ANALISIS ARTIKEL DIGITAL FORENSIK

Studi Komparasi Investigasi Digital Forensik pada Tindak Kriminal

Dosen: Robby Anggriawan SE., ME.

Nama Anggota Kelompok 1:

Muhammad Alfian (2141764173)

Arditiya Pratama (2141764170)

(2141764)

SIB 4D

POLITEKNIK NEGERI MALANG

JURUSAN TEKNOLOGI INFORMASI

PROGRAM STUDI SISTEM INFORMASI BISNIS

2023

PENGERTIAN STUDI KASUS

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*I 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].

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].

UNTUK NAVIGASI MEMAKAI MODEL GCFIM

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.

HASIL ANALISIS

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).

Berdasarkan perbandingan model-model investigasi digital forensik yang telah dijelaskan sebelumnya, dapat disimpulkan bahwa setiap model memiliki karakteristik unik dan keunggulan masing-masing. National Institute of Justice (NIJ) menawarkan panduan sistematis dan terstruktur, khususnya untuk responden pertama, sementara Digital Forensics Research Conference (DFRWS) memberikan pendekatan yang menyeluruh dan komprehensif. Integrated Digital Forensics Investigation Framework (IDFIF) menonjolkan integrasi antara analisis digital dan penelitian kejahatan, sedangkan Generic Computer Forensic Investigation Model (GCFIM) menawarkan pendekatan umum dan dapat disesuaikan. Systematic Digital Forensic Investigation Model (SRDFIM) menekankan kebutuhan untuk pendekatan sistematis dan berorientasi pada metodologi.

Kelebihan model-model tersebut mencakup panduan yang terstruktur, kemampuan adaptasi, dan fokus pada integrasi analisis. Namun, kelemahan dapat melibatkan tingkat keahlian yang tinggi, kompleksitas yang mungkin tidak sesuai dengan investigasi sederhana, atau keterbatasan dalam panduan teknis dan metode.

Penting untuk diingat bahwa hingga saat ini belum ada model investigasi digital forensik yang diakui secara universal di seluruh dunia. Pemilihan model tergantung pada kebutuhan investigatif spesifik, konteks kasus, dan preferensi lembaga penegak hukum atau organisasi terkait. Seiring dengan perkembangan teknologi dan penelitian lebih lanjut, model-model ini dapat mengalami evolusi dan peningkatan untuk memenuhi tuntutan investigasi digital yang semakin kompleks.

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.

Referensi

[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.