OPEN ACCESS
J. OF INISTA, VOL. 1, NO. 1, PP.63-70, SEPT 2018

E-ISSN 2622-8106
DOI: 10.20895/INISTA.V1I1

Journal of Informatics, Information System, Software Engineering and Applications

Studi Komparasi Investigasi Digital Forensik pada Tindak Kriminal

Muhammad Nur Faiz #1, Wahyu Adi Prabowo #2, Muhammad Fajar Sidiq #3

 # Program Studi Informatika, Fakultas Teknologi Industri dan Informatika
Institut Teknologi Telkom Purwokerto
Jl. D. I. Panjaitan No. 128, Purwokerto, Jawa Tengah 53147, Indonesia

[1] faiz@ittelkom-pwt.ac.id
[2] wahyuadi@ittelkom-pwt.ac.id
[3] fajar@ittelkom-pwt.ac.id

Accepted on September 27, 2018

Abstract

Investigasi digital forensik telah mengalami perubahan luar biasa dalam dekade akhir ini. Dari komputer awal hingga perangkat seluler saat ini dan perangkat penyimpanan. Digital forensik sangat penting untuk proses penuntutan terhadap penjahat digital yang melibatkan perangkat digital. Proses dalam menganalisis investigasi digital forensik membutuhkan suatu model ataupun framework agar proses investigasi tersebut dapat berjalan dengan lebih detail dan terstruktur. Seperti pada penelitian yang sebelumnya, tidak ada satu pun standar yang membahas semua proses investigasi forensik digital. Proliferasi kejahatan digital di dunia yang banyak dan beragam mengakibatkan model investigasi juga berkembang untuk dapat menemukan bukti digital. Pada beberapa penelitian sebelumnya telah banyak membahas mengenai model ataupun framework dalam menginvestigasi suatu kasus digital forensik, dan model-model tersebut dapat digunakan secara luas. Beberapa model membahas sebuah proses yang mendetail dan ada yang membahas sebuah proses secara umum, hal ini dapat menyebabkan investigator digital forensik kesulitan dalam memilih model yang tepat dalam menginvestigasi suatu kasus. Investigasi digital forensik harus dilaksanakan dengan efektif, efisien dan terstruktur, dengan sejumlah langkah signifikan yang harus dipertimbangkan. Setiap langkah dan fase haruslah menghasilkan dokumentasi yang penting dalam memahami bagaimana proses penyelidikan dibangun. Tujuan dari penelitian ini adalah mempelajari dan membandingkan model investigasi digital forensik Penelitian ini juga mencakup definisi dan deskripsi konsep dasar yang digunakan kerangka kerja atau model.

Keywords: Digital Forensik, Model, Investigasi, Perbandingan

I. PENDAHULUAN

Digital forensik saat ini semakin penting dengan beberapa insiden keamanan informasi yang rentan dan terus menerus menyorotinya. Pada digital forensik terdapat dua metode, yakni *static forensic* dan *live forensic*. *Static forensic* dimanamendapatkan datanya dari data yang disimpan secara permanen dalam perangkat media penyimpanan pada umumnya hardisk. *Live forensic* membutuhkan data dari sistem yang sedang berjalan atau data *volatile* yang biasanya *Random Access Memory* (RAM) atau transit pada jaringan [1]. Bukti digital atau elektronik terdiri dari informasi dan data nilai yang disimpan atau ditransmisikan oleh

perangkat digital [2]. Dengan demikian, bukti elektronik adalah bukti laten dalam arti yang sama bahwa sidik jari atau bukti DNA adalah laten [3]. Berkaitan dengan bukti digital, sangat diperlukan proses standar dan diformalkan agar bukti digital dapat diterima di pengadilan. Metode forensik merupakan faktor penting yang mendukung untuk investigasi tindak kejahatan yang lebih efektif dan efisien dalam menangani sebuah kasus [4]. Metode dan model proses forensik digital telah banyak dikembangkan oleh praktisi dan penyelidik forensik, berdasarkan pengalaman pribadi dan keahlian, pada basis ad hoc untuk mencapai standardisasi di tempat kejadian pelanggaran. Dalam dekade terakhir, ada juga sejumlah proyek penelitian akademis yang dilakukan untuk membentuk model proses penyelidikan forensik digital. Namun demikian, saat ini tidak ada standar internasional yang memformalkan proses investigasi forensik digital, meskipun upaya untuk menstandardisasi proses telah dimulai dalam International Standardization Organization (ISO) [5].

Fokus dari investigasi forensik digital adalah pada kejahatan yang dilakukan melalui komputer [6]. Namun, selama beberapa tahun terakhir tahun, bidang telah diperluas untuk memasukkan berbagai perangkat digital lainnya di mana informasi yang disimpan secara digital dapat diproses dan digunakan untuk berbagai jenis kejahatan [2]. Investigasi digital forensik, selanjutnya disebut sebagai *Digital forensics Investigations* (DFI), adalah fase menghubungkan informasi yang diekstraksi dan bukti digital untuk membangun informasi faktual untuk ditinjau oleh lembaga peradilan [6], [2]. Cohen [7] menyoroti kebutuhan untuk menetapkan informasi faktual sebagai hasil dari penyelidikan semacam itu. DFI dilakukan sebagai investigasi setelah terjadinya insiden [8]. Oleh karena itu merupakan jenis penyelidikan yang berbeda “di mana prosedur ilmiah dan teknik yang digunakan akan memungkinkan hasil, dengan kata lain bukti digital, dapat diterima di pengadilan [9].

Beberapa model cenderung sangat detail dan yang lain mungkin terlalu umum. Ini mungkin agak sulit atau bahkan membingungkan, terutama bagi penyelidik forensik pemula untuk mengadopsi model investigasi yang benar atau sesuai [10]. Langkah-langkah atau fase yang umum dalam semua model proses adalah:

- Pengumpulan: Bukti-bukti dapat dikumpulkan dalam fase ini
- Pemeriksaan: Pemeriksaan berdasarkan bukti asal.
- Analisis: Pencarian atau inspeksi berdasarkan pemeriksaan.
- Pelaporan: Kesimpulan dari semua fase.

Penelitian ini dimulai dengan review dari beberapa model investigasi forensik digital yang ada, menganalisis model yang ada untuk mengidentifikasi kekuatan dan beberapa kelemahan yang melekat pada model-model investigasi tersebut.

II. KAJIAN PUSTAKA

Pada bagian ini, model investigasi forensik digital dan kerangka kerja yang telah dilakukan oleh beberapa peneliti. Perkembangan beberapa model investigasi digital forensik di antaranya terfokus pada respons insiden atau investigasi atau menekankan fase atau aktivitas tertentu dari penyelidikan. Di bawah ini adalah deskripsi singkat dari proses pengembangan model.

Sebuah makalah penelitian berjudul "A New Approach of Digital Forensic Model for Digital Forensic Investigation”. Fokus dari penelitian ini adalah untuk mengusulkan pendekatan yang terstruktur dan konsisten untuk penyelidikan forensik digital. Untuk meningkatkan proses investigasi, model baru telah diusulkan yang bertujuan mengidentifikasi kegiatan dan membantu meningkatkan proses penyelidikan. Penelitian ini juga telah membahas model yang ada yang telah diusulkan sebelumnya seperti: Model SDFIM, model IDIP, Model Proses Forensik, dan lainnya. Model yang berbeda memiliki fase yang berbeda untuk melakukan penyelidikan digital. Model yang diusulkan ini, membagi proses penyelidikan menjadi empat tingkatan berdasarkan fase. Tingkat pertama terdiri dari empat fase yaitu persiapan, identifikasi, otorisasi dan komunikasi. Tingkat kedua terdiri dari tiga fase yang meliputi: pengumpulan, pelestarian dan dokumentasi. Tingkat ketiga juga terdiri dari tiga fase seperti pemeriksaan, pengujian dan analisis eksplorasi dan akhirnya tingkat keempat yang terdiri dari fase presentasi [11].

Studi Penelitian lainnya berjudul "Common Phases of Computer Forensics Investigations Models". Penelitian ini mengusulkan model investigasi baru yang disebut dengan model *Generic Computer Forensic Investigation Model* (GCFIM) dengan 5 tahapan [12]:

- *Pre-Process*: investigator melakukan hal yang berkaitan dengan pekerjaan sebelum melakukan investigasi, seperti mempersiapkan surat dan dokumen resmi, dan juga mempersiapkan alat atau *tools* yang akan digunakan.
- *Acquisition & Preservation*: Pada tahap ini, semua data yang relevan diambil, disimpan dan dipersiapkan untuk tahap selanjutnya. Tahap ini juga investigator mengamankan barang bukti dengan cara menggandakan dan memberikan blocking terhadapa barang bukti kemudian disimpan di tempat yang aman.
- *Analysis*: tahapan ini merupakan proses utama dalam penyelidikan komputer forensik, yakni dilakukan analisa pada data yang telah diperoleh pada tahap sebelumnya untuk dilakukan identifikasi sumber kejahatan, motif kejahatan dan pada akhirnya menemukan orang yang bertanggungjawab atas kejahatan tersebut.
- *Presentation* : tahapan ini melakukan presentasi terhadap hasil yang sudah didapatkan. Hasil dari tahap ini adalah untuk membuktikan dan/atau menyangkal dugaan tindak kejahatan.
- *Post-Process*: Tahapan ini merupakan tahapan akhir, yang mana bukti digital dan fisik harus dikembalikan kepada pemilik yang sah dan disimpan di tempat yang aman. Investigator meninjau ulang proses investigasi yang telah dilakukan agar dapat digunakan untuk perbaikan proses penyelidikan selanjutnya.

Penelitian lainnya yang berhubungan dengan model investigasi forensik adalah penelitian Agarwal, dkk [9] yang mempelajari model yang berbeda dan mengusulkan model baru berdasarkan hasil sebelumnya. Makalah ini mengusulkan perbandingan model yang berbeda dan atas dasar model yang diusulkan, model sistematis prosedur forensik digital muncul. Salah satu keuntungan utama dari model yang diusulkan ini adalah untuk menyediakan mekanisme kerangka kerja untuk dapat diterapkan di negara-negara atas dasar teknologi. Model ini menyediakan cara sistematis untuk menganalisis kecurangan cyber dan kejahatan dunia maya sesuai dengan teknologi yang digunakan di negara masing-masing

Penelitian selanjutnya tentang model investigasi digital forensik yang dilakukan oleh Sabah dan Bashayer [13] mengusulkan model tanpa membandingkan model sebelumnya atau yang sudah diteliti. Pada penelitian ini model didasarkan pada aliran yang diusulkan. Aliran ini menceritakan arah yang tepat dan akurat di mana informasi atau bukti dipisahkan ke dalam aliran aliran yang berbeda. Model yang diusulkan membahas tahap-tahap yang akan membantu dalam memisahkan aliran aliran. Fase meliputi: membuat, merilis, mentransfer, tiba, menerima, dan memproses

Penelitian lainnya dilakukan oleh Kyai, Zavarsky, dkk [14] membahas tentang salah satu kelemahan signifikan dalam penyelidikan forensik digital adalah bahwa mereka sering tidak menempatkan penekanan yang cukup pada potensi diterimanya bukti yang dikumpulkan. Investigasi forensik digital harus mematuhi standar bukti dan diterimanya tuntutan untuk penuntutan yang sukses. Oleh karena itu, sifat techno-legal dari model yang diusulkan ini digabungkan dengan penggabungan praktik terbaik dari model yang ada membuatnya unik. Model ini bukan model air terjun, tetapi bersifat iteratif membantu penyelidikan dan penuntutan yang sukses. Hasil dari penelitian ini diharapkan dapat meningkatkan seluruh proses investigasi termasuk kemungkinan litigasi.

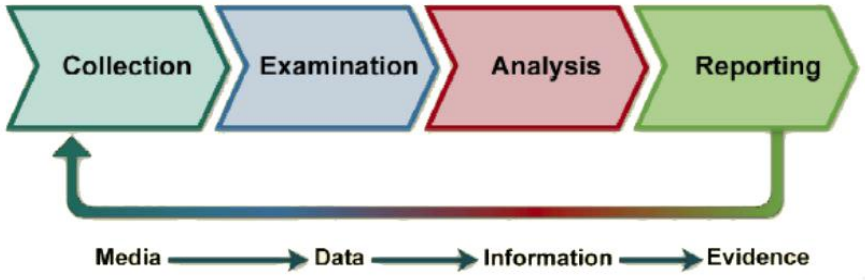
III. HASIL ANALISA

Pada pembahasan sebelumnya bahwa semua model memiliki kelebihan dan kelemahan. Model-model tersebut dikaji secara mendalam dari langkah, fase atau tahapannya setiap modelnya, sehingga nantinya investigator dapat memilih model mana yang akan digunakan dan sesuai dengan yang dibutuhkan. model investigasi digital forensik yang akan dikaji seperti National Institute of Justice (NIJ), Digital Forensics

Research Conference (DFRWS), Integrated Digital Forensics Investigation Framework (IDFIF), Generic Computer Forensic Investigation Model (GCFIM), Systematic digital forensic investigation model (SRDFIM).

A. National Institute of Justice (NIJ)

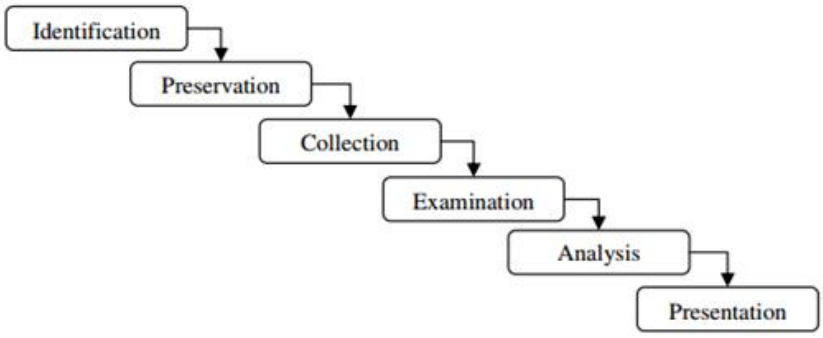
NIJ menerbitkan model proses dalam Investigasi sebagai panduan untuk responden pertama. Model ini mempuyai empat langkah yang terdiri dari tahap pengumpulan, pemeriksaan, analisis dan pelaporan. Fase pengumpulan berkaitan dengan perolehan berbagai bentuk bukti, fase pemeriksaan melakukan pengambilan bukti digital nilai probatif dari bukti yang dikumpulkan. Interpretasi hasil berasal dari fase pemeriksaan dengan bantuan teknik dan metodologi yang tepat dilakukan pada tahap analisis . Tahap keempat dan terakhir meliputi kegiatan seperti presentasi bukti, alat dan prosedur yang digunakan serta perumusan pedoman dan rekomendasi untuk perbaikan jika ada [15].



Gambar 1. Model Investigasi NIJ

B. Digital Forensics Research Workshop (DFRWS)

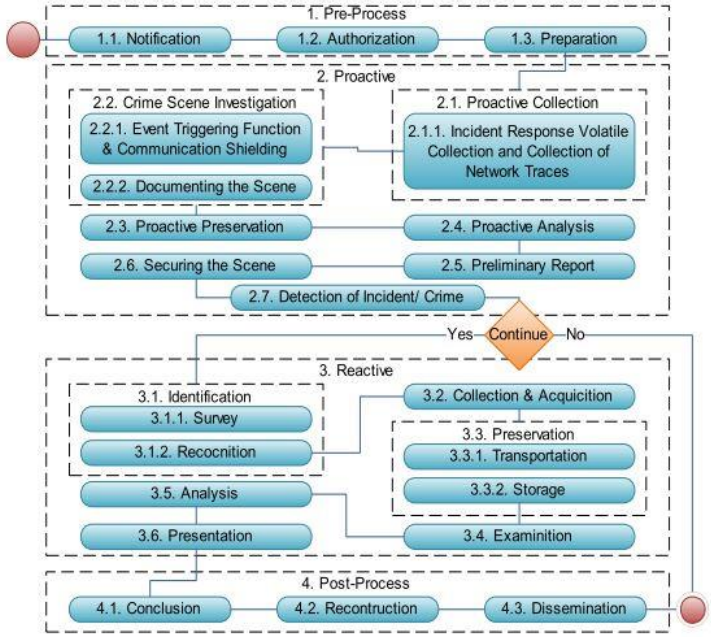
Model investigasi DFRWS ini meliputi enam tahapan dengan tahap pertama yaitu identifikasi. Tahap ini untuk melakukan penentuan kebutuhan yang akan diperlukan untuk penyelidikan dan pencarian bukti digital. Tahap kedua Pemeliharaan yaitu untuk menjaga bukti bukti dan memastikan keaslian atau integritas barang bukti sehingga bukti benar-benar valid/sah. Tahap ketiga yaitu tahap pengumpulan, merupakan tahap untuk identifikasi mengumpulkan sumber bukti yang berpotensi menjadi bukti yang kuat. Tahap keempat adalah tahap pemerikasaan yaitu tahapan untuk menentukan apa saja yang akan dianalisa atau lebih dikenal dengan filterisasi data, sehingga investigator dapat lebih fokus dalam melakukan tahapan selanjutnya. Tahap kelima adalah analisis yaitu tahap untuk mencari dan mengolah data termasuk data diperoleh dari mana, siapa yang membuuat dan bagaimana data tersebut dihasilkan. Tahap terakhir adalah tahap presentasi yaitu tahap dimana melaporkan dan mempresentasikan hasil analisa sehingga dapat dipahami oleh publik [16].



Gambar 2. Model Investigasi DFRWS

C. Integrated Digital Forensics Investigation Framework (IDFIF)

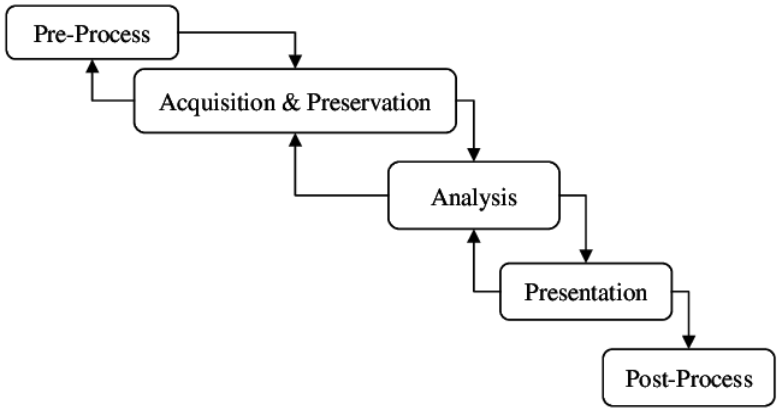
Metode IDFIF merupakan pengembangan dari sequential logic dari proses utama pada DFIF. Metode ini ini terbagi menjadi empat tahapan yakni Pre-Process, Proactive, Reactive dan Post-Process. Tahapan Pre-Process meliputi Notification, Authorization, Preparation. Tahapan Proactive ini ada tujuh sub-tahapan pendukung yakni : Proactive Collecction, Crime Scene Investigation, Proactive preservation, Proactive Analysis, Preliminary Report, Securing the Scene, Detection of Incident / Crime. Tahapan Reactive merupakan tahapan yang meliputi Identification, Collection & Acquisition, Preservation, Examination, Analysis dan Presentation. Tahapan Post-Process merupakan tahapan yang meliputi Conclusion, Reconstruction, Dissemination [17].



Gambar 3. Model Investigasi IDFIF

D. Generic Computer Forensic Investigation Model (GCFIM)

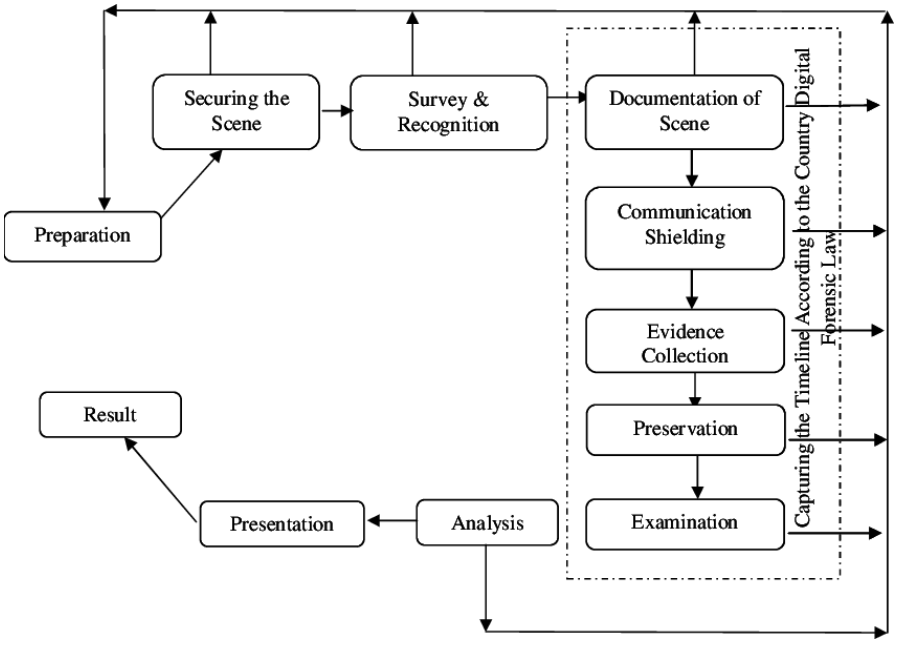
Model GCFIM, metode dengan 5 tahapan. Tahap pertama Pra-Proses, tahap ini berkaitan dengan semua yang perlu dilakukan sebelum penyelidikan dan pengumpulan data resmi. Tahap berikutnya yaitu tahap Akuisisi & Pelestarian, tahap yang terkait dengan identifikasi, mendapatkan, menngumpulkan menyimpan dan melestarikan data atau bukti yang didapat. Tahap selanjutnya adalah Analisis. Tahap dimana inti dari digital forensik. Berbagai hal analisis dilakukan pada data yang diperoleh untuk mengidentifikasi sumber kejahatan. Tahap keempat adalah Presentasi. Data, informasi atau bukti temuan dari tahap analisis didokumentasikan dan dipresentasikan. Invstigator harus mempresentasikan dengan bahasa yang mudah dipahami oleh semua pihak, tetapi juga harus didukung dengan bukti yang dapat diterima. tahap terakhir yaitu Post-Process. Tahapan ini untuk mengembalikan barang bukti digital dan fisik kepada yang berwenang. Bukti ini nantinya dapat dijadikan sumber belajar atau untuk pelatihan [12]



Gambar 4. Model Investigasi GCFIM

E. Systematic digital forensic investigation model (SRDFIM)

Model investigasi SRDFIM merupakan tahapan yang akan membantu dalam dinamika bukti dan rekonstruksi peristiwa dengan menyadari sifat Individualitas, Repeatability, Keandalan, Kinerja, Testability, Skalabilitas, Kualitas dan Standar dalam analisis penipuan komputer dan kejahatan cyber (CFCC). Model SRDFIM ini memiliki beberapa tahapan dari tahap Persiapan, Pengamanan TKP, Survei dan Pengakuan, Mendokumentasikan Adegan, Pelindungan Komunikasi, Pengumpulan Bukti, Pelestarian Butki, Pemeriksaan, Analisis, Presentasi, Hasil & Tinjauan [9]



Gambar 5. Model Investigasi SRDFIM

Model invsetigasi digital forensik yang telah dijelaskan merupakan model yang sudah digunakan oleh peneliti dengan skenario kasus tertentu. Namun, belum ada yang menjadi acuan model investigasi di dunia.. Perbandingan model yang telah dipaparkan sebelumnya diringkas pada tabel 1.

TABEL I
ANALISIS PERBANDINGAN MODEL INVETIGASI DIGITAL FORENSIK

Tahapan	NIJ	DFRWS	IDFIF	GCFIM	SRDFIM
Pengumpulan (Collection/Acquisiition)	✓	✓	✓	✓	✓
Pemeriksaan (Examination)	✓	✓	✓	-	✓
Analisis (Analysis)	✓	✓	✓	✓	✓
Pelaporan (Reporting)	✓	-	✓	-	-
Persiapan (Preparation)	-	-	✓	✓	✓
Pemeliharaan (Preservation)	-	✓	✓	✓	✓
Presentasi (Presentation)	-	✓	✓	✓	✓
Identifikasi (Identification)	-	✓	✓	✓	-
Rekonstruksi (Reconstruction)	-	-	✓	-	-
Dokumentasi (Documentation)	-	-	-	-	✓
Otorisasi (Authorization)	-	-	✓	-	-
Survey	-	-	✓	-	✓
Komunikasi (Communication)	-	-	-	-	✓
Transportasi (Transportation)	-	-	✓	-	-

IV. KESIMPULAN

Model investigasi belum memiliki pedoman yang mutlak sehingga masih dikembangkan sesuai dengan kebutuhan. Model-model di atas terdapat beberapa persamaan dan perbedaan pada setiap tahapannya. Model ini bisa digunakan sesuai dengan kepentingan dan kebutuhan investigator. Tujuan dari penelitian ini membandingkan berbagai model investigasi untuk membantu investigator untuk menggunakan dalam bermacam-macam skenario kasus, dimana setiap model ini dapat dengan mudah diadopsi penerapannya yang sudah senior maupun junior.

REFERENCES

[1] M. Nur Faiz, R. Umar, and A. Yudhana, "Implementasi Live Forensics untuk Perbandingan Browser pada Keamanan Email," *J. Inform. Sunan Kalijaga*, vol. 1, no. 3, pp. 108–114, 2017.

[2] R. Montasari, "Review and Assessment of the Existing Digital Forensic Investigation Process Models," *Int. J. Comput. Appl.*, vol. 147, no. 7, pp. 1–9, 2016.

[3] A. Valjarevic and H. Venter, "Analyses of the State-of-the-art Digital Forensic Investigation Process Models," *South. Africa Telecommun. Networks Appl. Conf.*, 2012.

[4] R. Umar, A. Yudhana, and M. N. Faiz, "Analisis Kinerja Metode Live Forensics Untuk Investigasi Random Access Memory Pada Sistem Proprietary," in *Prosiding Konferensi Nasional Ke- 4 Asosiasi Program Pascasarjana Perguruan Tinggi Muhammadiyah (APPPTM)*, 2016, pp. 207–211.

[5] ISO 27043, "INTERNATIONAL STANDARD ISO / IEC 27043: Information technology — Security techniques — Incident investigation principles and processes," 2015.

[6] E. Casey, *Digital Evidence and Computer Crime - Third edition*. Maryland: Elsevier, 2011.

[7] F. Cohen, "Chapter 2 TOWARD A SCIENCE OF DIGITAL FORENSIC EVIDENCE EXAMINATION," in *6th IFIP WG 11.9 International Conference on Digital Forensics*, 2010, pp. 17–35.

[8] T. Charles and M. Pollock, "Digital forensic investigations at universities in South Africa," in *2015 Second International Conference on Information Security and Cyber Forensics (InfoSec)*, 2015, pp. 53–58.

[9] A. Agarwal, M. Gupta, S. Gupta, and C. S. Gupta, "Systematic Digital Forensic Investigation Model," *Int. J. Comput. Sci. Secur.*, vol. 5, no. 1, pp. 118–131, 2011.

[10] S. Rani, "DIGITAL FORENSIC MODELS : A COMPARATIVE ANALYSIS," *Int. J. Manag. IT Eng.*, vol. 8, no. 6, pp. 432–443, 2018.

[11] I. O. Ademu, C. O. Imafidon, and D. S. Preston, "A New Approach of Digital Forensic Model for Digital Forensic Investigation," *Int. J. Adv. Comput. Sci. Appl.*, vol. 2, no. 12, pp. 175–178, 2011.

[12] Y. Yusoff, R. Ismail, and Z. Hassan, "Common Phases of Computer Forensics Investigation Models," *Int. J. Comput. Sci. Inf. Technol.*, vol. 3, no. 3, pp. 17–31, 2011.

[13] S. Al-fedaghi and B. Al-babtain, "Modeling the Forensics Process," *Int. J. Secur. Its Appl.*, vol. 6, no. 4, pp. 97–108, 2012.

[14] K. Kyei, P. Zavarsky, D. Lindskog, and R. Ruhl, "A Review and Comparative Study of Digital Forensic Investigation Models," *Digit. Forensics Cyber …*, pp. 314–327, 2013.

[15] G. Shrivastava, K. Sharma, and A. Dwivedi, "FORENSIC COMPUTING MODELS: TECHNICAL OVERVIEW," *Comput. Sci. Inf. Technol.*, vol. 02, no. 02, pp. 207–216, 2012.

[16] A. L. Suryana, R. R. El Akbar, and N. Widiyasono, "Investigasi Email Spoofing dengan Metode Digital Forensics Research Workshop (DFRWS)," *J. Edukasi dan Penelit. Inform.*, vol. 2, no. 2, pp. 111–117, 2016.

[17] Y. D. Rahayu and Y. Prayudi, "Membangun Integrated Digital Forensics Investigation Frameworks (IDFIF) Menggunakan Metode Sequential Logic," in *Seminar Nasional Teknologi Informasi dan Komunikasi 2014 (SENTIKA 2014)*, 2014, vol. 2014, no. Sentika.