Original Article

e-XXXX-XXXX

Original Article

Investigasi Digital Forensik pada Insiden Kebocoran Data Sistem Informasi

Rakhmadi Rahman[1], Darmiati[2] ✉, Putri Nabila Apriliani[3]
[1,2,3]Institut Teknologi Bacharuddin Jusuf Habibie, Parepare, Indonesia,
Korespondensi Author: darmiati.241031037@mahasiswa.ith.ac.id✉

Abstrak:

Perkembangan sistem informasi yang pesat meningkatkan ketergantungan organisasi pada data digital. Dengan demikian, meningkatnya risiko kebocoran data, yang mengancam keamanan data, reputasi, dan kepercayaan publik. Tujuan penelitian ini untuk menganalisis penerapan investigasi forensik digital dalam menangani insiden kebocoran data serta mengevaluasi kesiapan forensik digital. Metode yang digunakan adalah deskriptif kualitatif dengan pendekatan studi analisis berdasarkan kerangka kerja NIST. Hasil penelitian menunjukkan bahwa dengan menerapkan tahapan investigasi forensik digital secara sistematis, yang mencakup identifikasi, pengumpulan, analisis, dan pelaporan, mampu mengungkap kronologis dan sumber kebocoran data. Studi ini menemukan bahwa kesiapan forensik digital yang baik, melalui pencatatan log yang konsisten, secara signifikan meningkatkan efektivitas dan kecepatan investigasi.

Keywords: Digital Forensik, Kebocoran Data, Investigasi, Kerangka Kerja NIST, Kesiapan Forensik.

Pendahuluan

Perkembangan sistem informasi yang semakin cepat telah membuat organisasi semakin bergantung pada pengelolaan data digital. Penggunaan data digital memungkinkan organisasi untuk meningkatkan efisiensi operasional, mempercepat pengambilan keputusan, dan meningkatkan akurasi informasi. Namun, peningkatan ketergantungan ini juga menimbulkan risiko baru, terutama kebocoran data, yang dapat mengancam keamanan informasi, reputasi organisasi, dan kepercayaan publik. Risiko kebocoran data tidak hanya berdampak finansial, tetapi juga menimbulkan potensi masalah hukum, kerusakan citra, dan sanksi regulasi, sehingga menuntut organisasi untuk menerapkan mekanisme penanganan yang sistematis dan terstruktur (Whitman

Received: November 1, 2025 – Revised: November 12, 2025 - Accepted: Desember 7, 2025 - Published online: January 3, 2026

dan Mattord, 2018). Dalam konteks ini, investigasi forensik digital menjadi salah satu pendekatan yang penting. Proses forensik digital memungkinkan organisasi untuk mengidentifikasi insiden, mengumpulkan bukti, melakukan analisis, dan menyusun laporan secara sistematis, sehingga kronologi dan sumber kebocoran data dapat terungkap dengan jelas. Kerangka kerja National Institute of Standards and Technology (NIST) menyediakan pedoman komprehensif mengenai tahapan investigasi forensik digital, mulai dari identifikasi insiden hingga pelaporan, sehingga setiap langkah dapat dilakukan secara sah, terstruktur, dan dapat dipertanggungjawabkan.

Meskipun literatur mengenai keamanan informasi dan forensik digital telah berkembang, penelitian yang fokus pada penerapan investigasi forensik digital dalam konteks organisasi, khususnya di Indonesia, masih terbatas. Banyak studi sebelumnya lebih menyoroti teori dan praktik di sektor swasta atau pada skala global, sedangkan analisis kesiapan organisasi dan efektivitas prosedur forensik digital dalam konteks lokal masih jarang dilakukan. Hal ini menjadi penting, mengingat kompleksitas insiden digital meningkat, terutama selama pandemi dan krisis ekonomi, yang menuntut pendekatan adaptif dan strategis untuk memitigasi risiko keamanan informasi. Penelitian ini bertujuan untuk menganalisis penerapan investigasi forensik digital dalam menangani insiden kebocoran data pada sistem informasi, sekaligus mengevaluasi tingkat kesiapan organisasi dalam mendukung proses investigasi. Metode penelitian yang digunakan adalah deskriptif kualitatif dengan pendekatan studi analisis berdasarkan kerangka kerja NIST. Dengan pendekatan ini, penelitian dapat menelaah tahapan identifikasi, pengumpulan bukti, analisis, dan pelaporan secara rinci, sekaligus menilai efektivitas prosedur yang diterapkan oleh organisasi.

Hasil penelitian menunjukkan bahwa penerapan tahapan investigasi forensik digital yang sistematis mampu mengungkap kronologi dan sumber kebocoran data secara akurat. Bukti digital, seperti jejak audit, log sistem, dan log akses pengguna, terbukti sangat penting dalam menentukan efektivitas proses investigasi. Penelitian ini juga menekankan pentingnya kesiapan organisasi dalam hal sumber daya manusia, teknologi, dan prosedur internal, karena SDM yang terlatih dan perangkat teknologi yang memadai sangat mempengaruhi keberhasilan investigasi. Secara keseluruhan, penelitian ini diharapkan dapat meningkatkan pemahaman organisasi mengenai pentingnya investigasi forensik digital sebagai bagian dari strategi keamanan informasi. Penelitian ini juga membuka peluang untuk pengembangan analisis bukti digital lebih luas di penelitian selanjutnya, serta memberikan dasar bagi organisasi dalam meningkatkan kesiapan, memperkuat kontrol internal, dan mengelola risiko kebocoran data secara lebih efektif. Dengan demikian, organisasi dapat menjaga reputasi, meningkatkan kepercayaan publik, dan meminimalkan dampak negatif dari insiden kebocoran data.

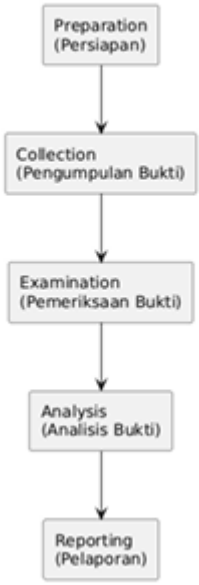
Metode Penelitian

Penelitian ini menggunakan metode deskriptif kualitatif dengan pendekatan studi analitis. Tujuan penelitian adalah untuk memperoleh pemahaman yang mendalam mengenai penerapan investigasi forensik digital dalam menangani insiden kebocoran data pada sistem informasi, tanpa melakukan pengujian atau eksperimen secara langsung. Data dikumpulkan melalui studi literatur yang bersumber dari buku, jurnal ilmiah, dan dokumen resmi terkait.

Analisis dilakukan dengan menggunakan kerangka kerja National Institute of

Received: November 1, 2025 – Revised: November 12, 2025 - Accepted: Desember 7, 2025 - Published online: January 3, 2026

Standards and Technology (NIST), yang mencakup empat tahapan utama, yaitu identifikasi, pengumpulan, analisis, dan pelaporan. Pendekatan ini digunakan untuk memahami peran masing-masing tahapan dalam mengungkap sumber kebocoran data secara kronologis. Selain itu, penelitian ini juga menganalisis konsep kesiapan forensik digital sebagai elemen penting yang dapat meningkatkan efisiensi penyelidikan, khususnya terkait prosedur penanganan insiden dan ketersediaan log sistem (Kent & Chevalier, 2016). Dengan metode ini, penelitian mampu memberikan gambaran sistematis tentang proses investigasi forensik digital serta menilai sejauh mana organisasi siap menghadapi insiden kebocoran data, sehingga hasilnya dapat digunakan sebagai dasar untuk meningkatkan prosedur keamanan informasi dan efektivitas penanganan insiden di masa mendatang.



Gambar 1. Alur Investigasi Forensik Digital Berdasarkan Kerangka NIST

Hasil dan Pembahasan

Berdasarkan hasil analisis literatur dan penerapan kerangka kerja NIST, investigasi forensik digital dapat dilakukan secara sistematis untuk menangani insiden kebocoran data pada sistem informasi. Kerangka kerja NIST memberikan panduan yang terstruktur sehingga setiap tahapan investigasi dapat dilakukan secara berurutan dan terkendali. Alur kerja investigasi digital ini digambarkan secara sistematis pada Gambar 1.Tahap pertama adalah identifikasi, di mana peneliti menentukan jenis kebocoran data yang terjadi, sistem yang terdampak, serta potensi sumber kebocoran. Tahap ini sangat penting karena membantu menetapkan ruang lingkup investigasi dan menghindari kesalahan dalam menangani bukti digital. Identifikasi yang tepat memungkinkan investigator fokus pada aset dan data yang relevan selama proses investigasi.

Tahap berikutnya adalah pengumpulan, yang bertujuan memperoleh bukti digital, seperti jejak audit, log akses pengguna, dan log sistem. Proses pengumpulan dilakukan dengan memperhatikan integritas dan keutuhan data agar bukti tidak berubah selama investigasi. Ketersediaan mekanisme pencatatan log yang baik menjadi faktor kunci yang mendukung keberhasilan tahap pengumpulan ini, karena memastikan bukti digital dapat dianalisis secara akurat pada tahapan selanjutnya.

Received: November 1, 2025 – Revised: November 12, 2025 - Accepted: Desember 7, 2025 - Published online: January 3, 2026

Gambar 1. Alur Analisis dan Temuan Digital Forensik pada Insiden Kebocoran Data

Tahap analisis dilakukan untuk menelusuri tindakan yang terekam dalam bukti digital guna merekonstruksi kronologi kejadian pada kebocoran data. Analisis log sistem dan jejak audit memungkinkan investigator mengidentifikasi pola akses yang mencurigakan serta waktu terjadinya insiden. Tahap ini penting dan merupakan inti dari investigasi forensik digital karena menentukan kesimpulan mengenai sumber kebocoran data (Casey, 2011).

Tahap pelaporan merupakan tahap akhir, di mana seluruh proses dan hasilnya dicatat secara menyeluruh. Laporan forensik digital yang dihasilkan dapat digunakan oleh pihak terkait untuk melakukan evaluasi keamanan sistem informasi dan sebagai dasar untuk pengambilan keputusan. Selain itu, pembahasan juga menunjukkan bahwa persiapan forensik digital sangat penting dalam efektivitas proses investigasi. Dalam menghadapi kebocoran data, sistem informasi yang menggunakan kebijakan pencatatan log, pengelolaan bukti digital, dan prosedur penanganan insiden cenderung lebih siap. Dengan persiapan forensik yang baik, investigasi dapat dilakukan lebih cepat dan akurat.

Kesimpulan

Hasil penelitian menunjukkan bahwa investigasi forensik digital yang didasarkan pada kerangka kerja NIST dapat memberikan pendekatan yang sistematis dalam menghadapi insiden kebocoran data pada sistem informasi. Dalam mengungkap kronologi serta sumber kebocoran data, tahapan identifikasi, pengumpulan, analisis, dan pelaporan saling berkaitan satu sama lain. Kesiapan forensik digital berperan penting dalam meningkatkan efektivitas dan kecepatan proses investigasi.

Received: November 1, 2025 – Revised: November 12, 2025 - Accepted: Desember 7, 2025 - Published online: January 3, 2026

Saran

Organisasi disarankan untuk meningkatkan kesiapan forensik digital dengan menerapkan pencatatan log yang konsisten, pengelolaan bukti digital yang terorganisir, dan prosedur penanganan insiden yang jelas. Selain itu, peningkatan kompetensi sumber daya manusia harus ditingkatkan dalam bidang keamanan informasi dan forensik digital perlu dilakukan agar proses investigasi kebocoran data dapat berjalan secara efektif dan akurat. Upaya evaluasi dan pembaruan kebijakan keamanan sistem informasi secara berkala sangat penting untuk meminimalkan risiko terjadinya kebocoran data di masa mendatang.

Daftar Pustaka

Whitman, M. E., & Mattord, H. J. (2018). *Principles of information Security* (6th ed.) Cengage Learning. https://www.cengage.com/c/principles-of-information-security-6e-whitman/9781285448367/

Kent, K., & Chevalier, S. (2016). Guide to computer and network data analysis: Applying forensic techniques to incident response (NIST Interagency Report 7676). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.IR.7676

Casey, E. (2011). Digital evidence and computer crime: Forensic science, computers, and the internet (3rd ed.) Academic Press.

Alraddadi, A. S. (2024). Reconstruction investigation model for database management systems. *Journal of Computer Science*, 20 (1), 33-43. https://doi.org/10.3844/jcssp.2024.33.43

Hakim, A. R., Ramli, K., Gunawan, T. S., & Windarta, S. (n.d.). A novel digital forensic framework for data breach investigation. *IEEE Access, 11* null, 42644-42659. https://doi.org/10.1109/ACCESS.2023.3270619

Ivanova, M., & Stefanov, S. (2023). Digital forensics investigation models: Current state and analysis. https://doi.org/10.23919/splitech58164.2023.10193176

Kamble, D. R., & Salunke, M. D. (2024). Designing an automated, privacy preserving, and efficient digital forensic framework. *Journal of autonomous intelligence*null. https://doi.org/10.32629/jai.v7i5.1270

Received: November 1, 2025 – Revised: November 12, 2025 - Accepted: Desember 7, 2025 - Published online: January 3, 2026