BAB II.
TINJAUAN PUSTAKA DAN LANDASAN TEORI

2.1. Identifikasi *Framework* Forensik digital

Pembahasan pada artikel yang ditulis Bankole, Taiwo, dan Claims berfokus pada alat ukur *framework* untuk proses forensik digital secara umum (Bankole, Taiwo, dan Claims, 2022). Penelitian ini membahas perluasan DFR Commonalities *Framework* (DFRCF) dan pemanfaatan strukturnya untuk mendesain sebuah Digital Forensic Maturity Assesment Model (DFMAM) yang menjadi validator pekerjaan praktisi forensik dan akademisi dengan wawancara semi terstruktur. *Framework* ini digunakan dalam penilaian dari penanganan forensik digital. Penilaian terhadap kerangka kerja forensik dapat menentukan apakah *framework* tersebut efektif atau tidak. Kerangka kerja penilaian yang dikembangkan dapat menjadi acuan dalam pembuatan kebijakan dewan kode etik pada bidang forensik digital.

Pengukuran terhadap kerangka kerja ini tidak terlepas dari nilai integritas yang harus dimiliki dalam proses forensik digital. Tian dan Wang menjelaskan bahwa unsur integritas data adalah salah satu inti dari keamanan informasi. Hasil dari penelitian ini berbentuk sebuah formulasi model sistem dan sebuah model keamanan untuk audit yang valid pada verifikasi integritas data berdasarkan konsep audit proses forensik (Tian, Wang, dan Wang, 2021). Hal ini sejalan dengan penelitian yang dilakukan oleh Balogun dan Zufa bahwa integritas data jadi satu bahasan yang perlu diidentifikasi ketika mengembangkan kode etik pada forensik digital sehingga penilaian terhadap *framework* yang didiskusikan di awal menjadi penting (Balogun dan Zuva, 2017).

Penilaian terhadap *framework* membutuhkan indikator dalam pengukuran aspek apa saja yang akan dinilai. Ariffin dan Ahmad membahas indikator untuk kematangan dan kesiapan organisasi forensik digital, yaitu: (1) Pengembangan orang dan kapasitasnya, (2) Organisasi, kebijakan, dan Kerjasama, (3) Proses, (4) Teknologi dan teknikal, (5) Pengesahan dan peraturan (Ariffin dan Ahmad, 2021).

Hal serupa telah dibahas oleh Seigfried-Spellar tentang nilai-nilai yang perlu dipertimbangkan untuk mengembangkan kode etik forensik digital (Seigfried-Spellar, dkk, 2017).

Ferguson, Renaud, Wilford, dan Irons mengembangkan *framework* berdasar penghargaan terhadap privasi pada proses investigasi forensik digital (Ferguson, dkk, 2020). *Framework* yang dinamai PRECEPT: *Privacy-respecting ethical framework* ini menyediakan dasar keseimbangan antara persyaratan dan harapan penyidik forensik digital di satu sisi dan hak individu dan organisasi di sisi lain. Graeme Horsman pada tahun berikutnya mengusulkan satu set dari sepuluh Privacy-Preserving Data Processing Principles (PPDPP) sebagai pertimbangan dalam proses ekstraksi dan eksaminasi data yang memisahkan data pribadi dengan data yang dapat diuji (Horsman, 2022). Sumber pustaka tersebut memberikan gambaran bahwa pembentukan *framework* baru dengan memahami kerahasiaan data pribadi memungkinkan untuk dilakukan. Hal tersebut merupakan bentuk praktik dari kode etik profesional yang perlu dilakukan oleh penyelidik forensik digital. Sungmi Park, Nikolay Akayev, Yunsik Jang, Jisoo Hwang, Donghyun Kim, Woonseon Yu, Hyunwoo Shin, Changhee Han, Jonghyun Kim menganggap bahwa perlu adanya kode etik forensik digital yang jelas dan organisasi yang mengawasinya (Park, dkk., 2018).

Identifikasi *framework* forensik digital dapat dilakukan dengan mengenali aspek-aspek penting di dalamnya melalui pengukuran dan penilaian. Audit terhadap praktik forensik digital menjadi tahapan evaluasi pelaksanaan *framework* untuk mendapatkan tingkat validitas dan realibilitasnya. Pembentukan *framework* forensik digital baru perlu melalui tahapan identifikasi dan evaluasi yang dapat mengakomodasi aspek sosial, hukum, dan kode etik yang berlaku.

2.2. Penggunaan Standar SNI ISO/IEC 27037

ISO/IEC 27037 merupakan standar internasional yang diadaptasi oleh Badan Standar Nasional menjadi dokumen SNI ISO/IEC 27037 yang memberikan pedoman teknis dalam proses identifikasi, pengumpulan, akuisisi, dan preservasi

bukti digital. Standar ini dikembangkan oleh International Organization for Standardization (ISO) dan International Electrotechnical Commission (IEC) untuk memastikan bahwa penanganan barang bukti elektronik dilakukan secara konsisten, sah, dan dapat dipertanggungjawabkan secara forensik (Faizal & Luthfi, 2024). Standar ISO/IEC 27037 digunakan di Indonesia sebagai acuan dalam proses forensik digital karena memberikan panduan baku terkait identifikasi, pengumpulan, akuisisi, dan preservasi bukti elektronik (Sudyana, 2019)

Standar ISO/IEC 27037 memposisikan proses penanganan awal bukti digital sebagai aktivitas yang dapat diaudit, dapat dipertanggungjawabkan, dan tidak memihak, serta menuntut keterhubungan dengan pengendalian keamanan informasi (ISO/IEC 27001 dan 27002). Penelitian ini menempatkan standar 27037 sebagai rujukan normatif pada tahap hulu penanganan bukti sehingga alur kerja forensik yang dihasilkan memiliki justifikasi metodologis yang kuat sebelum berlanjut ke tahap analisis.

Dokumen ISO/IEC 27037:2014 menjabarkan prosedur khusus yang mengendalikan risiko teknis dan etik, meliputi penetapan dan pemeliharaan rantai penguasaan (chain of custody), pengamanan lokasi insiden, serta dokumentasi rinci terhadap kondisi perangkat, waktu sistem, tindakan yang dilakukan, dan alat yang digunakan (Badan Standarisasi Nasional, 2014). Standar ini mengarahkan pengambilan keputusan berbasis prinsip volatilitas data (prioritas data yang paling mudah berubah), termasuk pertimbangan akuisisi secara *live* ketika perangkat tidak dapat dimatikan atau ketika enkripsi aktif, serta pengemasan dan transportasi yang mencegah kontaminasi bukti.

Kelebihan ISO/IEC 27037 terletak pada fokus preskriptif terhadap tahap awal penanganan bukti, penekanan pada auditabilitas, keterulangan, dan reprodusibilitas proses, serta keharusan dokumentasi yang rinci sehingga tata kelola etik forensik memperoleh pijakan prosedural yang jelas. Standar ini memiliki konsistensi prosedural dan legitimasi hukum yang memperkuat keabsahan barang bukti di pengadilan, namun kekurangannya terletak pada keterbatasan adaptasi terhadap teknologi baru dan konteks sosial lokal (Faizal & Luthfi, 2024). Standar SNI ISO/IEC 27037:2014 memiliki beberapa kekurangan terhadap praktik etis

digital forensik di Indonesia. Cakupannya dibatasi pada identifikasi, pengumpulan, akuisisi, preservasi sehingga tidak mengatur analisis, pelaporan di peradilan, dan komunikasi temuan; standar bersifat reaktif (*forensic readiness* berada di luar cakupan) serta tidak memandatkan alat/metode spesifik maupun kerangka proporsionalitas dan minimisasi data untuk akuisisi live. Persyaratan kompetensi bersifat generik dan bervariasi lintas yurisdiksi, perlindungan kerahasiaan hanya tersirat, konversi analog digital tidak tercakup, dan format dokumentasi bersifat *minimum set* sehingga rawan ketidakkonsistenan praktik, bias interpretasi, serta celah akuntabilitas.

2.3. Identifikasi Topik dan Area Penelitian

Teknik bibliometrik dilakukan untuk mengidentifikasi topik dan area penelitian ini. Kajian bibliometrik terhadap topik *framework* pada forensik digital yang telah dilakukan, menemukan hubungan antara forensik digital dan teknologi terbaru. Istilah teknologi yang bersinggungan dengan kata kunci forensik digital di antaranya adalah *internet of things*, *cloud computing, security,* dan *big data.* Topik-topik penelitian di area forensik digital dapat dilihat pada Tabel 2.1.

Tabel 2.1 Daftar 20 kata kunci teratas terkait topik forensik digital

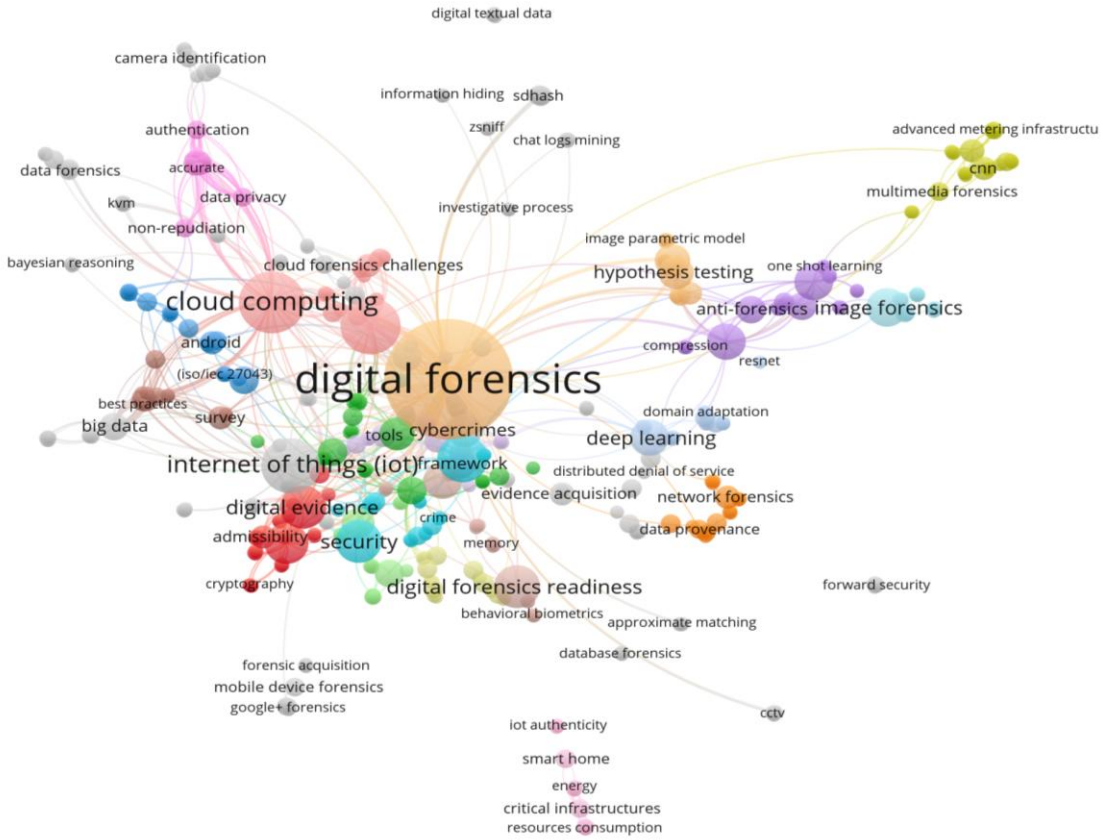
No.	*Keyword*	*occurrences*	*total link strength*
1	*digital forensics*	71	297
2	*cloud computing*	20	112
3	*cloud forensics*	17	69
4	*internet of things*	9	55
5	*Security*	10	46
6	*digital evidence*	9	39
7	*Blockchain*	9	36
8	*big data*	4	33
9	*Forensics*	9	33
10	Iot	6	32

Tabel 2.1 Daftar 20 kata kunci teratas terkait topik forensik digital (lanjutan)

No.	*Keyword*	*occurrences*	*total link strength*
11	*Investigation*	7	31
12	*digital forensic readiness*	8	30
13	*Survey*	3	30
14	*deep learning*	7	28
15	*image forensics*	8	28
16	*camera model identification*	7	27
17	*non-repudiation*	2	27
18	*Privacy*	5	27
19	*nuisance parameters*	6	25
20	*hypothesis testing*	6	24

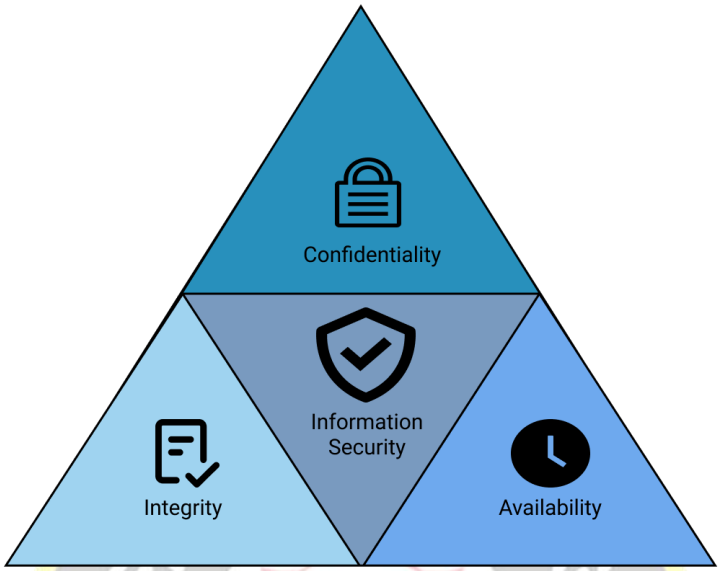
Tabel 2.1 memperlihatkan bahwa inti riset bertumpu pada "*digital forensics*" (71 kemunculan; total link strength 297) sebagai simpul paling terhubung, diikuti "*cloud computing*" (20; 112) dan "*computer forensics*" (17; 69). Pola ini menandakan medan kajian bergeser ke lingkungan bukti yang terdistribusi dan heterogen, ditunjukkan oleh keterkaitan kuat dengan "*internet of things*", sementara isu skala dan integritas data tercermin pada kemunculan "*big data*" dan "*blockchain*". Kata kunci "*security", "privacy*", serta "*non-repudiation*" menegaskan kebutuhan kontrol keamanan dan kepatuhan hukum dalam seluruh rantai penanganan bukti, sedangkan istilah seperti "*investigation*", "*digital forensic readiness*", "*survey*", dan "*hypothesis testing*" mengisyaratkan pentingnya prosedur baku, kesiapan organisasi, dan validasi ilmiah.

Kata kunci yang berkaitan dengan forensik digital menunjukkan jumlah artikel ilmiah yang membahas tema yang serupa dan dapat divisualisasikan menjadi peta bibliometrik. Peta bibliometrik yang mendasari penelitian ini dapat dilihat pada Gambar 2.1. Peta bibliometrik dapat berfungsi untuk identifikasi tren penelitian, menentukan area fokus, mendukung kebaruan, dan menunjukkan relevansi topik penelitian (Hasan & Djaenudin, 2023).



Gambar 2.1. Peta bibliometrik *Framework* pada Forensik digital

Kajian-kajian forensik digital masih berada di dalam bidang keamanan informasi. Konsep segitiga keamanan informasi digunakan sebagai patokan bagi proses forensik digital yang dilakukan. Segitiga keamanan informasi pada Gambar 2.2. menunjukkan bahwa integritas, kerahasiaan, dan ketersediaan data menjadi prioritas yang juga harus dijaga pada proses forensik digital. Kerangka kerja forensik digital perlu bersandar pada segitiga keamanan informasi sebagai acuan operasional pada setiap tahap investigasi.



Gambar 2.2. Segitiga Keamanan Informasi

Integritas data adalah salah satu inti dari keamanan informasi. Upaya audit keamanan untuk menjaga integritas pada proses forensik digital menjadi penting untuk dilakukan (Tian, Wang, dan Wang, 2021). Unsur integritas data merupakan satu hal yang perlu diprioritaskan ketika mengembangkan kode etik pada penanganan forensik digital (Balogun dan Zuva, 2017).

Pelanggaran data terjadi karena implementasi yang buruk dan tidak adanya kontrol penuh terhadap privasi dari pihak swasta maupun pemerintah. Integritas data yang menjadi prioritas keamanan akan mengalami gangguan dalam penanganan kasus forensik digital. Kode etik forensik digital yang jelas dan organisasi yang mengawasinya sangat diperlukan (Park, dkk., 2018).

Penelitian mengenai tingkat kematangan proses forensik digital mengidentifikasi urgensi perbaikan *framework* pengukuran agar dapat memvalidasi pekerjaan praktisi forensik dan akademisi dengan wawancara semi terstruktur (Bankole, Taiwo, dan Claims, 2022). Hasil dari wawancara kemudian dianalisis dan diklasifikasi berdasarkan domain *framework* forensik digital. Kesiapan dari proses forensik digital dianggap penting untuk bidang ini. Kerangka kerja penilaian kesiapan forensik digital dapat menjadi acuan dalam pembuatan kebijakan dewan kode etik pada bidang forensik digital.

Ariffin dan Ahmad menyebutkan lima indikator untuk mengukur tingkat kematangan dan kesiapan organisasi terhadap forensik digital yang menjadi parameter untuk mengembangkan proses forensik digital. Lima indikator tersebut adalah: (1) Pengembangan orang dan kapasitasnya, (2) Organisasi, kebijakan, dan Kerjasama, (3) Proses, (4) Teknologi dan teknikal, (5) Pengesahan dan peraturan (Ariffin dan Ahmad 2021). Nilai-nilai etis yang berasal dari indikator tersebut perlu diperhatikan juga dalam mengembangkan kode etik di bidang forensik digital (Seigfried-Spellar, Rogers, dan Crimmins 2017).

Pengembangan *framework* untuk kode etik investigasi forensik digital yang berfokus pada integritas data perlu dilakukan. PRECEPT: *Privacy-respecting ethical framework* merupakan salah satu *framework* yang menyediakan dasar keseimbangan antara persyaratan dan harapan penyidik forensik digital di satu sisi dan hak individu dan organisasi di sisi lain. *Framework* yang dirancang ini terdiri dari delapan tahapan yang disesuaikan dengan aktivitas forensik (Ferguson, dkk, 2020). Penelitian dengan topik pembahasan forensik digital dan kaitannya dengan penegakkan kode etik ditampilkan pada Tabel 2.2.

Tabel 2.2 Penelitian Terdahulu

No.	Penulis dan Tahun	Metode	Hasil	Kelemahan
1	(Bankole, Taiwo, dan Claims 2022)	Mix Method (kualitatif-kuantitatif)	Pengukuran terhadap kesiapan dan kematangan organisasi dalam bidang forensik digital	Model pengujian belum terstandarisasi sehingga masih diragukan realibilitasnya
2	(Stoykova, Andersen, Franke, dan Axelsson, 2022)	Deskriptif-Kualitatif	Investigasi pada kasus forensik digital di Norwegia menemukan tidak adanya reliabilitas bukti digital.	Belum ada klasifikasi kasus forensik digital sebelum validasi reliabilitas.

Tabel 2.2 Penelitian Terdahulu (lanjutan)

No.	Penulis dan Tahun	Metode	Hasil	Kelemahan
3	(Horsman, 2022)	Deskriptif	Usulan 10 prinsip Privacy-Preserving Data Process ing Principles (PPDPP)	Hanya berfokus pada teknis ekstraksi data dari perangkat digital. Tidak mengatur aktor yang melakukan proses forensik digital.
4	(Ferguson, Renaud, Wilford, dan Irons, 2020)	Deskriptif kualitatif	PRECEPT: Sebuah rancangan *framework* untuk investigasi forensik digital yang etis	Dasar yang dijadikan dasar rancangan *framework* tidak berdasarkan pembahasan mendalam terkait kasus yang terjadi di lapangan, hanya berdasarkan aturan-aturan yang berlaku, sehingga kurang realistis jika diterapkan.
5	(Baror, Venter, dan Adeyemi 2020)	Deskriptif Kualitatif	*Framework* forensik digital untuk layanan *cloud*	Belum adanya penerapan yang nyata pada kasus kejahatan *cloud computing*. Usulan *framework* masih teoritis dan pengujian terbatas.
6	(Stoyanova, Nikoloudakis,	Deskriptif Kualitatif	Identifikasi dan diskusi tantangan	Penulis hanya menyajikan bahan

Tabel 2.2 Penelitian Terdahulu (lanjutan)

No.	Penulis dan Tahun	Metode	Hasil	Kelemahan
	Panagiotakis, Pallis, dan Markakis, 2020)		investigasi forensik digital pada ranah IoT dan layanan *cloud*.	kajian yang menarik terkait proses forensik digital pada IoT dan layanan *cloud*.
7	(Alenezi, Atlam, dan Wills 2019)	Deskriptif kualitatif	*Framework* terkait kesiapan organisasi mengimplementasikan forensik digital pada layanan *cloud*.	Penulis mengumpulkan faktor-faktor kesiapan implementasi forensik digital dari para ahli, namun belum benar-benar melakukan kroscek faktor tersebut pada studi kasus yang nyata.
8	(Fukami, Stoykova, dan Geradts 2021)	Deskriptif kualitatif	Model proses forensik digital pada kasus perangkata *mobile*	Model forensik digital yang diusulkan masih dalam skala kecil, dan belum representatif untuk semua jenis kasus yang serupa.
9	(Goudbeek, Choo, dan Le-Khac 2018)	Deskriptif Kualitatif	Model proses forensik digital pada perangkat *smart home* /IoT	Model forensik digital yang diusulkan dalam skala kecil, sehingga belum merepresentasikan perangkat *smart-home* yang berbeda

Tabel 2.2 Penelitian Terdahulu (lanjutan)

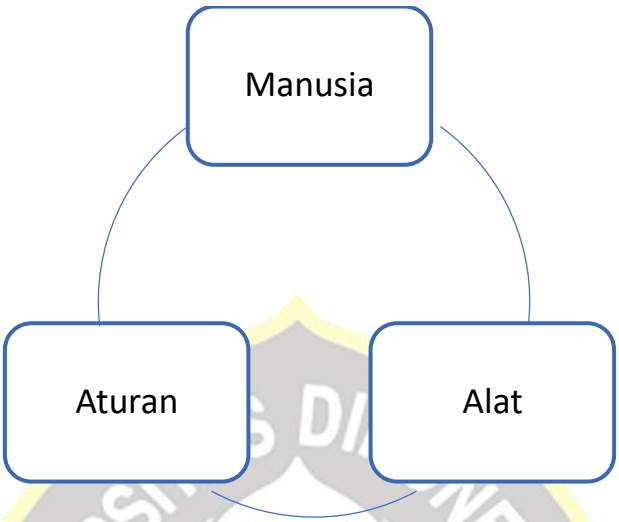
No.	Penulis dan Tahun	Metode	Hasil	Kelemahan
10	(Granja & Rafael, 2017)	Deskriptif Kualitatif	*Framework* forensik digital yang berfokus pada preservasi bukti digital	*Framework* forensik digital yang diusulkan menitikberatkan pada proses preservasi, sehingga prinsip kerahasiaan dan ketersediaan data pada bukti digital belum dapat dikontrol.
11	(Horsman, 2018)	Deskriptif Kualitatif	*Framework* untuk desain pengujian forensik digital	Penulis berfokus pada desain penelitian forensik digital, sehingga belum mampu diterapkan pada kasus nyata
12	(Jain, 2015)	Deskriptif Kualitatif	*Framework* forensik digital dengan teknik *case history keeper*	*Framework* ini masih belum diujikan pada segala kondisi dan lingkungan, sehingga masih berupa kerangka kerja teoritis
13	(Jayaraman & Stanislaus Panneerselvam, 2021)	Deskriptif Kualitatif & Kuantitatif	*Framework* forensik digital yang fokus pada data kesehatan pada layanan *cloud*	*Framework* masih diujikan pada data kesehatan di layanan *cloud* dengan *file* yang terenkripsi, sehingga belum dapat memberi

Tabel 2.2 Penelitian Terdahulu (lanjutan)

No.	Penulis dan Tahun	Metode	Hasil	Kelemahan
				gambaran pada kasus data yang tidak terenkripsi
14	(Montasari, dkk, 2015)	Deskriptif Kualitatif	*Framework* ICFIPM	Penelitian belum diuji *usability* dan *utility* nya.
15	(Soltani & Seno, 2019)	Deskriptif Kualitatif	Model untuk konstriksi ulang *file* yang dapat digunakan sebagai bukti digital	Model ini hanya berfokus pada barang bukti digital sehingga belum dapat mengontrol lingkungan di luarnya

Penelitian terdahulu pada Tabel 2.2 memberi gambaran bahwa *framework* forensik digital menjadi komponen penting pada investigasi forensik digital. *Framework* yang diterapkan di seluruh dunia secara spesifik memiliki elemen yang berbeda.

Bidang forensik digital mengenal tiga komponen penting, yaitu alat, manusia, dan aturan (Casey, 2011). Komponen-komponen tersebut berkaitan satu sama lain. Alat-alat forensik yang canggih memerlukan operator yang terlatih dan kompeten, sementara aturan-aturan yang jelas mengatur penggunaan alat dan tindakan para ahli forensik. Keterpaduan yang harmonis dari ketiga komponen ini menjadi kunci keberhasilan dalam investigasi digital. Ilustrasi keterkaitan masing-masing komponen ditunjukkan pada Gambar 2.3.



Gambar 2.3 Komponen dalam forensik digital.

Perubahan yang terjadi pada salah satu komponen dimungkinkan memengaruhi komponen-komponen yang lain. Perubahan pada aturan, dalam hal ini kerangka kerja forensik digital, akan memengaruhi pelaku dan infrastruktur pada bidang tersebut.

2.4. Analisis Elemen dan Sub elemen *Framework* Forensik digital

Integrated Computer Forensics Investigation Process Model (ICFIPM) adalah adalah kerangka atau model proses investigasi forensik yang dirancang khusus untuk mengumpulkan bukti digital dari berbagai sumber seperti komputer, jaringan, dan perangkat seluler. Model ini berfokus pada pengumpulan, analisis, dan interpretasi bukti digital dengan tujuan mengidentifikasi dan mengumpulkan bukti digital yang signifikan (Montasari, Peltola, dan Evans, 2015).

ICFIPM dibangun dengan beberapa tahapan proses investigasi yang saling terkait dan saling melengkapi, yaitu:

a. *Identification*: tahap identifikasi dan analisis terhadap tindakan kejahatan siber yang terjadi.
b. *Preservation*: tahap pemeliharaan dan pengamanan bukti digital yang ditemukan dalam penyelidikan.

c. *Collection*: tahap pengumpulan bukti digital yang relevan dan valid dalam penyelidikan kejahatan siber.
d. *Examination*: tahap analisis dan pemeriksaan bukti digital yang telah dikumpulkan, termasuk identifikasi, validasi, dan interpretasi data yang ditemukan.
e. *Analysis*: tahap analisis dan interpretasi bukti digital yang telah ditemukan dan diperiksa, termasuk pengembangan hipotesis dan pemecahan masalah.
f. *Presentation*: tahap presentasi hasil investigasi forensik digital, termasuk pembuatan laporan investigasi yang jelas dan terperinci.

ICFIPM menuntut proses investigasi forensik yang sistematis, terstruktur, dan komprehensif untuk pengumpulan, analisis, dan interpretasi bukti digital. ICFIPM memberdayakan penyelidik untuk memastikan bahwa proses investigasi dilakukan dengan hati-hati, didokumentasikan dengan baik dan berkualitas tinggi sesuai dengan proses hukum.

Framework for Reliable Experimental Design (FRED) adalah kerangka kerja atau model yang digunakan untuk merancang dan melakukan eksperimen yang andal dan dapat direproduksi Tujuan FRED adalah untuk mengoptimalkan keandalan hasil eksperimen melalui perencanaan yang cermat dan terstruktur (Horsman, 2018).

FRED terdiri dari beberapa tahap yang saling terkait, yaitu:

a. *Define*: tahap definisi masalah dan penentuan tujuan eksperimen.
b. *Design*: tahap perancangan eksperimen, termasuk pemilihan sampel dan kontrol eksperimen.
c. *Collect*: tahap pengumpulan data eksperimen secara akurat dan terperinci.
d. *Analyze*: tahap analisis data eksperimen, termasuk identifikasi variabel yang signifikan dan pengambilan kesimpulan.
e. *Interpret*: tahap interpretasi hasil eksperimen dan kesimpulan yang diambil.
f. *Report*: tahap pelaporan hasil eksperimen secara terperinci dan jelas.

FRED dapat digunakan untuk memastikan bahwa eksperimen yang dilakukan memiliki keandalan dan kepercayaan yang tinggi, sehingga hasil eksperimen dapat digunakan sebagai dasar dalam pengambilan keputusan.

PREDECI (*Practical REsearch into Digital Evidence and Cybercrime Investigation*) adalah sebuah kerangka kerja forensik digital yang dirancang untuk membantu dalam penyelidikan kejahatan siber (Granja dan Rafael, 2017). *Framework* ini terdiri dari lima tahap yaitu:

a. *Prepare*: tahap perencanaan untuk menentukan skala dan sumber daya yang dibutuhkan dalam penyelidikan.
b. *Responds*: tahap respons awal terhadap insiden yang terjadi, seperti pengumpulan dan pengamatan data awal.
c. *Evaluate*: tahap analisis data dan pengumpulan bukti, termasuk identifikasi bukti yang relevan dan verifikasi integritasnya.
d. *Documentation*: tahap dokumentasi hasil analisis data dan bukti, termasuk laporan investigasi yang jelas dan terperinci.
e. *Present*: tahap presentasi laporan investigasi, termasuk konsultasi dengan pengacara atau otoritas yang berwenang.

PREDECI sangat bermanfaat dalam membantu para penegak hukum untuk melakukan penyelidikan kejahatan siber dengan terstruktur dan sistematis, sehingga memungkinkan untuk mengumpulkan bukti-bukti secara efektif dan efisien.

PRECEPT (*Process for Recording and Executing Computer Forensic Examinations and Techniques*) adalah sebuah kerangka kerja forensik digital yang digunakan untuk memandu dan merekam proses eksaminasi forensik digital (Ferguson, dkk, 2020). *Framework* ini terdiri dari empat tahap yaitu:

a. *Planning*: tahap perencanaan untuk menentukan tujuan dan sumber daya yang dibutuhkan dalam eksaminasi forensik digital.
b. *Execution*: tahap pelaksanaan eksaminasi forensik digital, termasuk pengumpulan dan analisis data serta verifikasi hasil eksaminasi.
c. *Documentation*: tahap dokumentasi hasil eksaminasi forensik digital, termasuk laporan investigasi yang jelas dan terperinci.

d. *Presentation*: tahap presentasi laporan investigasi, termasuk konsultasi dengan pengacara atau otoritas yang berwenang.

PRECEPT membantu para penegak hukum dan profesional forensik digital dalam merencanakan, melaksanakan, mendokumentasikan, dan mempresentasikan hasil eksaminasi forensik digital secara terstruktur dan sistematis.

PPDPP (*Preparation, Collection, Analysis, Presentation, and Preservation*) adalah sebuah *framework* forensik digital yang dirancang untuk membantu proses investigasi kejahatan siber (Horsman, 2022). Kerangka kerja ini terdiri dari lima tahap yaitu:

a. *Preparation*: tahap perencanaan dan persiapan untuk menentukan tujuan dan sumber daya yang dibutuhkan dalam penyelidikan kejahatan siber.
b. *Collection*: tahap pengumpulan bukti digital yang relevan dan valid dalam penyelidikan kejahatan siber.
c. *Analysis*: tahap analisis bukti digital yang telah dikumpulkan, termasuk identifikasi, validasi, dan interpretasi data yang ditemukan.
d. *Presentation*: tahap presentasi hasil analisis bukti digital, termasuk pembuatan laporan investigasi yang jelas dan terperinci.
e. *Preservation*: tahap pemeliharaan dan pengamanan bukti digital yang telah dikumpulkan dan dianalisis agar dapat digunakan sebagai bukti di persidangan.

PPDPP sangat berguna bagi para penegak hukum dan profesional forensik digital dalam melakukan penyelidikan kejahatan siber dengan terstruktur dan sistematis, sehingga memungkinkan untuk mengumpulkan bukti-bukti secara efektif dan efisien.

Lima *framework* yang ditinjau memiliki kesamaan perlakuan, yaitu penggunaannya disesuaikan dengan kondisi di lapangan. *Framework* forensik digital tersebut kemudian dievaluasi untuk melihat kekurangan dari kerangka kerja yang diusulkan.

2.5. Evaluasi *Framework* Forensik digital

Framework yang menjadi tinjauan dalam penelitian ini dievaluasi berdasarkan kelebihan dan kekurangannya, sehingga dapat dibandingkan dan menjadi acuan dalam pengembangan dokumen naskah akademik yang berisi *framework* baru. Perbandingan kelebihan dan kekurangan *framework* dapat dilihat pada Tabel 2.3.

Tabel 2.3 Evaluasi *framework* forensik digital

No.	Metode	Kelebihan	Kekurangan
1	ICFIPM	• ICFIPM menggabungkan beberapa metode dan teknik investigasi forensik yang telah diakui secara internasional dalam satu model, sehingga memberikan pedoman yang komprehensif untuk melakukan investigasi forensik pada perangkat komputer. • ICFIPM mencakup tahap analisis yang terperinci dan sistematis, sehingga memungkinkan ahli forensik untuk mengidentifikasi dan memperoleh bukti digital yang relevan dengan lebih efektif.	• ICFIPM dinilai kompleks untuk digunakan oleh ahli forensik pemula atau oleh pengguna yang tidak berpengalaman dalam investigasi forensik. • ICFIPM memerlukan waktu dan sumber daya yang cukup untuk melakukan investigasi forensik yang menyeluruh menggunakan metode yang dijelaskan dalam model ini.

Tabel 2.3 Evaluasi *framework* forensik digital (lanjutan)

No.	Metode	Kelebihan	Kekurangan
2	FRED	• FRED dirancang untuk menjadi mudah digunakan dan dapat dioperasikan oleh ahli forensik yang tidak memiliki latar belakang teknis yang luas dalam bidang IT. • FRED menggunakan proses yang terstruktur dan sistematis untuk mengumpulkan dan menganalisis bukti digital, sehingga meminimalkan risiko kerusakan atau modifikasi pada bukti digital. • FRED mencakup teknologi yang inovatif dan dapat mendukung berbagai jenis perangkat yang digunakan dalam investigasi forensik.	• FRED memiliki keterbatasan dalam hal kemampuan teknis dibandingkan dengan *framework* forensik digital lainnya. • FRED kurang fleksibel dalam mengakomodasi berbagai jenis investigasi forensik yang kompleks atau sulit.
3	PREDECI	• PREDECI mengadopsi pendekatan yang sistematis dan terstruktur dalam mengumpulkan, menganalisis, dan	• PREDECI memerlukan waktu yang lebih lama untuk melakukan investigasi forensik secara menyeluruh

Tabel 2.3 Evaluasi *framework* forensik digital (lanjutan)

No.	Metode	Kelebihan	Kekurangan
		mempresentasikan bukti digital, sehingga meminimalkan potensi kesalahan atau kehilangan bukti digital. • PREDECI mencakup panduan praktis yang dapat membantu ahli forensik dalam menentukan strategi dan langkah-langkah investigasi forensik yang sesuai dengan situasi yang dihadapi. • PREDECI mencakup proses verifikasi dan validasi untuk memastikan keaslian dan integritas bukti digital.	dibandingkan dengan beberapa *framework* forensik digital lainnya. • PREDECI mungkin kurang fleksibel dalam mengakomodasi berbagai jenis investigasi forensik yang kompleks atau sulit.
4	PRECEPT	• PRECEPT mengadopsi pendekatan yang sistematis dan terstruktur dalam mengumpulkan, menganalisis, dan mempresentasikan bukti digital, sehingga meminimalkan potensi	• PRECEPT memerlukan waktu yang lebih lama untuk melakukan investigasi forensik secara menyeluruh dibandingkan dengan beberapa *framework* forensik digital lainnya.

Tabel 2.3 Evaluasi *framework* forensik digital (lanjutan)

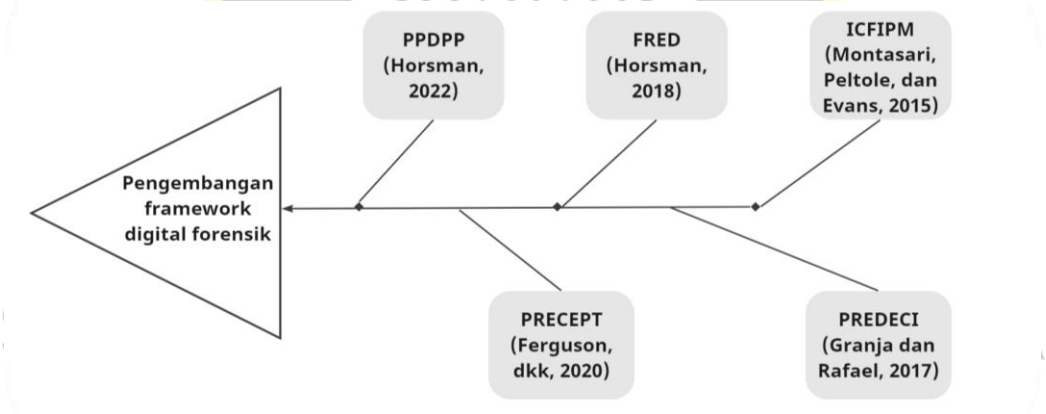
No.	Metode	Kelebihan	Kekurangan
		kesalahan atau kehilangan bukti digital. • PRECEPT mencakup panduan praktis yang dapat membantu ahli forensik dalam menentukan strategi dan langkah-langkah investigasi forensik yang sesuai dengan situasi yang dihadapi. • PRECEPT menekankan pentingnya etika dan privasi dalam melakukan investigasi forensik.	• PRECEPT kurang fleksibel dalam mengakomodasi berbagai jenis investigasi forensik yang kompleks atau sulit.
5	PPDPP	• PPDPP memberikan solusi yang inovatif dalam mengintegrasikan prinsip privasi dalam investigasi forensik. • PPDPP dapat membantu ahli forensik untuk mengambil dan memproses data dalam cara yang lebih aman dan etis, sehingga tidak merugikan privasi pemilik data.	• PPDPP memerlukan waktu dan upaya yang lebih besar untuk menerapkan prinsip privasi dalam investigasi forensik, yang mungkin mengganggu efisiensi dan produktivitas ahli forensik. • PPDPP memerlukan pengetahuan teknis yang lebih mendalam

Tabel 2.3 Evaluasi *framework* forensik digital (lanjutan)

No.	Metode	Kelebihan	Kekurangan
		• PPDPP juga memberikan panduan praktis untuk ahli forensik dalam menerapkan prinsip privasi dalam investigasi forensik.	dalam hal privasi dan pengolahan data, yang mungkin menjadi tantangan bagi ahli forensik yang tidak memiliki latar belakang teknis yang kuat.

2. 6 Pengembangan *Framework* Forensik digital

Identifikasi, analisis dan evaluasi yang telah dilakukan pada *framework* digital forensik kemudian dipetakan dalam diagram fishbone untuk melihat hubungan kausalitas yang menjadi titik temu penelitian dengan topik yang serupa. Gambar 2.4 menujukkan topik pembahasan utama penelitian terdahulu yang telah ditinjau berkaitan dengan digital forensik.



Gambar 2.4. Peta Kausalitas Penelitian *Framework* Digital Forensik

Topik pengembangan *framework* digital forensik dinilai menarik dan selalu dibahas oleh para peneliti pada artikel ilmiah. Pengembangan dokumen akademik berisi *framework* digital forensik yang memastikan kontrol terhadap kode etik praktisi menjadi bagian dari pembahasan topik tersebut.

Pengembangan *framework* menggunakan metode *Participatory Action Research* (PAR) dilakukan untuk mendapatkan kajian empiris dan teoritis secara sekaligus, dan metode ini banyak digunakan sebagai pendekatan pada penelitian yang melibatkan pemangku kebijakan (*stakeholder*). (Buckles dan Chevalier, 2019). Metode ini dipilih karena PAR menekankan keterlibatan aktif antara peneliti dan pemangku kepentingan (*stakeholder*) dalam seluruh proses penelitian, mulai dari identifikasi masalah, perancangan solusi, hingga evaluasi hasil. Setiap tahapan pengembangan *framework* dapat divalidasi langsung melalui partisipasi para ahli dan praktisi di bidang digital forensik, sehingga menghasilkan temuan yang tidak hanya relevan secara akademik tetapi juga aplikatif di lapangan.

2. 7 Etika di bidang IT

Etika di semua bidang keilmuan, khususnya bidang IT, merupakan hal penting yang perlu diperhatikan, diajarkan, dan diterapkan pada setiap sendi kehidupan manusia. Etika dapat diartikan sebagai moral atau nilai kewajaran seorang manusia terhadap lingkungannya. Interaksi manusia dengan lingkungannya, termasuk ranah teknologi, diharapkan memiliki dampak yang positif, sehingga etika menjadi indikator baik atau buruknya tindakan manusia.

Isu-isu etika dalam bidang teknologi informasi meliputi kerahasiaan, keakuratan, kepemilikan, dan aksesibilitas (Simarmata, Manuhutu dan Yendrianof, 2021). Isu-isu tersebut berpengaruh langsung terhadap legitimasi penerapan teknologi, maka penegakan hukum dalam kasus Teknologi Informasi harus memprioritaskan prinsip etika. Proses investigasi forensik digital berpotensi menimbulkan pelanggaran hak individu jika penanganannya tidak dilakukan secara etis, sehingga pengungkapan kasus kejahatan siber harus mengutamakan etika sebagai mekanisme pengendali. Pengungkapan kasus kejahatan siber harus mengutamakan prinsip etika untuk menjaga integritas institusi hukum. Setiap profesional yang terlibat dalam proses penanganan perkara wajib menegakkan etika secara disiplin karena integritas institusi hukum ditentukan oleh konsistensi penerapan standar etika. Penerapan etika dalam ranah hukum dan teknologi

informasi berfungsi sebagai landasan normatif untuk memastikan keadilan serta konsistensi dalam setiap tahapan investigasi.

Etika terkait dengan proses forensik terdiri dari privasi "keras" dan "lunak" (Saleem, Popov, dan Bagilli, 2014). Privasi keras atau *hard privacy* berarti berbagi data sesedikit mungkin sedangkan privasi lunak atau *soft privacy* dapat diartikan bahwa subjek investigasi kehilangan kendali atas data mereka dan harus mempercayai profesionalisme penyelidik (Deng, dkk., 2010). Penyelidik dalam bidang forensik digital harus merahasiakan data apapun, kecuali secara khusus diharuskan oleh hukum untuk mengungkapkannya.

Kode etik untuk forensik digital sangat dibutuhkan, tetapi saat ini belum ada kode etik yang diterima secara universal (Sloan, 2015). Losavio, Seigfried-Spellar, dan Sloan menyoroti kode etik untuk profesi di forensik digital (Losavio, Seigfried-Spellar, dan Sloan, 2016). Pembahasan mengenai etik di forensik digital menyoroti beberapa masalah, salah satunya *privacy* dan *confidentiality*.

Balogun dan Zuva dalam artikelnya membahas elemen-elemen penting dari *framework* forensik digital. Topik atau elemen yang perlu dibahas terkait pemahaman kode etik forensik digital menurut mereka yaitu *ethical concerns in information systems, information systems vs digital forensic systems, open ethical concerns in digital forensic systems, measures for identified concerns* (Balogun dan Zuva, 2017).

2. 8 Pelanggaran Etika Forensor Di Indonesia

Perkembangan teknologi informasi telah menjadikan forensik digital sebagai komponen krusial dalam sistem pembuktian hukum di Indonesia. Peran forensor tidak hanya terbatas pada penguasaan teknis akuisisi dan analisis bukti digital, tetapi juga menuntut kepatuhan ketat terhadap prinsip etika, hukum acara, serta perlindungan hak asasi manusia. Integritas proses forensik menjadi faktor penentu sah atau tidaknya alat bukti elektronik dalam proses peradilan, sebagaimana diatur dalam Kitab Undang-Undang Hukum Acara Pidana, Undang-

Undang Informasi dan Transaksi Elektronik, serta Undang-Undang Pelindungan Data Pribadi (Fahrezi Abdullah, 2023).

Pelanggaran-pelanggaran etika forensik yang terjadi di Indonesia menunjukkan adanya kesenjangan antara praktik teknis di lapangan dengan kerangka hukum dan regulasi yang berlaku. Pelanggaran tersebut mencakup akuisisi barang bukti tanpa dasar hukum yang sah, manipulasi atau perubahan data elektronik, pengabaian prinsip *chain of custody*, hingga penyalahgunaan dan kebocoran data pribadi (Bani & Al-Maliki, 2023). Tindakan-tindakan tersebut tidak hanya mencederai prinsip profesionalisme forensor, tetapi juga berpotensi menimbulkan konsekuensi hukum serius berupa tidak sahnya alat bukti, pelanggaran hak privasi, serta terjadinya salah putusan. Tabel 2.4 menunjukkan setiap penyimpangan prosedural dari forensor memiliki implikasi hukum yang jelas dan dapat dipertanggungjawabkan secara normatif. Pendekatan ini menegaskan bahwa etika forensik tidak bersifat abstrak melainkan terikat langsung pada aturan hukum yang berlaku.

Tabel 2.4 Pemetaan pelanggaran forensor dan regulasi yang dilanggar

No	Materi pelanggaran forensor	Regulasi yang dilanggar	Penjelasan keterkaitan hukum
1	Akuisisi CCTV langsung pada barang bukti asli tanpa prosedur forensik	UU No. 11 Tahun 2008 jo. UU No. 19 Tahun 2016 (UU ITE) Pasal 30 ayat (1) & Pasal 32 ayat (1)	Akses dan/atau perubahan data elektronik tanpa hak, berpotensi merusak integritas barang bukti
2	Akses perangkat tanpa izin/surat perintah	UUD 1945 Pasal 28G ayat (1); KUHAP Pasal 38	Melanggar hak atas rasa aman dan perlindungan harta benda serta prosedur penyitaan
3	Menggunakan data hasil peretasan sebagai bukti resmi	UU ITE Pasal 30 ayat (2)-(3)	Data diperoleh secara melawan hukum, tidak sah sebagai alat bukti

Tabel 2.4 Pemetaan pelanggaran forensor dan regulasi yang dilanggar (lanjutan)

No	Materi pelanggaran forensor	Regulasi yang dilanggar	Penjelasan keterkaitan hukum
4	Pelanggaran privasi & data pribadi saat akuisisi	UU No. 27 Tahun 2022 (UU PDP) Pasal 20, 21, 35	Pemrosesan data pribadi tanpa dasar hukum yang sah
5	Mengubah/menghapus/ menambah data sehingga hash tidak sesuai	UU ITE Pasal 32 ayat (1)-(2)	Perubahan dan perusakan informasi elektronik
6	Tidak menjaga *chain of custody*	KUHAP Pasal 183; Perkap Polri No. 10 Tahun 2010	Bukti menjadi tidak meyakinkan dan dapat dikesampingkan hakim
7	Analisis langsung pada *evidence* asli tanpa *forensic image*	Perkap Polri No. 10 Tahun 2010 Pasal 7	Melanggar prinsip kehati-hatian dan keilmiahan pembuktian
8	Tidak mengikuti standar/*guideline* forensik	UU No. 14 Tahun 2008 (KIP) Pasal 7 ayat (2)	Proses tidak transparan dan tidak akuntabel
9	Ketidakmampuan teknis (*mishandling tools*)	KUHP Pasal 359 (kelalaian)	Kelalaian profesional yang merugikan proses hukum
10	Tidak mendokumentasikan proses forensik	Perkap Polri No. 10 Tahun 2010 Pasal 13	Proses tidak dapat diaudit atau diverifikasi
11	Mengakses data pribadi yang tidak relevan	UU PDP Pasal 3 & 35	Melanggar prinsip purpose limitation
12	Membocorkan hasil analisis ke pihak luar	KUHP Pasal 322; UU PDP Pasal 67	Pelanggaran kerahasiaan jabatan
13	Menyalahgunakan data untuk kepentingan pribadi	KUHP Pasal 362 / 378	Pencurian atau penipuan berbasis data
14	Memanipulasi bukti untuk mendukung narasi tertentu	KUHP Pasal 263	Pemalsuan dokumen/alat bukti
15	Memalsukan laporan forensik atau *metadata*	KUHP Pasal 266	Memberikan keterangan palsu dalam dokumen resmi

Tabel 2.4 Pemetaan pelanggaran forensor dan regulasi yang dilanggar (lanjutan)

No	Materi pelanggaran forensor	Regulasi yang dilanggar	Penjelasan keterkaitan hukum
16	*Overclaiming* (kesimpulan di luar bukti ilmiah)	KUHAP Pasal 186	Keterangan ahli harus berbasis keahlian dan fakta
17	Memberi akses *image* forensik ke pihak tak berwenang	UU PDP Pasal 31	Pengungkapan data tanpa hak
18	Penyimpanan evidence di media tidak aman	UU PDP Pasal 39	Kegagalan pengamanan data pribadi
19	Tidak menerapkan prinsip *least privilege*	PP No. 71 Tahun 2019 Pasal 14	Kewajiban pengendalian akses sistem elektronik
20	Pelanggaran etik profesi forensik	Kode Etik Profesi Polri / Ahli Digital Forensik	Pelanggaran standar integritas, objektivitas, dan independensi

Pemetaan pelanggaran etika forensor terhadap regulasi di Indonesia menunjukkan bahwa mayoritas penyimpangan forensik digital memiliki dimensi hukum yang konkret dan terukur. Pelanggaran prosedural bersifat teknis maupun administratif, berpotensi melanggar ketentuan Undang-Undang ITE, Undang-Undang Pelindungan Data Pribadi, KUHAP, serta peraturan pelaksana lainnya. Kondisi ini menegaskan bahwa kesalahan forensik tidak dapat dipandang sebagai kekeliruan teknis semata, melainkan sebagai tindakan yang dapat menimbulkan konsekuensi hukum dan etika secara bersamaan.

2. 9 Privasi Data

Forensik digital adalah salah satu cabang ilmu forensik yang berfokus pada investigasi perangkat digital. Forensik digital saat ini menjadi bagian yang umum pada investigasi kejahatan dan juga dan juga menjadi fitur dalam situasi lain seperti respons insiden perusahaan yang dihasilkan dari serangan terhadap sistem informasi (Neale, dkk., 2022). Urgensi forensik digital pada proses investigasi adalah untuk mendukung atau menyanggah asumsi dari motif kejahatan pada barang bukti digital.

Studi yang dilakukan telah mempelajari konflik antara perlindungan data pribadi dengan forensik komputer. Hal tersebut sangat dimaklumi karena hampir tidak mungkin ada proses investigasi forensik digital tanpa pelanggaran terhadap prinsip keamanan informasi. Prinsip keamanan informasi yang dimaksud adalah *confidentiality, integrity*, dan *availability* (Halboob, dkk., 2015).

Perlindungan privasi yang diberikan dapat melalui kebijakan (misalnya aturan etika, kebijakan) atau solusi keamanan informasi lainnya seperti audit dan kontrol akses. Pemilik data membangun kepercayaannya atas perlindungan privasi yang diberikan oleh investigator, yang dapat diartikan bahwa tingkat kepercayaan adalah tentang seberapa besar kepercayaan pemilik data terhadap otoritas investigasi dalam hal solusi perlindungan privasi yang diberikan.

2. 10 *Framework* Forensik digital

Pembahasan mengenai *framework* bidang forensik digital mulai dari mengakses perangkat yang terproteksi password (Bang, Park, dan Lee, 2022), pengungkapan bukti multimedia, hingga *framework* untuk proses forensik digital yang etis. Kerangka kerja ini dibuat untuk meningkatkan kualitas proses forensik digital (Ferguson, dkk., 2020).

Hasil proses forensik digital tidak terhindar dari permasalahan bias interpretasi. Renauld menyebutkan, sebagian besar bias ini terpengaruh pada lingkungan eksternal dan kebijakan. Kesadaran akan adanya bias dan implementasi *framework* ini bertujuan untuk mencegah kepincangan subjektifitas yang terjadi pada proses investigasi di peradilan (Renaud, dkk., 2021).

Pengusulan *framework* forensik digital telah beberapa kali dilakukan oleh akademisi dengan beberapa pertimbangan dan studi kasus. Penelitian ini mengusulkan satu *framework* yang dirancang berdasarkan pelanggaran etika sebagai parameter yang harus dihindari.