Wiley (Security Privacy) dengan 3 artikel. Metode eksperimen digunakan oleh 4 penelitian dan design research digunakan 2 penelitian. Obyek paling banyak disasar oleh peneliti pada tahun 2021 adalah IoT sebanyak 5 penelitian.

Tabel 4. Hasil Seleksi Referensi Tahun 2022

Peneliti	*Publisher*	Metode; *Tools*;	Obyek; Standarisasi;
(Jimenez & Fernandez, 2022)	IEEE (Conference on Network Function Virtualization and Software Defined Networks)	Penggabungan framework; Simulasi	*Software-Defined Network*
(Khanji et al., 2022)	Elsevier (Forensic Science International: Digital Investigation)	SLR	IoT
(F. M. Alotaibi et al., 2022)	Hindawi (Computational Intelligence and Neuroscience)	*Design research;*	Drone; ISO/IEC 27043
(Sanda et al., 2022)	Springer (Computing)	Analisis perbandingan	*Cloud;* NIST
(Gundu et al., 2022)	Wiley (Cyber Security and Network Security)	Simulasi; Server; Virtualisasi; Remote Desktop	*Cloud*
(Thron et al., 2022)	ACM (International Conference on Industrial Engineering and Industrial Management)	Mapping framework	Industri
(Singh et al., 2022)	IEEE Access	Eksperimen; Django	Penyimpanan
(Fagbola & Venter, 2022)	MDPI (Applied Sciences)	Integrasi ISO/IEC 27043	IoT; ISO/IEC 27043

Penelitian tahun 2022 pada Tabel 4, topik DFR banyak tersebar ke berbagai *pubsliher* seperti ACM, Elsevier, Hindawi, IEEE, MDPI, Springer dan Wiley. Metode penelitian paling banyak digunakan adalah simulasi yang dilakukan sebanyak 2 kali oleh peneliti berbeda. Obyek paling banyak pada lingkungan IoT dan standarisasi yang digunakan paling banyak adalah ISO/IEC 27043.

Tabel 5. Hasil Seleksi Referensi Tahun 2023

Peneliti	*Publisher*	Metode; *Tools*;	Obyek; Standarisasi;
(F. Alotaibi et al., 2023)	Engineering, Technology & Applied Science Research	*Design research*;	Drone
(Nugroho et al., 2023)	IEEE (International Conference on Cryptography, Informatics, and Cybersecurity)	Penggabungan framework	E-Government
(Mpungu et al., 2023)	Springer (Advanced Sciences and Technologies for Security Applications)	Penggabungan framework	Industri Kesehatan; Network
(Akinbi, 2023)	Wiley (WIREs Forensic Science)	SLR	IoT
(Azzam et al., 2023)	Elsevier (Computers & Security)	Live forensik; Simulasi	Industri
(Rais et al., 2023)	Elsevier (Forensic Science International: Digital Investigation)	Mapping domain framework; 3D printing	Industri; 3D Printing

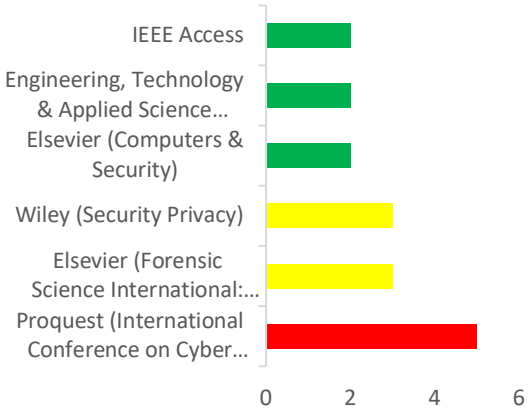
Tabel 5 menunjukkan metode penelitian paling banyak digunakan adalah penggabungan framework sebanyak 2 penelitian. Metode lainnya yang digunakan antara lain *design research*, simulasi, mapping domain dan SLR. Obyek paling banyak digunakan pada lingkungan industri dan lainnya tersebar ke drone, *e-government*, jaringan dan IoT. *Publisher* Elsevier paling banyak yang mempublikasikan topik DFR, namun tersebar ke jurnal yang berbeda. *Publsiher* lainnya yang mempublikasikan DFR adalah IEEE, Springer, Wiley dan jurnal Engineering, Technology & Applied Sceience Research.

Tabel 6. Hasil Seleksi Referensi Tahun 2024

Peneliti	*Publisher*	Metode; *Tools*;	Obyek; Standarisasi;
(Koen & Venter, 2024)	Proquest (International Conference on Cyber Warfare and Security)	Mapping domain	*Cloud*
(Albugmi, 2024)	Engineering, Technology & Applied Science Research	*Design research;*	Database
(Friedl & Pernul, 2024)	Elsevier (Forensic Science	SLR	IoT

Peneliti	*Publisher*	Metode; *Tools*;	Obyek; Standarisasi;
	International: Digital Investigation)		
(Al Mahdi & Baror, 2024)	Proquest (International Conference on Cyber Warfare and Security)	NLP	*Network*

Berdasarkan Tabel 2, Tabel 3, Tabel 4, Tabel 5, dan Tabel 6 untuk pertanyaan ID 1, publikasi dengan topik DFR tertinggi pada jurnal prosiding ProQuest (International Conference on Cyber Warfare and Security) sebanyak 5 artikel. Publikasi lainnya pada jurnal Elsevier (Forensic Science International: Digital Investigation) dan Wiley (Security Privacy) masing-masing terdapat 3 artikel. Jurnal Elsevier (Computers & Security), Engineering, Technology & Applied Science Research, dan IEEE Access masing-masing terdapat 2 artikel dengan topik DFR.



Gambar 3. Jurnal Tertinggi dengan Topik DFR

Gambar 3 menunjukkan *publisher* atau jurnal dengan artikel dengan topik DFR lebih dari 1 artikel yang terbit pada tahun 2020-2024. *Publisher* lain yang memiliki publikasi dengan topik DFR adalah ACM, Hindawi, Springer, Taylor & Francis, dan MDPI. *Publisher* ACM, Hindawi, dan Springer memiliki beberapa artikel DFR yang dipublikasikan pada jurnal yang lain meskipun *publisher* yang sama.

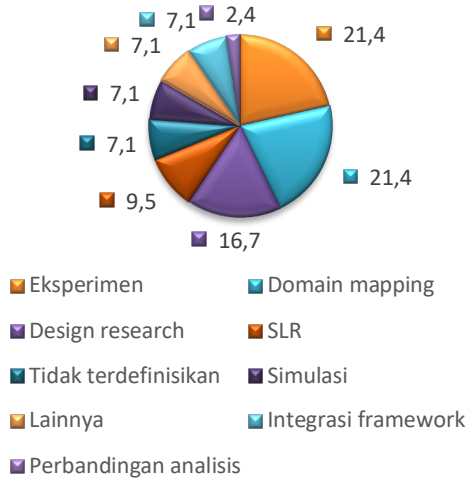
Pertanyaan kedua terkait obyek yang dijadikan penelitian didominasi pada lingkungan jaringan, seperti pada Tabel 7. Obyek pada lingkungan cloud dan jaringan sebanyak 14 dan IoT sebanyak 11. Lingkungan industri termasuk otomotif dilakukan oleh peneliti sebanyak 5, dan obyek lainnya masih sedikiti dibahas seperti *Software-Defined Network, ByoD*, Drone, Kesehatan, Organisasi, Database dan lainnya.

Tabel 7. Obyek Penelitian DFR

Obyek	Jumlah
Cloud dan Jaringan	14
IoT	11
Otomotif dan Industri	5
Software-Defined Network	3
BYoD	2
Drone	2
Kesehatan	2
Organisasi	1
Database	1
E-Government	1
Keuangan	1
Penyimpanan	1
Smart Home	1
Sofware	1

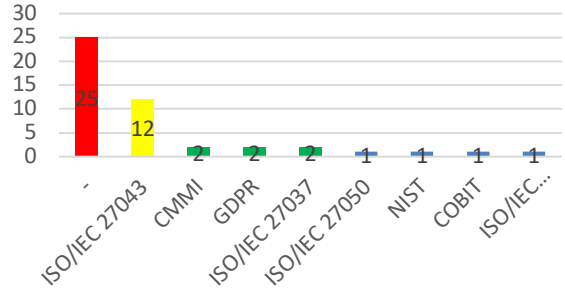
Metode penelitian yang dilakukan paling banyak menggunakan metode eksperimen dan *mapping* sebanyak 9 atau sebesar 21,4%. Metode *design research* sebanyak 7 atau sebesar 16,7%, metode SLR sebanyak 4 atau sebesar 9,5%.

Gambar 4 menunjukkan bahwa ada penelitian yang tidak spesifik menjelaskan metode yang digunakan sebanyak 3 atau sebesar 7,1%. Jumlah yang sama sebesar 7,1% juga ada untuk metode simulasi, lain-lain, dan penggabungan *framework*. Metode lain-lain pada gambar tersebut adalah metode NLP, *Mixed Method*, dan Integrasi.



Gambar 4. Metode Penelitian yang Dilakukan pada Topik DFR

Standarisasi yang paling banyak digunakan adalah ISO/IEC 27043 sebanyak 12 penelitian. Standarisasi CMMI, GDPR, dan ISO/IEC 27037 sebanyak 2 diikuti oleh standarisasi lainnya ISO/IEC 27050, NIST, COBIT dan ISO/IEC 10118-2 sebanyak 1 penelitian.



Gambar 5. Standarisasi Penelitian DFR

Gambar 5 menunjukkan informasi standarisasi yang digunakan oleh peneliti, standarisasi ada yang digunakan lebih dari 1 dalam penelitian. Penelitian juga terdapat yang belum menerapkan standarisasi dalam DFR sebesar 25 penelitian atau >50% dari total studi literatur.

Hasil dari pengelolaan data, didapatkan hasil yang menjawab pertanyaan pada ID5. Terdapat beberapa unsur yang wajib pada implementasi DFR yaitu orang, teknologi, data, prosedur (Kristyan et al., 2020b), (Ariffin & Ahmad, 2021), operasional, pengetahuan, kepedulian (Nik Zulkipli & Wills, 2021), dan *device* (Asante & Amankona, 2021). DFR yang baik juga memiliki beberapa tantangan di antaranya pada penetapan standarisasi (Kebande et al., 2020) (Daubner et al., 2020), perbedaan pada skala organisasi (Gunawan & Yazid, 2020) (Mudau et al., 2021), dan programmer yang membuat software belum menerapkan unsur kesiapan forensik digital (Daubner et al., 2020).

3.2. PEMBAHASAN

Implementasi DFR dalam sebuah organisasi memerlukan berbagai pertimbangan dari para pemangku kepentingan yang terlibat, mengingat karakteristiknya yang beragam dan ketiadaan standar yang tetap (Englbrecht et al., 2020). Organisasi perlu meningkatkan kemampuan keamanan informasi secara global mengatasi permasalahan baik teknis maupun non teknis (Tawar et al., 2022), untuk mampu mengumpulkan dan melindungi data digital yang dapat digunakan sebagai bukti saat terjadi insiden keamanan (Fadlil et al., 2024). Berdasarkan tinjauan pustaka sistematis, standar seperti ISO, GDPR, NIST, COBIT, dan CMMI telah digunakan dalam mengintegrasikan pengembangan DFR. Pendekatan tersebut masih terbatas dan masih sedikit yang menghubungkan untuk pengukuran tingkat kematangan organisasi dalam mengimplementasikan DFR. Tantangan utama dalam penerapan DFR ini mendorong kebutuhan akan kerangka kerja yang dapat digunakan untuk mengukur kematangan organisasi, sehingga membantu pencapaian tata kelola IT yang efektif dalam organisasi (Ariffin & Ahmad, 2021).

4. KESIMPULAN

Berdasarkan penelitian ini dapat diketahui bahwa, penelitian dengan topik DFR banyak dipublikasikan pada ProQuest dan Elsevier. Obyek terbanyak yang dilakukan oleh peneliti sebelumnya adalah pada lingkungan jaringan termasuk *cloud* dan IoT. Metode yang digunakan oleh peneliti didominasi menggunakan *mapping*, eksperimen, dan disusul dengan *design research*. Standarisasi yang paling banyak menggunakan ISO/IEC 27043 dan masih terbatas pada *maturity* seperti CMMI, COBIT, dan lainnya. Unsur utama yang penting pada DFR adalah orang, teknologi, data, prosedur, operasional, pengetahuan, kepedulian, dan *device*. DFR memiliki tantangan pada penetapan standarisasi yang digunakan, perbedaan skala organisasi dan *programmer* yang membuat sebuah aplikasi belum menerapkan kesiapan dari sisi forensik digital. Hasil penelitian ini diharapkan dapat menjadi rujukan peneliti akademisi maupun praktisi pada bidang forensik digital ataupun pengembang aplikasi untuk memperhatikan kesiapan forensik digital.

DAFTAR PUSTAKA

Akinbi, A. O. (2023). Digital Forensics Challenges and Readiness for 6G Internet of Things (IoT) Networks. *WIREs Forensic Science*, *5*(6). https://doi.org/10.1002/wfs2.1496

Al Mahdi, M. M., & Baror, S. (2024). Proof of Concept of a Digital Forensic Readiness Cybercrime Language as a Service. *Proceedings of the 19th International Conference on Cyber Warfare and Security*.

Albugmi, A. (2024). Digital Forensics Readiness Framework (DFRF) to Secure Database Systems. *Engineering, Technology and Applied Science Research*, *14*(2), 13732–13740. https://doi.org/10.48084/etasr.7116

Alexakos, C., Katsini, C., Votis, K., Lalas, A., Tzovaras, D., & Serpanos, D. (2021). Enabling Digital Forensics Readiness for Internet of Vehicles. *Transportation Research Procedia*, *52*, 339–346. https://doi.org/10.1016/j.trpro.2021.01.040

Ali, M. I., & Kaur, S. (2021). Next-Generation Digital Forensic Readiness BYoD Framework. *Security and Communication Networks*, *2021*. https://doi.org/10.1155/2021/6664426

Alotaibi, F., Al-Dhaqm, A., & Al-Otaibi, Y. D. (2023). A Conceptual Digital Forensic Investigation Model Applicable to the Drone Forensics Field. *Engineering, Technology and Applied Science Research*, *13*(5), 11608–11615. https://doi.org/10.48084/etasr.6195

Alotaibi, F. M., Al-Dhaqm, A., & Al-Otaibi, Y. D. (2022). A Novel Forensic Readiness Framework Applicable to the Drone Forensics Field. *Computational Intelligence and Neuroscience*, *2022*. https://doi.org/10.1155/2022/8002963

Ariffin, K. A. Z., & Ahmad, F. H. (2021). Indicators for Maturity and Readiness for Digital Forensic Investigation in Era of Industrial Revolution 4.0. *Computers and Security*, *105*. https://doi.org/10.1016/j.cose.2021.102237

Asante, A., & Amankona, V. (2021). Digital Forensic Readiness Framework Based on Honeypot and Honeynet for BYoD. *Journal of Digital Forensics, Security and Law*, *16*(2). https://doi.org/10.58940/1558-7223.1706

Azzam, M., Pasquale, L., Provan, G., & Nuseibeh, B. (2023). Forensic readiness of industrial control systems under stealthy attacks.

Computers and Security, *125*. https://doi.org/10.1016/j.cose.2022.103010

Baror, S. O., Venter, H. S., & Adeyemi, R. (2020). A Natural Human Language Framework for Digital Forensic Readiness in the Public Cloud. *Australian Journal of Forensic Sciences*, 1–26. https://doi.org/10.1080/00450618.2020.1789742

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

Bernadinus Pramudita. (2023, August 1). *Q2 2023, Kaspersky Catat 7 Juta Lebih Serangan Siber di Indonesia*. Marketeers. https://www.marketeers.com/q2-2023-kaspersky-catat-7-juta-lebih-serangan-siber-di-indonesia/

Bhatia, S., & Malhotra, J. (2020). CFRF: Cloud Forensic Readiness Framework – A Dependable Framework for Forensic Readiness in Cloud Computing Environment. In *Lecture Notes on Data Engineering and Communications Technologies* (Vol. 46, pp. 765–775). Springer Science and Business Media Deutschland GmbH. https://doi.org/10.1007/978-3-030-38040-3_88

Daubner, L., MacAk, M., Buhnova, B., & Pitner, T. (2020). Verification of Forensic Readiness in Software Development: A Roadmap. *Proceedings of the ACM Symposium on Applied Computing*, 1658–1661. https://doi.org/10.1145/3341105.3374094

Englbrecht, L., Meier, S., & Pernul, G. (2020). Towards a Capability Maturity Model for Digital Forensic Readiness. *Wireless Networks*, *26*(7), 4895–4907. https://doi.org/10.1007/s11276-018-01920-5

Fadlil, A., Riadi, I., & Mu'Min, M. A. (2024). Mitigation from SQL Injection Attacks on Web Server using Open Web Application Security Project Framework. *International Journal of Engineering, Transactions A: Basics*, *37*(4), 635–645. https://doi.org/10.5829/ije.2024.37.04a.06

Fagbola, F. I., & Venter, H. (2022). Smart Digital Forensic Readiness Model for Shadow IoT Devices. *Applied Sciences (Switzerland)*, *12*(2). https://doi.org/10.3390/app12020730

Firmansyah, Fadlil, A., & Umar, R. (2019). Analisis Keamanan Data dengan Metode Pertahanan Interaktif Menggunakan Virtual Ridgeback pada Forensik Jaringan. *Seminar Nasional Teknologi Fakultas Teknik Universitas Krisnadwipayana*.

Forfot, A. D., & Østby, G. (2021). Digital Forensic Readiness in IoT - A Risk Assessment Model. *Communications in Computer and Information Science*, *1382*, 53–64. https://doi.org/10.1007/978-3-030-71711-7_5

Friedl, S., & Pernul, G. (2024). IoT Forensics Readiness - influencing factors. In *Forensic Science International: Digital Investigation* (Vol. 49). Elsevier Ltd. https://doi.org/10.1016/j.fsidi.2024.301768

Garba, A. A., & Musa Bade, A. (2019). A Recommended Digital Forensic Readiness Framework for Nigerian Banks. *International Journal of Development Research*, *9*. http://www.journalijdr.com

Gunawan, F., & Yazid, S. (2020). Improving Digital Forensic Readiness in DevOps Context: Lessons Learned from XYZ Company. *Proceedings - 2020 International Seminar on Application for Technology of Information and Communication: IT Challenges for Sustainability, Scalability, and Security in the Age of Digital Disruption, ISemantic 2020*, 459–463. https://doi.org/10.1109/iSemantic50169.2020.9234194

Gundu, S. R., Panem, C., & Satheesh, S. (2022). High-Performance Computing-Based Scalable "Cloud Forensics-as-a-Service" Readiness Framework Factors—A Review. In *Cyber Security and Network Security* (pp. 27–45). Wiley. https://doi.org/10.1002/9781119812555.ch2

Id-SIRTII/CC – BSSN. (2024). *Lanskap Keamanan Siber Indonesia*. https://www.bssn.go.id/wp-content/uploads/2024/03/Lanskap-Keamanan-Siber-Indonesia-2023.pdf

Jayaraman, I., & Stanislaus Panneerselvam, A. (2021). A Novel Privacy Preserving Digital Forensic Readiness Provable Data Possession Technique for Health Care Data in Cloud. *Journal of Ambient Intelligence and Humanized Computing*, *12*(5), 4911–4924. https://doi.org/10.1007/s12652-020-01931-1

Jimenez, M. B., & Fernandez, D. (2022). A Framework for SDN Forensic Readiness and Cybersecurity Incident Response. *2022 IEEE Conference on Network Function Virtualization and Software Defined Networks, NFV-SDN 2022 - Proceedings*, 112–116. https://doi.org/10.1109/NFV-SDN56302.2022.9974648

Joe Arton. (2023, July 24). *Serangan Siber ke Perguruan Tinggi Semakin Meningkat, Ketahanan Siber di Sektor Pendidikan Wajib Ditingkatkan*. Universitas Muhammadiyah Kotabumi. https://www.umko.ac.id/2023/07/24/serangan-siber-ke-perguruan-tinggi-semakin-meningkat-ketahanan-siber-di-sektor-pendidikan-wajib-ditingkatkan/

Jupriadi Fakhri, L., Riadi, I., & Yudhana, A. (2023). Forensic Tools Comparison on File Carving using Digital Forensics Research Workshop Framework. *Scientific Journal of Informatics*, *10*(4). https://doi.org/10.15294/sji.v10i4.46901

Kebande, V. R., & Choo, K. R. (2021). Finite state machine for cloud forensic readiness as a service (CFRaaS) events. *Security and Privacy*, *5*(1). https://doi.org/10.1002/spy2.182

Kebande, V. R., Karie, N. M., Choo, K. R., & Alawadi, S. (2021). Digital forensic readiness intelligence crime repository. *Security and Privacy*, *4*(3). https://doi.org/10.1002/spy2.151

Kebande, V. R., Mudau, P. P., Ikuesan, R. A., Venter, H. S., & Choo, K.-K. R. (2020). Holistic Digital Forensic Readiness Framework for IoT-Enabled Organizations. *Forensic Science International: Reports*, *2*, 100117. https://doi.org/10.1016/j.fsir.2020.100117

Kebande, V. R., & Venter, H. S. (2019a). A comparative analysis of digital forensic readiness models using CFRaaS as a baseline. *WIREs Forensic Science*, *1*(6). https://doi.org/10.1002/wfs2.1350

Kebande, V. R., & Venter, H. S. (2019b). CFRaaS: Architectural design of a Cloud Forensic Readiness as-a-Service Model using NMB solution as a forensic agent. *African Journal of Science, Technology, Innovation and Development*, *11*(6), 749–769. https://doi.org/10.1080/20421338.2019.1585675

Khanji, S., Alfandi, O., Ahmad, L., Kakkengal, L., & Al-kfairy, M. (2022). A systematic analysis on the readiness of Blockchain integration in IoT forensics. *Forensic Science International: Digital Investigation*, *42–43*. https://doi.org/10.1016/j.fsidi.2022.301472

Koen, R., & Venter, H. (2024). A Federated Distributed Digital Forensic Readiness Model for the Cloud. *Proceedings of the 19th International Conference on Cyber Warfare and Security*.

Kristyan, S. A., Suhardi, & Juhana, T. (2020a). Design Framework Forensics Readiness as a Service for Automatic Processing. *2020 International Conference on Information Technology Systems and Innovation, ICITSI 2020 - Proceedings*, 370–374. https://doi.org/10.1109/ICITSI50517.2020.9264965

Kristyan, S. A., Suhardi, & Juhana, T. (2020b). Modeling Cloud Forensics Readiness using MetaAnalysis Approach. *2020 International Conference on Information Technology Systems and Innovation, ICITSI 2020 - Proceedings*, 364–369. https://doi.org/10.1109/ICITSI50517.2020.9264943

Lagrasse, M., Singh, A., Munkhondya, H., Ikuesan, A., & Venter, H. (2020). Digital Forensic Readiness Framework for Software-Defined Networks Using a Trigger-Based Collection Mechanism. *Proceedings of the 15th International Conference on Cyber Warfare and Security, ICCWS 2020*, 296–305. https://doi.org/10.34190/ICCWS.20.045

Lee, S. J., & Kim, G. B. (2021). K-FFRaaS: A Generic Model for Financial Forensic Readiness as a Service in Korea. *IEEE Access*, *9*, 130094–130110. https://doi.org/10.1109/ACCESS.2021.3114233

Makura, S., Venter, H. S., Kebande, V. R., Karie, N. M., Ikuesan, R. A., & Alawadi, S. (2021). Digital forensic readiness in operational cloud leveraging ISO / IEC 27043 guidelines on security monitoring. *Security and Privacy*, *4*(3). https://doi.org/10.1002/spy2.149

Mpungu, C., George, C., & Mapp, G. (2023). Developing a Novel Digital Forensics Readiness Framework for Wireless Medical Networks Using Specialised Logging. *Advanced Sciences and Technologies for Security Applications*, 203–226. https://doi.org/10.1007/978-3-031-20160-8_12

Mudau, P. P., Venter, H. S., Kebande, V. R., Ikuesan, R. A., & Karie, N. M. (2021). Cursory View of IoT-Forensic Readiness Framework Based on ISO/IEC 27043 Recommendations. *Lecture Notes in Networks and Systems*, *254*, 229–239. https://doi.org/10.1007/978-3-030-80216-5_17

Munkhondya, H., Ikuesan, A. R., & Venter, H. S. (2020). A Case for a Dynamic Approach to Digital Forensic Readiness in an SDN Platform. *Proceedings of the 15th International Conference on Cyber Warfare and Security, ICCWS 2020*, 584–593. https://doi.org/10.34190/ICCWS.20.049

Nik Zulkipli, N. H., & Wills, G. B. (2021). An Exploratory Study on Readiness Framework in IoT Forensics. *Procedia Computer Science*, *179*, 966–973. https://doi.org/10.1016/j.procs.2021.01.086

Nugroho, H. A., Briliyant, O. C., & Sunaringtyas, S. U. (2023). A Novel Digital Forensic Readiness (DFR) Framework for e-Government. *Proceedings - 2023 IEEE International Conference on Cryptography, Informatics, and Cybersecurity: Cryptography and Cybersecurity: Roles, Prospects, and Challenges, ICoCICs 2023*, 184–189. https://doi.org/10.1109/ICoCICs58778.2023.10276423

Philomin, S., Singh, A., Ikuesan, A., & Venter, H. (2020). Digital Forensic Readiness Framework

for Smart Homes. *Proceedings of the 15th International Conference on Cyber Warfare and Security, ICCWS 2020*, 627–636. https://doi.org/10.34190/ICCWS.20.047

Rais, M. H., Ahsan, M., & Ahmed, I. (2023). FRoMEPP: Digital forensic readiness framework for material extrusion based 3D printing process. *Forensic Science International: Digital Investigation*, *44*. https://doi.org/10.1016/j.fsidi.2023.301510

Riadi, I., Fadlil, A., & Mu'min, M. A. (2023). OWASP Framework-based Network Forensics to Analyze the SQLi Attacks on Web Servers. *MATRIK : Jurnal Manajemen, Teknik Informatika Dan Rekayasa Komputer*, *22*(3), 481–494. https://doi.org/10.30812/matrik.v22i3.3018

Riadi, I., & Ruslan, T. (2023). Analisis Forensik Digital pada Whatsapp dan Facebook Menggunakan Metode NIST. *Jurnal Fasilkom*, *13*.

Riadi, I., Sunardi, S., & Fitri, F. T. (2022). Spamming Forensic Analysis Using Network Forensics Development Life Cycle Method. *INTENSIF: Jurnal Ilmiah Penelitian Dan Penerapan Teknologi Sistem Informasi*, *6*(1), 108–117. https://doi.org/10.29407/intensif.v6i1.16830

Rochmadi, T., & Pasa, I. Y. (2021). Pengukuran Risiko dan Evaluasi Keamanan Informasi Menggunakan Indeks Keamanan Informasi di BKD XYZ Berdasarkan ISO 27001 / SNI. *CyberSecurity Dan Forensik Digital*, *4*(1), 38–43.

Sadineni, L., Pilli, E. S., & Battula, R. B. (2021). Ready-IoT: A Novel Forensic Readiness Model for Internet of Things. *7th IEEE World Forum on Internet of Things, WF-IoT 2021*, 89–94. https://doi.org/10.1109/WF-IoT51360.2021.9595902

Sanda, P., Pawar, D., & Radha, V. (2022). An insight into cloud forensic readiness by leading cloud service providers: a survey. *Computing*, *104*(9), 2005–2030. https://doi.org/10.1007/s00607-022-01077-2

Sheunesu M. Makura, H. S. V., Victor R. Kebande, Richard Adeyemi Ikuesan, & Nickson M. Karie. (2020). Proactive Forensics: Keystroke Logging from the Cloud as Potential Digital Evidence for Forensic Readiness Purposes. *IEEE Xplore*.

Simon Kemp. (2024, February 21). *Digital 2024: Indonesia*. Global Digital Reports. https://datareportal.com/reports/digital-2024-indonesia

Singh, A., Ikuesan, R. A., & Venter, H. (2022). Secure Storage Model for Digital Forensic Readiness. *IEEE Access*, *10*, 19469–19480. https://doi.org/10.1109/ACCESS.2022.3151403

Tawar, Imam Riadi, Ariqah Adliana Siregar, & Adiniah Gustika Pratiwi. (2022). Security on Charity Crowdfunding Services using KAMI Index 4.1. *Engineering Science Letter*, *1*(01), 15–19. https://doi.org/10.56741/esl.v1i01.61

Thron, R., Dirnberger, H., Tjoa, S., & Quirchmayr, G. (2022). Requirements and Challenges for Digital Forensic Readiness in Industrial Automation and Control Systems. *ACM International Conference Proceeding Series*, 232–238. https://doi.org/10.1145/3524338.3524374

Wahono, R. S. (2015). A Systematic Literature Review of Software Defect Prediction: Research Trends, Datasets, Methods and Frameworks. *Journal of Software Engineering*, *1*(1).