Journal of Law, Economics, and Engineering
ISSN XXX XXX
Vol.1, No.1 2025, Hal.22-29
website: https://jolens.org

Forensik Digital dalam Tata Kelola Keamanan Informasi Pendidikan Tinggi Indonesia: Tinjauan Sistematis

Digital Forensics in Information Security Governance in Indonesian Higher Education: A Systematic Review

Rosyid R. Al-Hakim[1,2] ✉, Esa R.C. Putri[3]
1) Program Studi Sistem Informasi, Universitas Harapan Bangsa
2) Program Profesi Insinyur, Universitas Lambung Mangkurat
3) Program Studi Kearsipan, Universitas Terbuka

✉ Corresponding author:
2530811310125@mhs.ulm.ac.id

Abstrak

Era transformasi digital yang cepat telah menjadikan sektor pendidikan tinggi (PT) sebagai sasaran utama kejahatan siber, yang mencakup insiden *data breach* dan kecurangan akademik. Kemampuan untuk melakukan investigasi insiden dan mengumpulkan bukti digital yang sah merupakan kebutuhan manajerial yang vital dalam tata kelola keamanan informasi. Penelitian ini bertujuan menjembatani kesenjangan antara penerapan teknis forensik digital (FD) dan implikasi strategis manajerial, hukum, serta kepatuhan di lingkungan PT Indonesia. Metode yang digunakan adalah Tinjauan Literatur Sistematis (*Systematic Literature Review* atau SLR) berdasarkan kerangka PRISMA untuk menjamin rigor metodologis. Hasilnya menunjukkan bahwa FD berperan penting dalam menjaga integritas akademik, misalnya melalui analisis artefak digital untuk kasus *contract cheating*. Secara hukum, meskipun UU ITE mengakui bukti elektronik, PT menghadapi tantangan dalam standardisasi prosedur FD dan pemeliharaan *Chain of Custody* (CoC) untuk memastikan keabsahan bukti. Kesimpulannya, efektivitas FD di PT menuntut komitmen manajerial strategis dan integrasi *Digital Forensic Readiness* (DFR) ke dalam kebijakan tata kelola untuk memperkuat akuntabilitas publik.

Kata Kunci: *Tata Kelola TI; Kepatuhan Hukum; Digital Forensic Readiness; UU ITE; SLR.*

Abstract

The era of rapid digital transformation has made the higher education (HE) sector a prime target for cybercrime, including data breach incidents and academic fraud. The ability to investigate incidents and collect valid digital evidence is a vital managerial requirement in information security governance. This study aims to bridge the gap between the technical application of digital forensics (FD) and its strategic managerial, legal, and compliance implications in Indonesian HEIs. The method used is a Systematic Literature Review (SLR) based on the PRISMA framework to ensure methodological rigor. The results show that FD plays a crucial role in maintaining academic integrity, for example through the analysis of digital artifacts in contract cheating cases. Legally, although the ITE Law recognizes electronic evidence, HEIs face challenges in standardizing FD procedures and maintaining a Chain of Custody (CoC) to ensure the validity of evidence. In conclusion, the effectiveness of FD in HEIs requires strategic managerial commitment and the integration of Digital Forensic Readiness (DFR) into governance policies to strengthen public accountability.

Keyword: *IT Governance; Legal Compliance; Digital Forensic Readiness; ITE Law; SLR*

Journal of Law, Economics, and Engineering
ISSN XXX XXX
Vol.1, No.1 2025, Hal.22-29
website: https://jolens.org

PENDAHULUAN

Pemanfaatan teknologi informasi (TI) telah menjadi bagian integral dalam operasional institusi Pendidikan Tinggi (PT) di Indonesia, mencakup seluruh proses dari administrasi hingga kegiatan akademik (Wahid, 2004). Namun, akselerasi digitalisasi ini juga meningkatkan kerentanan PT terhadap berbagai ancaman siber yang kompleks. Sektor pendidikan kini diidentifikasi sebagai salah satu sasaran utama kejahatan siber, di mana insiden keamanan siber, mulai dari peretasan hingga pencurian data, terus meningkat (Iman et al., 2020). Menghadapi ancaman ini, kemampuan institusi untuk menanggapi insiden dan mengamankan bukti digital menjadi prioritas manajerial (Johnson et al., 2022; Salfati & Pease, 2022). Forensik Digital (FD) merupakan pondasi penting dalam keamanan siber modern dan instrumen kunci dalam pembuktian hukum (Maesyaroh, 2024; Mawlidya, 2025; Rachmie, 2020; Wu et al., 2020). Urgensi ini terlihat dari inisiatif pemerintah seperti pembentukan *EduCSIRT* oleh Kemendikbudristek, yang menunjukkan perlunya kapabilitas penanganan insiden yang matang di tingkat institusi Pendidikan (Alsisca, 2022; Rogeleonick et al., 2022).

Secara konseptual, FD adalah cabang dari ilmu forensik yang berfokus pada identifikasi, pengumpulan, pemeriksaan, dan analisis bukti digital dari perangkat elektronik (Aji et al., 2017; Raharjo, 2013; SANS Institute, 2025). Tujuan utamanya adalah mengumpulkan bukti yang sah secara hukum (*legally admissible evidence*) untuk digunakan dalam investigasi (Bowen, 2018; Maesyaroh, 2024). Beberapa peneliti telah membandingkan model-model proses forensik inti, mulai dari tiga tahap (akuisisi, analisis, dan pelaporan) hingga model sembilan fase seperti *Abstract Digital Forensic Model* (ADFM) (Du et al., 2017; Sremack, 2007). Model yang terperinci ini menekankan pentingnya prosedur yang ketat, terutama dalam aspek *Chain of Custody* (CoC) atau rantai pengawasan bukti, untuk menjaga integritas data (Rafique & Khan, 2013).

Meskipun fondasi teknis FD sudah mapan, penerapannya di lingkungan non-kriminal seperti PT menimbulkan tantangan unik (Firmansyah, 2025; Johnson et al., 2022; Sudirman et al., 2019). Penelitian sebelumnya menyoroti bahwa FD adalah bidang yang reaktif, dipaksa untuk beradaptasi cepat terhadap perkembangan teknologi dan teknik anti-forensik yang semakin canggih (Sremack, 2007). Di Indonesia, meskipun UU ITE mengakui bukti elektronik, praktik FD masih menghadapi kendala signifikan, termasuk keterbatasan tenaga ahli dan kurangnya standar prosedur baku yang seragam untuk investigasi internal (Gemilang, 2024; Mawlidya, 2025). Isu ini semakin diperparah oleh kebutuhan untuk menyeimbangkan investigasi dengan kepatuhan terhadap Undang-Undang Perlindungan Data Pribadi (UU PDP) (Maesyaroh, 2024).

Kajian sebelumnya seringkali fokus pada aspek teknis FD atau pada aplikasi hukum pidana, sedangkan integrasi FD dalam konteks *e-governance* dan administrasi publik di PT masih kurang dieksplorasi (Firmansyah, 2025). Kajian ini berfokus pada dimensi manajerial dan kebijakan: bagaimana manajemen PT mengintegrasikan proses FD—seperti yang diatur dalam kerangka *Digital Forensic Readiness* (DFR)—ke dalam manajemen risiko institusional, kebijakan kepatuhan, dan tata kelola TI (C. Johnson et al., 2022). Penelitian ini penting karena kegagalan manajemen dalam menyiapkan diri untuk investigasi forensik berimplikasi langsung pada akuntabilitas publik PT dan kemampuan institusi untuk menjaga integritas operasional dan akademik. Oleh karena itu, penelitian ini bertujuan menyintesis literatur untuk menghasilkan implikasi kebijakan strategis bagi tata kelola PT di Indonesia.

METODE

Metode yang digunakan dalam penelitian ini adalah Tinjauan Literatur Sistematis (*Systematic Literature Review* atau SLR) (Maulana et al., 2024; Meliante et al., 2025). SLR adalah cara sistematis untuk mengumpulkan, mengevaluasi secara kritis, mengintegrasikan, dan menyajikan temuan dari berbagai studi penelitian mengenai suatu topik atau pertanyaan (Pati & Lorusso,

Journal of Law, Economics, and Engineering
ISSN XXX XXX
Vol.1, No.1 2025, Hal.22-29
website: https://jolens.org

2018). Metode ini dipilih karena memberikan pemahaman yang lebih luas dan lebih akurat dibandingkan tinjauan literatur tradisional.

Protokol Tinjauan Literatur Sistematis (SLR)

Protokol SLR yang diadopsi mengikuti tiga fase utama: Perencanaan (*Planning*), Pelaksanaan (*Conducting*), dan Pelaporan (*Reporting*). Kerangka kerja *Preferred Reporting Items for Systematic Reviews and Meta-Analysis* (PRISMA) digunakan sebagai panduan untuk menjamin rigor metodologis dan transparansi temuan (Meliante et al., 2025; Pati & Lorusso, 2018):

1. Perencanaan: Fase ini mencakup perumusan tujuan dan identifikasi kebutuhan informasi, seperti yang diwujudkan dalam pertanyaan penelitian pada bagian pendahuluan (Rochmadi et al., 2024).
2. Pelaksanaan: Fase ini meliputi pencarian literatur sesuai protokol, penyaringan awal (*screening*) judul/abstrak, dan seleksi artikel berdasarkan kriteria inklusi/eksklusi (Jennifer & Sophie, 2023).
3. Pelaporan dan Sintesis: Fase akhir melibatkan ekstraksi data, analisis kritis, dan sintesis temuan untuk menghubungkan praktik FD dengan tantangan manajerial dan kebijakan (Aron et al., 2021).

Protokol Pencarian dan Kriteria Seleksi

Pencarian literatur difokuskan pada jurnal dan prosiding internasional bereputasi, termasuk basis data utama seperti *ScienceDirect, Springer, IEEE, ACM*, dan *Google Scholar* yang terindeks. Kata Kunci (*Keywords*) yang digunakan melalui pencarian menggunakan kombinasi istilah Boolean untuk memastikan cakupan komprehensif, meliputi: "*Digital Forensics*"; "*DFIR*"; "*Digital Forensic Readiness*"; "*Higher Education*"; "*University*"; "*E-governance*"; "*Legal*"; "*Compliance*"; dan "*UU ITE*".

Sementara itu dalam kriteria inklusi yakni artikel harus membahas penerapan atau implikasi strategis Forensik Digital (termasuk DFIR atau DFR) dalam konteks manajerial, kebijakan, atau administrasi organisasi, dengan preferensi pada sektor pendidikan tinggi. Publikasi dibatasi pada rentang waktu 5-10 tahun terakhir (2015-2024) untuk menjaga relevansi teknologi dan hukum terkini. Selain itu, kriteria eksklusi yakni artikel yang berfokus murni pada aspek teknis FD tanpa pembahasan manajemen, kebijakan, atau kepatuhan, serta protokol atau errata. Tabel 1 menjelaskan secara ringkas protokol metodologi yang digunakan dalam artikel ini.

Tabel 1. Ringkasan Protokol Metodologi Tinjauan Literatur Sistematis (SLR)

Fase SLR	Aktivitas Kunci	Kriteria Seleksi
Perencanaan	Merumuskan RQ dan Protokol Pencarian	Menjamin transparansi dan metodologi yang kokoh.
Pelaksanaan	Pencarian, Penyaringan Judul/Abstrak, Ekstraksi Data	Fokus pada konteks manajerial/kebijakan Pendidikan Tinggi.
Sintesis	Analisis Kritis dan Integrasi Temuan	Menghubungkan praktik FD dengan tantangan manajerial dan hukum.

HASIL DAN PEMBAHASAN

HASIL

Tinjauan sistematis ini menyintesis kerangka kerja FD dengan tuntutan tata kelola keamanan informasi dan kepatuhan hukum di PT Indonesia. Hasil yang diperoleh diorganisasikan berdasarkan tujuan penelitian dan diperbandingkan dengan literatur terkait.

Journal of Law, Economics, and Engineering
ISSN XXX XXX
Vol.1, No.1 2025, Hal.22-29
website: https://jolens.org

Adaptasi Kerangka Forensik Digital dalam Konteks Manajerial

Forensik Digital adalah proses sistematis yang bertujuan mengumpulkan bukti yang sah secara hukum, dan secara konvensional sering diringkas menjadi tiga tahap: akuisisi bukti, analisis, dan pelaporan (Brunty, 2023; Horsman, 2019; Kumari & Mohapatra, 2016; Ruuhwan et al., 2016). Namun, untuk konteks organisasi yang kompleks seperti PT, model yang lebih rinci diperlukan (Stigall & Choo, 2022). *Abstract Digital Forensic Model* (ADFM) membagi proses menjadi sembilan fase, termasuk Identifikasi, Preservasi, Koleksi, Eksaminasi, Analisis, Rekonstruksi, Dokumentasi, Presentasi, dan Pengembalian Bukti (Du et al., 2017; Rafique & Khan, 2013). Model terperinci ini meningkatkan kemungkinan keberhasilan identifikasi dan pembuktian, yang relevan untuk kasus internal di PT.

Pentingnya aspek manajerial di PT terletak pada transisi dari pendekatan reaktif menjadi proaktif melalui implementasi *Digital Forensic Readiness* (DFR). DFR adalah status kesiapan organisasi, baik secara prosedural, teknis, maupun hukum, untuk segera memulai investigasi forensik ketika insiden terjadi (Firmansyah, 2025). Kesiapan ini diintegrasikan ke dalam proses *Incident Response* (IR) atau DFIR (Salfati & Pease, 2022), yang di pandu oleh kerangka kerja seperti NIST SP 800-86 (Barkem & Sidabutar, 2023). DFR memastikan bahwa pengumpulan data relevan dilakukan secara prosedural sejak dini, yang sangat penting untuk mempertahankan *Chain of Custody* (CoC) atau rantai pengawasan bukti (Wu et al., 2020). Tabel 2 membandingkan model proses forensic digital dan aplikasinya di perguruan tinggi.

Tabel 2. Perbandingan Model Proses Forensik Inti dan Aplikasinya di PT

Fase Forensik	Definisi Inti (4 Fase Tradisional)	Fokus Manajerial di PT
Koleksi (*Collection*)	Akuisisi bukti digital, memastikan data tidak hilang atau rusak.	Pembangunan kebijakan *logging* sistem yang memadai dan audit trail.
Pemeriksaan (*Examination*)	Identifikasi dan ekstraksi data yang relevan.	Memastikan personel memiliki keahlian teknis untuk menggunakan alat forensik log (misalnya, *EventLog Analyzer*).
Analisis (*Analysis*)	Menggunakan data untuk mendukung atau menolak suatu kasus.	Kemampuan analisis untuk membuktikan atau menolak kecurangan akademik atau penyalahgunaan TI internal.
Pelaporan (*Reporting*)	Sintesis temuan menjadi format yang jelas dan mudah dipahami.	Dukungan untuk pengambilan keputusan administrasi (misalnya, sanksi atau pemutusan kerja).

Tantangan Hukum dan Kepatuhan

Penerapan FD dalam tata kelola PT harus beroperasi di bawah kerangka hukum Indonesia (Gemilang, 2024). Undang-Undang No. 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik (UU ITE) secara eksplisit mengakui dokumen dan informasi elektronik sebagai alat bukti hukum yang sah. Pengakuan ini memberikan legitimasi bagi manajemen PT untuk menggunakan temuan FD, baik untuk penegakan disiplin internal maupun untuk kasus yang diteruskan ke proses peradilan pidana. Bukti digital harus memenuhi persyaratan formal dan

Journal of Law, Economics, and Engineering
ISSN XXX XXX
Vol.1, No.1 2025, Hal.22-29
website: https://jolens.org
substantif yang ketat, sejalan dengan prinsip legalitas, untuk menetapkan keabsahannya di pengadilan (Gemilang, 2024).

Meskipun landasan hukumnya kuat, praktik FD di Indonesia menghadapi kendala operasional yang signifikan. Salah satu tantangan terbesar adalah kurangnya regulasi teknis yang terperinci dan standar prosedur baku yang seragam, yang secara langsung memengaruhi penegakan *Chain of Custody* (CoC) (Mawlidya, 2025). CoC adalah dokumentasi penting yang mencatat setiap perpindahan dan penanganan bukti digital untuk memastikan bahwa bukti asli tidak dirusak (*non-repudiation*). Tanpa SOP baku yang ketat, CoC akan rentan terhadap serangan balik hukum, meskipun investigasi dilakukan di tingkat internal PT.

Selain itu, FD harus mematuhi Undang-Undang Perlindungan Data Pribadi (UU PDP) (Maesyaroh, 2024). Investigasi forensik, yang melibatkan analisis mendalam terhadap perangkat atau sistem, secara inheren mengakses data sensitif mahasiswa, dosen, atau staf. Akses dan analisis data harus dilakukan secara proporsional dan didasarkan pada kebijakan yang transparan, untuk meminimalkan risiko hukum dan etika.

PEMBAHASAN

Aplikasi FD dalam Menjaga Integritas Pendidikan Tinggi

FD berperan sebagai alat manajerial yang kuat untuk menegakkan tata kelola yang baik dan melindungi integritas institusi (Wahid, 2004).

1) Penanganan Kecurangan Akademik (Academic Misconduct)

Isu kecurangan akademik kini meluas dari plagiarisme konvensional ke *contract cheating* (memesan pekerjaan pihak ketiga) (C. S. Johnson & Davies, 2020). Meskipun perangkat lunak pencocokan teks standar dapat diakali dengan teknik seperti *patchworking* atau perubahan kata tunggal, FD dapat mengatasinya. Teknik *Computer Forensics* digunakan untuk menganalisis artefak digital tersembunyi, seperti metadata dalam format dokumen (misalnya, OOXML). Analisis artefak ini memberikan indikasi forensik yang kuat bahwa suatu pekerjaan telah disalin atau dikerjakan di luar lingkungan akademik yang seharusnya (C. S. Johnson & Davies, 2020). Dalam kasus *contract cheating* yang terbukti, temuan forensik menjadi bukti kunci dalam sidang disiplin (C. Johnson et al., 2022).

2) Forensik Jaringan dan Penanganan Insiden Siber (DFIR)

Sebagai objek serangan siber, PT harus memiliki kapabilitas *Digital Forensics and Incident Response* (DFIR) yang responsive (Yonavilbia, 2024). FD memungkinkan PT untuk mengidentifikasi akar penyebab insiden dan tidak hanya sekadar memulihkan system (Salfati & Pease, 2022; SANS Institute, 2025). Contohnya, *Network Forensics* menggunakan alat analisis paket seperti Wireshark untuk menangkap dan memeriksa data lalu lintas (Aji et al., 2017). Ini esensial untuk mengidentifikasi anomali, menginvestigasi serangan siber, dan memecahkan masalah jaringan (misalnya, *packet loss* atau *latency* tinggi). Selain itu, penggunaan alat forensik log (seperti *EventLog Analyzer*) membantu mengumpulkan dan menganalisis *log event* sistem, mendeteksi aktivitas mencurigakan yang mengarah pada kebocoran data (Sudirman et al., 2019).

3) Kesenjangan Penelitian dan Rekomendasi

Forensik Digital adalah bidang muda yang terus dipaksa untuk beradaptasi terhadap perkembangan teknologi yang cepat dan canggih (Sremack, 2007). Hal ini menciptakan kesenjangan antara penelitian teoritis dan praktik lapangan, terutama dalam mengadaptasi model forensik yang ketat ke lingkungan administratif non-kriminal seperti PT. Secara operasional, tantangan di Indonesia diperburuk oleh kekurangan tenaga ahli forensik yang mumpuni, serta infrastruktur yang memadai untuk melakukan investigasi komprehensif (Mawlidya, 2025).

Untuk mengatasi kesenjangan ini, manajemen PT harus segera berinvestasi dalam membangun kerangka kerja *Digital Forensic Readiness* (DFR) (Firmansyah, 2025). DFR adalah

Journal of Law, Economics, and Engineering
ISSN XXX XXX
Vol.1, No.1 2025, Hal.22-29
website: https://jolens.org

kunci untuk memastikan bahwa data digital dikumpulkan dan dipertahankan sedemikian rupa sehingga memudahkan proses forensik pasca-insiden (Du et al., 2017). Secara strategis, PT harus mengadopsi kerangka pendidikan keamanan siber seperti NIST *National Initiative for Cybersecurity Education* (NICE), yang menyediakan pelatihan untuk berbagai area spesialisasi. Praktik berbasis simulasi insiden adalah kunci untuk mengembangkan keterampilan praktis tim forensik internal (Salfati & Pease, 2022; SANS Institute, 2025).

Ke depan, integrasi Kecerdasan Buatan (AI) dan *Machine Learning* (ML) dapat mengotomatisasi proses forensik, yang berpotensi meningkatkan kecepatan dan akurasi pengumpulan bukti (Irons & Lallie, 2014; Stigall & Choo, 2022). Manajemen PT perlu merencanakan investasi yang cermat dalam alat-alat forensik berbasis AI, sambil memastikan bahwa aspek legalitas dan metodologi ilmiah forensik tetap terjaga.

SIMPULAN

Forensik Digital telah bertransformasi menjadi komponen wajib dalam tata kelola keamanan informasi dan administrasi publik di Pendidikan Tinggi. Dalam konteks Indonesia, yang menghadapi ancaman siber yang meningkat, kemampuan menerapkan FD secara efektif menentukan akuntabilitas institusi dan integritas akademik. Tinjauan ini menunjukkan bahwa FD adalah instrumen manajerial yang esensial, namun implementasi efektifnya memerlukan komitmen strategis. Untuk mencapai efektivitas, PT harus mengatasi kesenjangan operasional dengan berinvestasi dalam *Digital Forensic Readiness* (DFR). PT juga harus menyusun Standar Operasional Prosedur (SOP) Forensik Internal yang ketat, selaras dengan UU ITE dan UU PDP, untuk memastikan bahwa *Chain of Custody* (CoC) dipertahankan dan bukti sah secara hukum.

Sebagai rekomendasi kebijakan, diusulkan tiga pilar kebijakan FD bagi manajemen PT: Kepatuhan (Penyusunan SOP ketat sesuai UU ITE/PDP), Kesiapan (Implementasi DFR dan investasi infrastruktur), dan Tata Kelola (Pengakuan FD sebagai fungsi strategis audit). Penelitian selanjutnya dapat berfokus pada studi empiris mengenai dampak penerapan kerangka DFR berbasis simulasi NIST NICE di PT Indonesia, serta mengeksplorasi tantangan dan potensi etika forensik dalam menghadapi integrasi AI dan *Machine Learning*.

UCAPAN TERIMA KASIH

Penulis mengucapkan terima kasih pada Dr. Ir. Yuslena Sari, S.Kom., M.Kom., IPM, yang telah memberikan saran masukannya terhadap naskah ini sehingga dapat layak untuk dipublikasikan. Penulis juga berterima kasih pada seluruh Staf Laboratorium Pemrograman Lanjut Universitas Harapan Bangsa yang telah memberikan kelancaran dalam penulisan *review paper* ini.

DAFTAR PUSTAKA

Aji, S., Fadlil, A., & Riadi, I. (2017). Pengembangan Sistem Pengaman Jaringan Komputer Berdasarkan Analisis Forensik Jaringan. *Jurnal Ilmiah Teknik Elektro Komputer Dan Informatika*, *3*(1), 11. https://doi.org/10.26555/JITEKI.V3I1.5665

Alsisca, M. A. (2022). *Konfigurasi dan Analisis Performansi Routing OSPF Pusdatin Kemendikbud dengan Simulator Cisco Packet Tracer*. Politeknik Negeri Jakarta.

Aron, E. F., Diana, N., & Junaidi, J. (2021). Analisis Pengaruh Penyalahgunaan Teknologi Informasi Terhadap Perilaku Academic Fraud Mahasiswa Akuntansi pada Masa Pandemi Covid-19 dengan Motivasi Belajar Sebagai Variabel Intervening (Studi Kasus Terhadap Mahasiswa Program Studi Akuntansi pada Perguruan Tinggi di Kota Malang). *E_Jurnal Ilmiah Riset Akuntansi*, *10*(02).

Journal of Law, Economics, and Engineering
ISSN XXX XXX
Vol.1, No.1 2025, Hal.22-29
website: https://jolens.org
Barkem, W., & Sidabutar, J. (2023). Digital Forensic Analysis of WhatsApp Business Applications on Android-Based Smartphones Using NIST. *MATRIK: Jurnal Manajemen, Teknik Informatika Dan Rekayasa Komputer*, *22*(3), 615–626. https://doi.org/10.30812/matrik.v22i3.3033

Bowen, R. T. (2018). Ethics and the Practice of Forensic Science. In *International Forensic Science & Investigation* (2nd ed.). CRC Press.

Brunty, J. (2023). Validation of forensic tools and methods: A primer for the digital forensics examiner. *WIREs Forensic Science*, *5*(2). https://doi.org/10.1002/WFS2.1474

Du, X., Le-Khac, N. A., & Scanlon, M. (2017). Evaluation of Digital Forensic Process Models with Respect to Digital Forensics as a Service. *European Conference on Information Warfare and Security, ECCWS*, *0*, 573–581.

Firmansyah, R. A. (2025). *Framework Integrasi Digital Forensic Readiness dan Information Security Management System di lingkungan Pemerintahan* [Thesis Universitas Islam Indonesia]. https://dspace.uii.ac.id/handle/123456789/55373

Gemilang, H. F. (2024). Meninjau Ilmu Digital Forensik Terhadap Bukti Elektronik dalam Tindak Pidana Informasi dan Transaksi Elektronik. *Perahu (Penerangan Hukum): Jurnal Ilmu Hukum*, *12*(2). https://doi.org/10.51826/PERAHU.V12I2.984

Horsman, G. (2019). Tool testing and reliability issues in the field of digital forensics. *Digital Investigation*, *28*, 163–175. https://doi.org/10.1016/J.DIIN.2019.01.009

Iman, N., Susanto, A., & Inggi, R. (2020). Analisa Perkembangan Digital Forensik dalam Penyelidikan Cybercrime di Indonesia (Systematic Review). *Jurnal Telekomunikasi Dan Komputer*, *9*(3), 186. https://doi.org/10.22441/INCOMTECH.V9I3.7210

Irons, A., & Lallie, H. S. (2014). Digital Forensics to Intelligent Forensics. *Future Internet*, *6*(3), 584–596. https://doi.org/10.3390/FI6030584

Jennifer, L., & Sophie, D. (2023). How to write a systematic review. *The American Journal of Surgery*, *226*(4), 553–555. https://doi.org/10.1016/J.AMJSURG.2023.05.015

Johnson, C., Davies, R., & Reddy, M. (2022). Using digital forensics in higher education to detect academic misconduct. *International Journal for Educational Integrity*, *18*(1). https://doi.org/10.1007/S40979-022-00104-1

Johnson, C. S., & Davies, R. (2020). Plagiarism from a Digital Forensics Perspective. *Integrity in Education for Future Happiness*, 78–89. https://doi.org/10.11118/978-80-7509-772-9-0078

Kumari, N., & Mohapatra, A. K. (2016). An insight into digital forensics branches and tools. *2016 International Conference on Computational Techniques in Information and Communication Technologies, ICCTICT 2016 - Proceedings*, 243–250. https://doi.org/10.1109/ICCTICT.2016.7514586

Maesyaroh, D. (2024). Peran Digital Forensik Terhadap Pencurian Data Pribadi. *Datin Law Jurnal*, *5*(2), 76–86. https://doi.org/10.36355/dlj.v1i1

Maulana, T. D., Nugroho, A. A. S., Suryaputra, B. A., & Wulansari, A. (2024). Tinjauan Literatur Sistematis: Manajemen Sumber Daya TI di Lingkungan Pendidikan. *JATI (Jurnal Mahasiswa Teknik Informatika)*, *8*(1), 57–62.

Mawlidya, A. (2025). Penerapan Digital Forensik dalam Mengidentifikasi Pelaku Penipuan dan Peran Digital Forensik Sebagai Alat Bukti. *Causa: Jurnal Hukum Dan Kewarganegaraan*, *15*(7), 91–100. https://doi.org/10.6679/TWQYKF83

Meliante, L. A., Coco, G., Rabiolo, A., De Cillà, S., & Manni, G. (2025). Evaluation of AI Tools Versus the PRISMA Method for Literature Search, Data Extraction, and Study Composition in Glaucoma Systematic Reviews: Content Analysis. *JMIR AI*, *4*. https://doi.org/10.2196/68592

Pati, D., & Lorusso, L. N. (2018). How to Write a Systematic Review of the Literature. *HERD*, *11*(1), 15–30. https://doi.org/10.1177/1937586717747384

Journal of Law, Economics, and Engineering
ISSN XXX XXX
Vol.1, No.1 2025, Hal.22-29
website: https://jolens.org
Rachmie, S. (2020). Peranan Ilmu Digital Forensik Terhadap Penyidikan Kasus Peretasan Website. *LITIGASI*, *21*(1), 104–127. https://doi.org/10.23969/LITIGASI.V21I1.2388

Rafique, M., & Khan, M. N. A. (2013). Exploring Static and Live Digital Forensics: Methods, Practices and Tools. *International Journal of Scientific & Engineering Research*, *4*(10), 1048–1056.

Raharjo, B. (2013). Sekilas Mengenai Forensik Digital. *Jurnal Sosioteknologi*, *12*(29), 384–387. https://doi.org/10.5614/SOSTEK.ITBJ.2013.12.29.3

Rochmadi, T., Fadlil, A., & Riadi, I. (2024). Tinjauan Pustaka Sistematis: Tantangan Dan Faktor-Faktor Pengembangan Kesiapan Forensik Digital. *Cyber Security Dan Forensik Digital*, *7*(2), 81–89. https://doi.org/10.14421/csecurity.2024.7.2.4861

Rogeleonick, A., Hartono, S., Pramudita, P., Kusuma, A., Sari, P., Bahari, A., Retnawati, D., Aji, S. P., Fangidae, A. W., Marida, L. A., Sugianto, D., & Hikmat, A. A. (2022). Transformasi Digital Pendidikan. *Jendela Pendidikan Dan Kebudayaan: Media Komunikasi Dan Inspirasi*. https://repositori.kemendikdasmen.go.id/31338/1/MAJALAH_JENDELA_2022_EDISI_63_%28WJ%29_OKE.pdf

Ruuhwan, R., Riadi, I., & Prayudi, Y. (2016). Analisis Kelayakan Integrated Digital Forensics Investigation Framework Untuk Investigasi Smartphone. *Jurnal Buana Informatika*, *7*(4). https://doi.org/10.24002/JBI.V7I4.767

Salfati, E., & Pease, M. (2022). Digital Forensics and Incident Response (DFIR) Framework for Operational Technology (OT). *National Institute of Standards and Technology*. https://doi.org/10.6028/NIST.IR.8428

SANS Institute. (2025). *Digital Forensics and Incident Response Training*. Cybersecurity Focus Area. https://www.sans.org/cybersecurity-focus-areas/digital-forensics-incident-response

Sremack, J. C. (2007). The Gap between Theory and Practice in Digital Forensics. *Annual ADFSL Conference on Digital Forensics, Security and Law*, *2*. https://commons.erau.edu/adfsl/2007/session-8/2

Stigall, M., & Choo, K. K. R. (2022). Digital Forensics Education: Challenges and Future Opportunities. *National Cyber Summit (NCS) Research Track 2021*, *310*, 28–46. https://doi.org/10.1007/978-3-030-84614-5_4

Sudirman, A., Sugiantoro, B., & Prayudi, Y. (2019). Kerangka Kerja Digital Forensic Readiness pada Sebuah Organisasi (Studi Kasus: PT Waditra Reka Cipta Bandung). *Cyber Security Dan Forensik Digital*, *2*(2), 82–88. https://doi.org/10.14421/csecurity.2019.2.2.1641

Wahid, F. (2004). Peluang dan Tantangan Pemanfaatan Teknologi Informasi di Perguruan Tinggi. *Media Informatika*, *2*(1), 11–22. https://journal.uii.ac.id/media-informatika/article/view/2

Wu, T., Breitinger, F., & O'Shaughnessy, S. (2020). Digital forensic tools: Recent advances and enhancing the status quo. *Forensic Science International: Digital Investigation*, *34*, 300999. https://doi.org/10.1016/J.FSIDI.2020.300999

Yonavilbia, E. (2024, July 24). *Sektor Pendidikan Salah Satu Sasaran Utama Kejahatan Siber*. InfoPublik. https://infopublik.id/kategori/nusantara/844721/tim-gabungan-berhasil-temukan-420-rokok-ilegal-di-wedung