

PROBLEMATIKA PEMBUKTIAN ELEKTRONIK DALAM PENYIDIKAN TINDAK PIDANA AKSES TANPA HAK: STUDI EMPIRIS DI KEPOLISIAN DAERAH JAWA TIMUR

Dewinta Maharani

Universitas Pembangunan Nasional “Veteran” Jawa Timur

E-mail: 21071010075@student.upnjatim.ac.id

Eka Nanda Ravizki

Universitas Pembangunan Nasional “Veteran” Jawa Timur

E-mail: eka.nanda.ih@upnjatim.ac.id

Abstract

Unauthorized access to electronic systems presents new challenges for the criminal justice system because its evidentiary process relies heavily on electronic data that are volatile, susceptible to alteration, and require standardized forensic procedures. Although unauthorized access offenses are regulated under the Electronic Information and Transactions Law, and personal data protection has been strengthened through the Personal Data Protection Law, a gap remains between the normative framework, investigative practices, and the standardization of electronic evidence. This study aims to analyze the investigation mechanism for unauthorized access offenses, identify the problems associated with electronic evidence, and examine the integration of their handling within the framework of the Integrated Criminal Justice System (ICJS) at the Cyber Investigation Directorate of the East Java Regional Police. The study employs an empirical legal method using socio-legal, statutory, and case approaches. Primary data were obtained through interviews with investigators from the Cyber Investigation Directorate of the East Java Regional Police, while secondary data were obtained from legislation, case documents, court decisions, books, and scholarly articles. The data were analyzed qualitatively through interpretive analysis and content analysis and validated through triangulation between interview findings and case documents. The findings indicate that the investigation of Case Number 293/Pid.Sus/2023/PN Mjk operationalized the provisions of criminal procedural law, the Electronic Information and Transactions Law, the Personal Data Protection Law, and police investigative procedures. However, the practice of electronic evidence examination continues to face regulatory fragmentation, inconsistent digital forensic procedures, dependence on individual investigator capabilities, technical limitations, and suboptimal inter-agency coordination. These findings demonstrate that the primary problem is not merely the absence of a legal basis, but rather the lack of integration among legal norms, institutional structures, technical standards, and evidentiary practices within a consistent procedural regime. This study contributes to the development of an integrated cyber-investigation model through the harmonization of procedural law, standardization of digital forensic protocols, strengthening of cross-agency coordination, and enhancement of investigator capacity. The study implies the need for integrated technical guidelines on electronic evidence and stronger implementation of the ICJS to ensure the authenticity of evidence, procedural consistency, protection of rights, and legal certainty.

Keywords: *Unauthorized Access; Electronic Evidence; Digital Forensics; Cyber Investigation; Integrated Criminal Justice System.*

Abstrak

Tindak pidana akses tanpa hak terhadap sistem elektronik menghadirkan persoalan baru bagi sistem peradilan pidana karena pembuktiannya sangat bergantung pada data elektronik yang bersifat volatil, mudah berubah, dan memerlukan prosedur forensik yang terstandar. Meskipun tindak pidana akses tanpa hak telah diatur dalam Undang-Undang Informasi dan Transaksi Elektronik serta perlindungan data pribadi telah diperkuat melalui Undang-Undang Perlindungan Data Pribadi, masih terdapat

kesenjangan antara kerangka normatif, praktik penyidikan, dan standardisasi pembuktian elektronik. Penelitian ini bertujuan menganalisis mekanisme penyidikan tindak pidana akses tanpa hak, mengidentifikasi problematika pembuktian elektronik, serta menganalisis keterpaduan penanganannya dalam kerangka Integrated Criminal Justice System (ICJS) pada Direktorat Reserse Siber Kepolisian Daerah Jawa Timur. Penelitian menggunakan metode hukum empiris dengan pendekatan socio-legal, pendekatan perundang-undangan, dan pendekatan kasus. Data primer diperoleh melalui wawancara dengan penyidik Ditres Siber Polda Jawa Timur, sedangkan data sekunder diperoleh dari peraturan perundang-undangan, dokumen perkara, putusan pengadilan, buku, dan artikel ilmiah. Data dianalisis secara kualitatif melalui analisis interpretatif dan content analysis serta divalidasi melalui triangulasi antara hasil wawancara dan dokumen perkara. Hasil penelitian menunjukkan bahwa penyidikan perkara Nomor 293/Pid.Sus/2023/PN Mjk telah mengoperasionalkan ketentuan hukum acara, UU ITE, UU PDP, dan prosedur penyidikan kepolisian, tetapi praktik pembuktian elektronik masih menghadapi fragmentasi regulasi, ketidakseragaman prosedur digital forensik, ketergantungan pada kapasitas individual penyidik, keterbatasan teknis, serta belum optimalnya koordinasi antarlembaga. Temuan tersebut menunjukkan bahwa problem utama bukan semata-mata ketiadaan dasar hukum, melainkan belum terintegrasinya norma, struktur kelembagaan, standar teknis, dan praktik pembuktian dalam satu rezim prosedural yang konsisten. Penelitian ini berkontribusi pada pengembangan model penyidikan siber yang terintegrasi melalui harmonisasi hukum acara, standardisasi digital forensic protocol, penguatan koordinasi lintas lembaga, dan peningkatan kapasitas penyidik. Implikasi penelitian menunjukkan perlunya pedoman teknis terpadu pembuktian elektronik dan penguatan ICJS untuk menjamin autentisitas bukti, konsistensi prosedur, perlindungan hak, dan kepastian hukum.

Kata Kunci: Akses Tanpa Hak; Bukti Elektronik; Digital Forensik; Penyidikan Siber; Integrated Criminal Justice System.

I. PENDAHULUAN

Kejahatan siber telah berkembang menjadi salah satu bentuk kejahatan yang menantang kemampuan sistem peradilan pidana konvensional. Karakteristik kejahatan yang memanfaatkan sistem elektronik menyebabkan proses penyidikan tidak lagi hanya bergantung pada keterangan saksi dan barang bukti fisik, tetapi juga pada informasi elektronik, dokumen elektronik, data log, metadata, alamat Internet Protocol (IP), perangkat digital, serta hasil

pemeriksaan digital forensik.¹ Kondisi tersebut menempatkan pembuktian elektronik sebagai salah satu titik kritis dalam penanganan tindak pidana siber karena bukti digital memiliki karakteristik mudah berubah, mudah dipindahkan, dapat dihapus², dan memerlukan metode khusus untuk menjamin integritas, autentisitas, dan reliabilitasnya³. Perkembangan praktik penyidikan siber juga menunjukkan bahwa proses investigasi tidak hanya merupakan kegiatan teknis untuk memperoleh

¹ Valjarevic, Aleksandar, and Hein S. Venter. "A Comprehensive and Harmonized Digital Forensic Investigation Process Model." *Journal of Forensic Sciences* 60, no. 6 (2015): 1467–1483. DOI: 10.1111/1556-4029.12823.

² Stoykova, Radina, Stig Andersen, Katrin Franke, and Stefan Axelsson. "Reliability Assessment of Digital Forensic Investigations in the Norwegian

Police." *Forensic Science International: Digital Investigation* 40 (2022): 301351. DOI: 10.1016/j.fsidi.2022.301351.

³ Stoykova, Radina, and Katrin Franke. "Reliability Validation Enabling Framework (RVEF) for Digital Forensics in Criminal Investigations." *Forensic Science International: Digital Investigation* 45 (2023): 301554. DOI: 10.1016/j.fsidi.2023.301554.

data dari perangkat digital, tetapi merupakan rangkaian kegiatan yang harus menghubungkan pemeriksaan teknologi dengan kebutuhan pembuktian dalam proses penegakan hukum⁴.

Salah satu bentuk kejahatan siber adalah tindak pidana akses tanpa hak atau *illegal access*, yaitu tindakan mengakses sistem elektronik atau komputer milik pihak lain tanpa hak atau tanpa kewenangan. Dalam praktiknya, akses tanpa hak sering kali tidak berhenti pada tindakan memasuki sistem elektronik, tetapi dapat diikuti dengan pengambilan, pemindahan, pengubahan, atau penggunaan data elektronik. Dengan demikian, proses penyidikan tidak hanya dituntut membuktikan adanya akses tanpa hak, tetapi juga harus mampu menunjukkan hubungan antara aktivitas digital, perangkat atau akun yang digunakan, data yang diperoleh, serta pelaku yang bertanggung jawab. Karakteristik tersebut menjadikan penyidikan kejahatan siber membutuhkan keterpaduan antara kemampuan investigatif, pemeriksaan teknologi, dan pengelolaan bukti digital agar hubungan antara artefak digital dan peristiwa pidana dapat dibangun secara dapat dipertanggungjawabkan⁵.

Persoalan utama penelitian ini terletak pada adanya kesenjangan antara pengaturan normatif dan praktik pembuktian elektronik. Pada saat perkara Nomor 293/Pid.Sus/2023/PN Mjk diproses, hukum acara pidana Indonesia

masih menggunakan Undang-Undang Nomor 8 Tahun 1981 tentang Kitab Undang-Undang Hukum Acara Pidana (KUHP), sedangkan pengakuan terhadap informasi dan dokumen elektronik sebagai alat bukti terutama bersumber dari Undang-Undang Informasi dan Transaksi Elektronik. Kerangka tersebut kemudian berinteraksi dengan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi serta peraturan kepolisian mengenai penyidikan. Konsekuensinya, penyidik harus mengoperasionalkan beberapa instrumen hukum sekaligus dalam menangani bukti elektronik. Kondisi demikian menunjukkan bahwa persoalan pembuktian elektronik tidak semata-mata berkaitan dengan ada atau tidaknya dasar hukum, tetapi juga dengan bagaimana berbagai norma tersebut diterjemahkan ke dalam prosedur investigasi yang konsisten.

Persoalan tersebut menunjukkan karakter yang dapat disebut sebagai *fragmented cyber procedural regime*, yaitu kondisi ketika norma mengenai penyidikan, bukti elektronik, perlindungan data, dan prosedur digital forensik tersebar dalam berbagai instrumen hukum dan belum sepenuhnya membentuk satu standar prosedural yang terpadu. Literatur mengenai digital evidence menunjukkan bahwa persoalan pembuktian elektronik bukan hanya

⁴ Karie, N. M., H. S. Venter, and J. H. P. Eloff. "The Stages of Cybercrime Investigations: Bridging the Gap between Technology Examination and Law Enforcement Investigation." *Computer Law & Security Review* 27, no. 1 (2011): 61–67. DOI: 10.1016/j.clsr.2010.11.001.

⁵ Yar, Majid, and Kevin F. Steinmetz. "The Contemporary Cybercrime Ecosystem: A Multi-Disciplinary Overview of the State of Affairs and Developments." *Computer Law & Security Review* 34, no. 6 (2018): 1180–1196. DOI: 10.1016/j.clsr.2018.08.005.

menyangkut pengakuan normatif terhadap bukti digital, tetapi juga autentikasi, integritas, reliabilitas, dokumentasi proses pemeriksaan, serta standardisasi metode forensik⁶. Dengan demikian, keberadaan aturan yang mengakui bukti elektronik belum secara otomatis menjamin bahwa seluruh tahapan pengumpulan, preservasi, pemeriksaan, analisis, dan penyajian bukti dilakukan melalui prosedur yang seragam.

Persoalan standardisasi tersebut juga ditemukan dalam praktik digital forensik. Casey (2020) menekankan pentingnya standardisasi dalam pembentukan dan penyampaian pendapat evaluatif terhadap bukti digital karena bukti elektronik dapat mengalami salah tafsir apabila proses evaluasinya tidak didukung metode yang sistematis. Stoykova et al. (2022) dalam penelitian terhadap praktik digital forensik kepolisian di Norwegia menunjukkan bahwa dokumentasi yang tidak memadai dapat menyulitkan penelusuran tindakan forensik yang dilakukan terhadap suatu barang bukti serta hubungan antara bukti digital dan sumbernya. Sementara itu, Stoykova and Franke (2023) mengembangkan *Reliability Validation Enabling Framework* yang menempatkan validasi teknologi, metode, dan penerapan sebagai bagian penting dalam menjamin reliabilitas digital forensic investigation. Temuan-temuan tersebut memperlihatkan bahwa standardisasi digital forensik merupakan

persoalan yang berkaitan langsung dengan kualitas dan dapat dipertanggungjawabkannya bukti elektronik dalam proses peradilan⁷.

Dalam konteks Indonesia, perkembangan tersebut menjadi semakin penting karena sejak 2 Januari 2026 telah berlaku Undang-Undang Nomor 20 Tahun 2025 tentang Kitab Undang-Undang Hukum Acara Pidana yang mencabut Undang-Undang Nomor 8 Tahun 1981. Undang-Undang Nomor 20 Tahun 2025 merupakan pembaruan hukum acara pidana yang antara lain memperkuat kewenangan penyidik dan penuntut umum serta koordinasi antara keduanya. Perkembangan ini penting bagi penelitian karena memperlihatkan adanya perubahan paradigma hukum acara pidana Indonesia dalam merespons perkembangan teknologi informasi. Dengan demikian, penelitian terhadap perkara tahun 2023 tetap harus menggunakan kerangka hukum yang berlaku pada saat perkara diproses, sedangkan KUHAP 2025 dapat digunakan untuk membaca arah perkembangan hukum acara pidana dan kebutuhan standardisasi pembuktian elektronik pada masa sekarang.

Secara teknis, *digital evidence* memerlukan proses yang terstruktur sejak identifikasi, akuisisi, pemeriksaan, analisis, dokumentasi, sampai penyajian hasil. Valjarevic and Venter menunjukkan pentingnya model investigasi digital forensik yang komprehensif

⁶ Casey, Eoghan. "Standardization of Forming and Expressing Preliminary Evaluative Opinions on Digital Evidence." *Forensic Science International: Digital Investigation* 32 (2020): 200888. DOI: 10.1016/j.fsidi.2019.200888.

⁷ Stoykova, Radina, and Katrin Franke. "Reliability Validation Enabling Framework (RVEF) for Digital Forensics in Criminal Investigations." *Forensic Science International: Digital Investigation* 45 (2023): 301554. DOI: 10.1016/j.fsidi.2023.301554

dan terharmonisasi untuk memastikan bahwa tahapan pemeriksaan bukti digital dapat dilakukan secara sistematis⁸. Horsman juga menekankan kebutuhan standardisasi prosedur pemeriksaan digital forensik, terutama pada tahap pengumpulan, penanganan, akuisisi, analisis, interpretasi, serta pelaporan dan penyajian bukti⁹. Sementara itu, Tully et al. (2020) menunjukkan bahwa penerapan standar kualitas dan validasi merupakan aspek penting dalam meningkatkan reliabilitas proses digital forensik dalam sistem peradilan pidana. Dengan demikian, kualitas penyidikan siber harus dipahami sebagai persoalan hukum sekaligus persoalan prosedural dan teknis.¹⁰

Dalam perkara Nomor 293/Pid.Sus/2023/PN Mjk, terdakwa Ahmad Saleh didakwa berkaitan dengan penggunaan modus *phishing* terhadap warga negara Jepang. Perkara tersebut relevan untuk dikaji karena proses penyidikannya melibatkan penggunaan bukti elektronik dan pemeriksaan digital yang kemudian dinilai dalam proses persidangan. Perkara ini memberikan ruang untuk melihat bagaimana ketentuan normatif diterjemahkan menjadi praktik penyidikan, khususnya dalam pengumpulan, pengamanan, pemeriksaan, dan penyajian bukti elektronik. Dengan demikian, perkara tersebut tidak hanya relevan sebagai studi mengenai tindak pidana akses tanpa hak,

tetapi juga sebagai kasus untuk menganalisis hubungan antara norma hukum acara dan praktik pengelolaan bukti digital.

Pemilihan Direktorat Reserse Siber Kepolisian Daerah Jawa Timur sebagai lokasi penelitian didasarkan pada keterlibatan institusi tersebut dalam penyidikan perkara Nomor 293/Pid.Sus/2023/PN Mjk. Berdasarkan naskah perkara dan data penelitian, penyidikan dilakukan oleh Subdirektorat V Siber Ditreskrimsus Polda Jawa Timur yang kemudian sejak Desember 2024 berkembang menjadi Direktorat Reserse Siber Polda Jawa Timur. Oleh karena itu, Polda Jawa Timur tidak ditempatkan sebagai representasi statistik seluruh penyidikan siber di Indonesia, tetapi sebagai studi kasus institusional yang memungkinkan penelitian mengidentifikasi hubungan antara norma hukum, praktik penyidikan, digital forensik, dan koordinasi antarlembaga.

Penelitian terdahulu mengenai tindak pidana akses tanpa hak di Indonesia masih relatif terbatas dan sebagian besar menitikberatkan pada efektivitas penyidikan atau konstruksi pertanggungjawaban pidana. Ismail, Thalib, and Arief (2024), misalnya, mengkaji efektivitas penyidikan tindak pidana *illegal access* pada tingkat Kepolisian Resor

⁸ Valjarevic and Venter, 2015, *Op cit*

⁹ Horsman, Graeme. "Standardizing Digital Forensic Examination Procedures: A Look at Windows 10 in Cases Involving Images Depicting Child Sexual Abuse." *WIREs Forensic Science* 3, no. 6 (2021): e1417. DOI: 10.1002/wfs2.1417.

¹⁰ Tully, Gillian, Neil Cohen, David Compton, Gareth Davies, Roy Isbell, and Tim Watson. "Quality Standards for Digital Forensics: Learning from Experience in England & Wales." *Forensic Science International: Digital Investigation* 32 (2020): 200905. DOI: 10.1016/j.fsidi.2020.200905

Soppeng¹¹. Penelitian tersebut memberikan dasar penting mengenai praktik penyidikan tindak pidana akses tanpa hak, tetapi belum secara mendalam mengkaji hubungan antara fragmentasi hukum acara, pembuktian elektronik, digital forensik, dan keterpaduan *Integrated Criminal Justice System* (ICJS). Sementara itu, penelitian mengenai digital evidence secara internasional lebih banyak membahas reliabilitas, standardisasi, dan validasi pemeriksaan bukti digital. Dengan demikian, terdapat *research gap* pada level integrasi antara aspek normatif, teknis, dan kelembagaan dalam penyidikan tindak pidana akses tanpa hak di Indonesia.

Penelitian ini menggunakan pendekatan *Integrated Criminal Justice System* (ICJS) dan teori sistem hukum Lawrence M. Friedman. ICJS digunakan untuk menganalisis keterhubungan penyidik, penuntut umum, pengadilan, serta lembaga pendukung dalam proses penyidikan dan pembuktian. Sementara itu, teori Friedman digunakan untuk menganalisis tiga dimensi yang mempengaruhi efektivitas penegakan hukum, yaitu substansi hukum, struktur hukum, dan budaya hukum¹². Dengan kerangka tersebut, fragmentasi pembuktian elektronik tidak hanya dipahami sebagai kekurangan norma, tetapi sebagai persoalan yang melibatkan struktur kelembagaan, kapasitas sumber daya manusia,

prosedur teknis, koordinasi, serta literasi hukum dan digital.

Dalam perspektif ICJS, efektivitas penyidikan tidak berhenti pada kemampuan kepolisian memperoleh bukti elektronik, tetapi juga bergantung pada kemampuan sistem peradilan pidana untuk mempertahankan kesinambungan pengelolaan dan penilaian bukti dari tahap penyidikan sampai persidangan. Literatur mengenai investigasi siber menunjukkan bahwa perkembangan teknologi telah menciptakan kebutuhan untuk menjembatani pemeriksaan teknis terhadap perangkat digital dengan kebutuhan investigasi dan pembuktian dalam proses hukum¹³. Oleh karena itu, koordinasi antara penyidik, penuntut umum, pengadilan, dan lembaga pendukung menjadi penting untuk memastikan bahwa bukti elektronik yang diperoleh secara teknis dapat dipertanggungjawabkan secara hukum.

Berdasarkan uraian tersebut, *problem statement* penelitian ini adalah bahwa meskipun tindak pidana akses tanpa hak telah memperoleh dasar hukum dalam regulasi teknologi informasi dan hukum pidana, mekanisme penyidikannya masih menghadapi persoalan pada pembuktian elektronik, standardisasi digital forensik, koordinasi antarlembaga, dan konsistensi prosedural. Persoalan tersebut berpotensi menjadikan proses penyidikan bersifat *person-dependent*, yaitu sangat bergantung pada

¹¹ Ismail, Muh. Akbar, H. Thalib, and A. Arief. "Efektivitas Penyidikan terhadap Pelaku Tindak Pidana Illegal Access di Kepolisian Resor Soppeng." *Journal of Lex Philosophy* 5, no. 1 (2024): 143–159.

¹² Friedman, Lawrence M. *The Legal System: A Social Science Perspective*. New York: Russell Sage Foundation, 1975.

¹³ Karie, Venter, and Eloff 2019, *Op cit*

kemampuan dan pengalaman individual penyidik atau unit forensik. Dalam konteks ini, persoalan utama bukan semata-mata kekurangan norma, melainkan belum sepenuhnya terintegrasinya substansi hukum, struktur kelembagaan, kapasitas teknis, dan budaya hukum ke dalam satu mekanisme penyidikan siber yang konsisten.

Penelitian ini bertujuan menganalisis: pertama, mekanisme penyidikan tindak pidana akses tanpa hak pada Direktorat Reserse Siber Polda Jawa Timur; kedua, problematika pembuktian elektronik dan digital forensik dalam perkara Nomor 293/Pid.Sus/2023/PN Mjk; dan ketiga, keterpaduan penyidikan dalam kerangka ICJS. Penelitian ini berkontribusi pada pengembangan model penyidikan siber yang terintegrasi melalui harmonisasi hukum acara dan *digital evidence*, standarisasi prosedur digital forensik, serta penguatan koordinasi antarlembaga dalam kerangka ICJS. Dengan demikian, penelitian ini tidak hanya mempersoalkan kecukupan dasar hukum tindak pidana akses tanpa hak, tetapi juga menawarkan kerangka analitis untuk memahami bagaimana norma, struktur, dan praktik pembuktian elektronik dapat diintegrasikan dalam sistem peradilan pidana yang mampu merespons karakteristik kejahatan siber.

II. METODE PENELITIAN

Penelitian ini merupakan penelitian hukum empiris dengan pendekatan *socio-legal* yang memadukan analisis normatif terhadap peraturan perundang-undangan dengan

penelitian lapangan untuk mengkaji implementasi mekanisme penyidikan tindak pidana akses tanpa hak. Pendekatan ini digunakan karena persoalan pembuktian elektronik tidak dapat dianalisis hanya dari keberadaan norma hukum, tetapi juga harus dilihat dari bagaimana norma tersebut diterapkan oleh penyidik dalam praktik.

Penelitian dilaksanakan pada Direktorat Reserse Siber Kepolisian Daerah Jawa Timur dengan fokus pada penanganan perkara Nomor 293/Pid.Sus/2023/PN Mjk. Pemilihan lokasi dilakukan secara purposive karena institusi tersebut merupakan unit kepolisian yang menangani proses penyidikan perkara yang menjadi objek penelitian. Perkara tersebut digunakan sebagai studi kasus untuk menganalisis hubungan antara hukum acara pidana, UU ITE, UU PDP, digital forensik, dan koordinasi dalam sistem peradilan pidana.

Subjek penelitian adalah aparat penegak hukum yang terlibat dalam proses penyidikan tindak pidana siber, dengan informan utama Rafi Septia Budianto Pansariadi, S.H., selaku penyidik pada Bagian Pembinaan Operasional Direktorat Reserse Siber Kepolisian Daerah Jawa Timur. Data empiris dari wawancara digunakan untuk memperoleh informasi mengenai praktik penyidikan, kendala teknis, pengelolaan bukti elektronik, koordinasi kelembagaan, dan strategi penyidik dalam menangani tindak pidana akses tanpa hak.

Data penelitian terdiri atas data primer dan data sekunder. Data primer diperoleh melalui wawancara dengan penyidik dan

informasi empiris mengenai praktik penanganan perkara. Data sekunder diperoleh melalui studi dokumen terhadap berkas perkara Nomor 293/Pid.Sus/2023/PN Mjk, putusan pengadilan, peraturan perundang-undangan, buku, serta artikel jurnal nasional dan internasional yang relevan dengan cybercrime, electronic evidence, digital forensics, dan criminal justice system.

Bahan hukum primer meliputi Undang-Undang Nomor 8 Tahun 1981 tentang Hukum Acara Pidana sebagai hukum acara yang berlaku pada saat perkara tahun 2023 diproses, Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik beserta perubahannya, Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, serta Peraturan Kepolisian Negara Republik Indonesia Nomor 6 Tahun 2019 tentang Penyidikan Tindak Pidana. Untuk memperkuat relevansi penelitian terhadap perkembangan hukum saat ini, penelitian juga memperhatikan Undang-Undang Nomor 20 Tahun 2025 tentang Kitab Undang-Undang Hukum Acara Pidana yang mulai berlaku pada 2 Januari 2026. Dengan demikian, penelitian membedakan hukum yang berlaku pada saat perkara ditangani dengan rezim hukum acara pidana yang berlaku pada saat artikel ini disusun.

Pengumpulan data dilakukan melalui tiga teknik, yaitu studi kepustakaan, studi dokumen, dan wawancara. Studi kepustakaan digunakan untuk memperoleh kerangka konseptual mengenai cybercrime, electronic

evidence, digital forensics, ICJS, dan sistem hukum. Studi dokumen digunakan untuk mengidentifikasi mekanisme penyidikan serta kedudukan bukti elektronik dalam perkara yang diteliti. Wawancara digunakan untuk memperoleh informasi mengenai praktik dan hambatan empiris yang tidak dapat diperoleh hanya melalui dokumen hukum.

Data dianalisis secara kualitatif menggunakan metode interpretatif dan *content analysis*. Tahap analisis dilakukan dengan mengidentifikasi data berdasarkan lima tema utama: (1) substansi hukum dan fragmentasi regulasi; (2) mekanisme dan standardisasi pembuktian elektronik; (3) struktur kelembagaan dan kapasitas sumber daya manusia; (4) koordinasi antarlembaga dalam kerangka ICJS; dan (5) budaya hukum serta literasi digital. Setiap temuan empiris kemudian dibandingkan dengan ketentuan hukum dan konsep yang relevan untuk menemukan kesenjangan antara *law in the books* dan *law in action*.

Kerangka analisis ICJS digunakan untuk mengoperasionalkan hubungan antara penyidik, penuntut umum, pengadilan, serta lembaga pendukung seperti Badan Siber dan Sandi Negara dan kementerian/lembaga yang memiliki kewenangan atas data atau infrastruktur elektronik. Analisis tidak dimaksudkan untuk mengasumsikan adanya koordinasi formal tertentu apabila tidak didukung oleh data, tetapi untuk mengidentifikasi titik koordinasi, hambatan sinkronisasi, dan kebutuhan integrasi

prosedural berdasarkan data empiris yang tersedia.

Validitas data dilakukan melalui triangulasi sumber, terutama dengan membandingkan informasi hasil wawancara dengan isi dokumen perkara, putusan pengadilan, dan ketentuan peraturan perundang-undangan. Triangulasi digunakan untuk mengurangi ketergantungan pada satu sumber informasi dan memastikan bahwa kesimpulan penelitian tidak hanya didasarkan pada persepsi informan.

III. HASIL PENELITIAN DAN PEMBAHASAN

3.1 Mekanisme Penyidikan Tindak Pidana Akses Tanpa Hak

Tindak pidana akses tanpa hak pada dasarnya tetap tunduk pada ketentuan hukum acara pidana umum, sedangkan karakteristik khusus tindak pidana yang dilakukan melalui sistem elektronik memerlukan penerapan ketentuan khusus dalam Undang-Undang Informasi dan Transaksi Elektronik (UU ITE), Undang-Undang Perlindungan Data Pribadi (UU PDP), serta ketentuan teknis penyidikan kepolisian¹⁴. Dalam perspektif *Integrated Criminal Justice System* (ICJS), penyidikan tidak dapat dipandang sebagai proses yang berdiri sendiri, melainkan merupakan bagian

dari rangkaian proses peradilan pidana yang harus memiliki kesinambungan dengan tahap penuntutan dan pemeriksaan di pengadilan¹⁵.

Dalam perkara Nomor 293/Pid.Sus/2023/PN Mjk, mekanisme penyidikan dilakukan oleh Subdirektorat V Siber Ditreskrimsus Polda Jawa Timur. Berdasarkan data penelitian, perkara tersebut berkaitan dengan modus *phishing* yang melibatkan penggunaan sarana elektronik dan data digital. Proses penyidikan tidak hanya diarahkan untuk mengidentifikasi perbuatan akses tanpa hak, tetapi juga untuk memperoleh dan menghubungkan bukti elektronik dengan aktivitas pelaku¹⁶. Dengan demikian, karakter penyidikan dalam perkara ini berbeda dari penyidikan tindak pidana konvensional karena objek pemeriksaan tidak hanya berupa benda fisik, tetapi juga perangkat, akun, data, komunikasi elektronik, dan jejak digital.¹⁷

Secara prosedural, tahapan penyidikan tetap mencakup penerbitan surat perintah penyidikan, pemanggilan dan pemeriksaan pihak terkait, penggeledahan, penyitaan, pemeriksaan barang bukti, serta penetapan dan pengujian alat bukti. Namun, ketika objek yang diperiksa berupa perangkat elektronik, tahapan tersebut memerlukan penyesuaian teknis. Perangkat elektronik tidak cukup diperlakukan sebagai barang bukti fisik,

¹⁴ Hamzah, Andi. *Cyber Crime: Kejahatan Masa Depan*. Jakarta: Sinar Grafika, 2015

¹⁵ Flora, Henny Saida, et al. *Hukum Pidana di Era Digital*. Batam: Rey Media Grafika, 2024

¹⁶ Ismail, Muh. Akbar, H. Thalib, and A. Arief. "Efektivitas Penyidikan terhadap Pelaku Tindak Pidana

Illegal Access di Kepolisian Resor Soppeng." *Journal of Lex Philosophy* 5, no. 1 (2024): 143–159

¹⁷ Sitanggang, A. S., F. Darmawan, and D. Saputra. "Hukum Siber dan Penegakan Hukum di Indonesia: Tantangan dan Solusi Memerangi Kejahatan Siber." *Jurnal Pendidikan dan Teknologi Indonesia* 4, no. 3 (2024): 79–83

karena nilai pembuktiannya justru berada pada data yang tersimpan, diproses, atau dapat dipulihkan dari perangkat tersebut. Literatur mengenai akuisisi dan penyajian *digital evidence* di Indonesia menunjukkan bahwa karakteristik bukti digital memerlukan metode perolehan dan penyajian yang berbeda dari bukti konvensional¹⁸.

Dalam praktik penyidikan, proses tersebut melibatkan *digital tracing*, pengamanan perangkat, akuisisi data, pemeriksaan digital forensik, serta dokumentasi terhadap proses pengelolaan barang bukti¹⁹. Tahapan ini penting karena perubahan terhadap data asli dapat mempengaruhi kemampuan penyidik untuk menunjukkan bahwa data yang diajukan merupakan data yang berasal dari perangkat atau sistem yang diperiksa²⁰. Oleh karena itu, prinsip *chain of custody*, dokumentasi tindakan pemeriksaan, dan penggunaan metode forensik yang dapat dipertanggungjawabkan menjadi bagian penting dari proses pembuktian.

Temuan penelitian menunjukkan bahwa mekanisme penyidikan di Polda Jawa Timur pada dasarnya telah mampu mengoperasionalkan ketentuan hukum acara, UU ITE, UU PDP, dan prosedur penyidikan kepolisian. Akan tetapi, mekanisme tersebut

belum sepenuhnya didukung oleh satu pedoman teknis terpadu mengenai pengelolaan bukti elektronik. Dengan kata lain, persoalan yang ditemukan bukan ketiadaan mekanisme penyidikan, melainkan adanya jarak antara mekanisme hukum formal dan kebutuhan teknis pemeriksaan bukti digital.

Temuan tersebut sejalan dengan penelitian Stoykova yang menunjukkan bahwa penggunaan teknologi dalam penyidikan pidana dapat menimbulkan persoalan reliabilitas dan fairness apabila prosedur teknologi yang digunakan tidak disertai standar validasi yang memadai²¹. Dengan demikian, mekanisme penyidikan tindak pidana akses tanpa hak perlu dipahami sebagai suatu proses yang berada pada persimpangan antara hukum acara pidana, teknologi informasi, dan ilmu forensik.

3.2 Fragmentasi Regulasi: Antara KUHAP, UU ITE, UU PDP, dan Digital Forensik

Temuan penelitian menunjukkan adanya fragmentasi pengaturan dalam penyidikan tindak pidana akses tanpa hak. Dalam praktik, penyidik harus menggabungkan beberapa sumber hukum, yaitu KUHAP sebagai hukum acara pidana umum, UU ITE sebagai dasar

¹⁸ Santosa, Dewa Gede Giri, and Karell Mawla Ibnu Kamali. "Acquisition and Presentation of Digital Evidence in Criminal Trial in Indonesia." *Jurnal Hukum dan Peradilan* 11, no. 2 (2022): 195–218. DOI: 10.25216/jhp.11.2.2022.195-218

¹⁹ Karie, N. M., H. S. Venter, and J. H. P. Eloff. "The Stages of Cybercrime Investigations: Bridging the Gap between Technology Examination and Law Enforcement Investigation." *Computer Law & Security*

Review 27, no. 1 (2011): 61–67. DOI: 10.1016/j.clsr.2010.11.001

²⁰ Casey, Eoghan. *Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet*. 3rd ed. London: Academic Press, 2011

²¹ Stoykova, Radina. "Digital Evidence: Unaddressed Threats to Fairness and the Presumption of Innocence." *Computer Law & Security Review* 42 (2021): 105575. DOI: 10.1016/j.clsr.2021.105575

pengaturan tindak pidana yang berkaitan dengan sistem elektronik²², UU PDP sebagai instrumen perlindungan data pribadi, serta peraturan kepolisian sebagai pedoman penyidikan²³.

Fragmentasi tersebut tidak berarti bahwa masing-masing peraturan tidak memiliki fungsi. Persoalannya terletak pada belum sepenuhnya tersedianya hubungan prosedural yang terpadu antara ketentuan mengenai penyidikan, penyitaan perangkat elektronik, pemeriksaan digital, perlindungan data pribadi, dan penyajian bukti elektronik di pengadilan. Dalam konteks penyidikan siber, penyidik harus menentukan bagaimana norma-norma tersebut diterapkan secara bersamaan tanpa mengurangi nilai pembuktian maupun hak-hak pihak yang diperiksa²⁴.

Persoalan ini menjadi semakin kompleks karena bukti elektronik tidak hanya mempunyai dimensi pembuktian, tetapi juga dimensi privasi dan perlindungan data. Dalam proses penyitaan perangkat elektronik, satu perangkat dapat memuat data yang berkaitan dengan tindak pidana sekaligus data pribadi pihak lain yang tidak memiliki hubungan dengan perkara. Oleh sebab itu, pengumpulan dan pemeriksaan data harus dilakukan secara

proporsional dan tetap memperhatikan perlindungan data pribadi.

Literatur Indonesia mengenai akuisisi dan penyajian bukti digital juga menunjukkan bahwa sebelum pembaruan hukum acara pidana, terdapat ketegangan antara sistem alat bukti dalam KUHAP dan pengaturan bukti elektronik dalam UU ITE. Persoalan tersebut menunjukkan bahwa pengakuan normatif terhadap bukti elektronik belum secara otomatis menghasilkan standar prosedural yang seragam²⁵.

Dalam perkembangan hukum terbaru, sejak 2 Januari 2026 berlaku Undang-Undang Nomor 20 Tahun 2025 tentang Kitab Undang-Undang Hukum Acara Pidana yang menggantikan Undang-Undang Nomor 8 Tahun 1981. Perubahan tersebut penting karena hukum acara pidana Indonesia kini memberikan pengaturan yang lebih eksplisit terhadap bukti elektronik²⁶. Namun, dalam penelitian ini, perubahan tersebut tidak digunakan untuk menilai keabsahan proses penyidikan perkara tahun 2023 secara retroaktif. Perkara Nomor 293/Pid.Sus/2023/PN Mjk tetap dianalisis berdasarkan hukum yang berlaku ketika proses penyidikan dan pemeriksaan perkara berlangsung.

²² Pribadi, Insan. "Legalitas Alat Bukti Elektronik dalam Sistem Peradilan Pidana." *Lex Renaissance* 3, no. 1 (2019). DOI: 10.20885/JLR.vol3.iss1.art4

²³ July, Wiarti. "Legality of Electronic Evidence in Cyber Crime Cases." *Ahmad Dahlan Indonesian Law Journal* 1, no. 2 (2023): 11–19. DOI: 10.12928/adil.v1i1.572

²⁴ Sitanggang, A. S., F. Darmawan, and D. Saputra, 2024. *Op cit*

²⁵ Santosa and Kamali, 2022. *Op cit*

²⁶ De Hert, Paul, Cihan Parlan, and Juraj Sajfert. "The Cybercrime Convention Committee's 2017 Guidance Note on Production Orders: Unilateralist Transborder Access to Electronic Evidence Promoted via Soft Law." *Computer Law & Security Review* 34, no. 2 (2018): 327–336. DOI: 10.1016/j.clsr.2018.01.003

Perkembangan tersebut justru memberikan implikasi penting bagi penelitian. Penguatan pengakuan normatif terhadap bukti elektronik perlu diikuti oleh standarisasi mengenai bagaimana bukti tersebut diperoleh, diamankan, diperiksa, diverifikasi, dan dipresentasikan. Penelitian terbaru mengenai kerangka bukti elektronik Indonesia juga menunjukkan bahwa persoalan utama tidak hanya terletak pada pengakuan terhadap bukti digital, tetapi pada koherensi arsitektur hukum, standarisasi, dan penerapannya dalam proses peradilan.

Dengan demikian, fragmentasi yang ditemukan dalam penelitian ini lebih tepat dipahami sebagai *fragmented cyber procedural regime*. Istilah tersebut menggambarkan keadaan ketika substansi hukum telah berkembang melalui berbagai regulasi, tetapi integrasi prosedur teknis dan kelembagaan belum sepenuhnya terbentuk. Persoalan tersebut berpotensi menyebabkan prosedur pengelolaan bukti elektronik berbeda berdasarkan karakteristik perkara, kemampuan unit penyidik, dan kapasitas personel yang menangani pemeriksaan digital.

3.3 Pembuktian Elektronik dan Kebutuhan Standarisasi Digital Forensik

Bukti elektronik memiliki karakteristik berbeda dengan alat bukti konvensional. Data digital dapat disalin, dipindahkan, diubah, dihapus, atau mengalami perubahan akibat proses teknis yang terjadi secara otomatis pada perangkat atau sistem²⁷. Oleh karena itu, pembuktian elektronik tidak cukup hanya menunjukkan keberadaan suatu data, tetapi juga harus mampu menjelaskan sumber data, proses perolehannya, integritasnya, metode pemeriksaannya, dan hubungan data tersebut dengan peristiwa pidana²⁸.

Dalam perkara Nomor 293/Pid.Sus/2023/PN Mjk, penggunaan bukti elektronik menjadi bagian penting dalam proses pembuktian. Berdasarkan dokumen perkara yang ditelaah, alat bukti elektronik yang diajukan dalam proses persidangan dinilai oleh majelis hakim dan memiliki relevansi terhadap pembuktian tindak pidana. Hal ini menunjukkan bahwa secara praktis bukti elektronik telah menjadi bagian penting dalam proses pembuktian perkara pidana.

Namun, penerimaan bukti elektronik pada tingkat persidangan tidak menghilangkan kebutuhan terhadap standarisasi proses memperoleh dan memeriksa bukti tersebut. Sebaliknya, semakin penting posisi bukti elektronik, semakin tinggi pula kebutuhan terhadap prosedur yang mampu memastikan autentisitas dan integritasnya²⁹.

²⁷ Casey, 2011, *Op cit*

²⁸ Pribadi, Insan. "Legalitas Alat Bukti Elektronik dalam Sistem Peradilan Pidana." *Lex Renaissance* 3, no. 1 (2019). DOI: 10.20885/JLR.vol3.iss1.art4.

²⁹ Hardianto, Aris, Barda Nawawi Arief, and Joko Setiyono. "The Significance of Computer Forensics in Electronic Documents as Evidence in Criminal Law." *Jurnal Cakrawala Hukum* 14, no. 2 (2023): 155–166. DOI: 10.26905/idjch.v14i2.10820

Santosa dan Kamali menunjukkan bahwa karakteristik bukti digital menyebabkan proses akuisisi dan penyajiannya memerlukan metode yang berbeda dari bukti konvensional, termasuk dalam kaitannya dengan bagaimana hakim mengevaluasi cara bukti tersebut diperoleh dan disajikan³⁰.

Persoalan standarisasi juga ditemukan dalam penelitian internasional. Stoykova, Andersen, Franke, and Axelsson menemukan bahwa dalam sampel investigasi digital pada kepolisian Norwegia terdapat kekurangan dokumentasi yang menyulitkan penilaian reliabilitas bukti digital, termasuk kesulitan menelusuri tindakan forensik dan menghubungkan bukti digital dengan sumbernya³¹. Temuan tersebut relevan dengan penelitian ini karena menunjukkan bahwa kualitas bukti digital tidak hanya ditentukan oleh kecanggihan perangkat forensik, tetapi juga oleh kualitas dokumentasi dan keterlacakan seluruh proses pemeriksaan.

Stoykova and Franke kemudian mengembangkan *Reliability Validation Enabling Framework* (RVEF) yang menempatkan validasi sebagai unsur penting dalam memastikan reliabilitas pemeriksaan digital forensik³². Sementara itu, penelitian mengenai standarisasi pembentukan pendapat evaluatif terhadap bukti digital

menunjukkan pentingnya proses yang sistematis agar kesimpulan terhadap bukti digital tidak hanya didasarkan pada interpretasi subjektif pemeriksa³³.

Berdasarkan temuan empiris dan literatur tersebut, persoalan digital forensik dalam penelitian ini dapat dirumuskan dalam tiga aspek. Pertama, belum optimalnya standarisasi prosedur dari tahap akuisisi hingga pelaporan. Kedua, perbedaan kapasitas teknis penyidik dan unit forensik dapat mempengaruhi konsistensi pemeriksaan. Ketiga, belum sepenuhnya terintegrasinya hasil pemeriksaan teknis dengan kebutuhan pembuktian pada tahap penuntutan dan persidangan.

Dengan demikian, *digital forensic protocol* seharusnya tidak diposisikan semata-mata sebagai pedoman teknis internal kepolisian. Protokol tersebut harus dirancang sedemikian rupa sehingga dapat menghasilkan bukti yang dapat ditelusuri, diverifikasi, dan dipertanggungjawabkan pada seluruh tahapan sistem peradilan pidana³⁴.

3.4 Analisis Sistem Hukum Lawrence

M. Friedman: Substansi, Struktur, dan Budaya Hukum

Temuan penelitian selanjutnya dianalisis menggunakan teori sistem hukum Lawrence

³⁰ Santosa, Dewa Gede Giri, and Karell Mawla Ibnu Kamali. "Acquisition and Presentation of Digital Evidence in Criminal Trial in Indonesia." *Jurnal Hukum dan Peradilan* 11, no. 2 (2022): 195–218. DOI: 10.25216/jhp.11.2.2022.195-218

³¹ Stoykova et al., 2022, *Op cit*

³² Stoykova and Franke, 2023, *Op cit*

³³ Casey, 2011, *Op cit*

³⁴ AlBusaidi, Arwa Juma, Laiha Binti Mat Kiah, and Ainuddin Wahid Bin Abdul Waha. "Toward a Unified Methodology for Preliminary Digital Evidence Assessment: Standardizing Forensic Investigations." *Journal of Forensic Sciences* 70, no. 4 (2025): 1571–1583. DOI: 10.1111/1556-4029.70070

M. Friedman yang memandang bekerjanya hukum melalui interaksi antara substansi hukum (*legal substance*), struktur hukum (*legal structure*), dan budaya hukum (*legal culture*)³⁵.

3.4.1 Substansi Hukum

Dari aspek substansi, penelitian menemukan bahwa dasar hukum penyidikan tindak pidana akses tanpa hak telah tersedia melalui KUHP, UU ITE, UU PDP, dan peraturan kepolisian. Akan tetapi, substansi tersebut tersebar dalam beberapa instrumen dan belum seluruhnya memberikan pedoman teknis yang seragam mengenai pembuktian elektronik³⁶.

Kondisi ini menunjukkan bahwa persoalan substansi bukan semata-mata kekosongan hukum. Persoalan yang lebih mendasar adalah harmonisasi dan operasionalisasi norma. Norma hukum harus mampu menjawab pertanyaan teknis mengenai bagaimana perangkat disita, bagaimana data diakuisisi, bagaimana integritas data diverifikasi, bagaimana *chain of custody* didokumentasikan, dan bagaimana hasil pemeriksaan digital forensik disampaikan kepada penuntut umum dan pengadilan³⁷.

Dengan demikian, *legal substance* dalam penyidikan siber perlu dipahami tidak hanya sebagai keberadaan pasal yang mengkriminalisasi akses tanpa hak atau

mengakui bukti elektronik, tetapi juga sebagai kemampuan sistem hukum menyediakan aturan prosedural yang dapat diterapkan secara konsisten.

3.4.2 Struktur Hukum

Dari aspek struktur, penelitian menunjukkan bahwa Ditres Siber Polda Jawa Timur telah memiliki fungsi kelembagaan yang memungkinkan penyidikan tindak pidana siber dilakukan secara khusus. Akan tetapi, penyidikan siber tidak hanya bergantung pada struktur internal kepolisian. Bukti elektronik sering kali membutuhkan koordinasi dengan lembaga atau pihak lain, terutama ketika data berada pada sistem atau penyelenggara elektronik tertentu.

Hambatan koordinasi dan perbedaan prosedur pertukaran data dapat mempengaruhi kecepatan penyidikan. Hal tersebut menjadi semakin penting karena bukti digital dapat berubah atau hilang apabila tidak segera diamankan. Dengan demikian, struktur hukum dalam penyidikan siber perlu dilihat sebagai jaringan kelembagaan yang menghubungkan kepolisian, kejaksaan, pengadilan, serta lembaga pendukung yang memiliki akses atau kompetensi terhadap data elektronik.

Perspektif ini sejalan dengan penelitian digital forensik yang menunjukkan bahwa kualitas pemeriksaan tidak hanya bergantung pada metode³⁸, tetapi juga pada kemampuan

³⁵ Friedman, 1975, *Op cit*

³⁶ Flora, Henny Saida, et al. *Hukum Pidana di Era Digital*. Batam: Rey Media Grafika, 2024

³⁷ Rasiwan, Iwan. *Suatu Pengantar Hukum Pembuktian Tindak Pidana*. Bantul: Mitra Edukasi Negeri, 2025

³⁸ Stoykova et al. 2022, *Op cit*

organisasi mendokumentasikan dan menjamin keterlacakan proses pemeriksaan³⁹.

3.4.3 Budaya Hukum

Dimensi budaya hukum terlihat dari kapasitas dan perilaku aparat maupun masyarakat dalam menghadapi kejahatan berbasis teknologi. Dari sisi penyidik, kejahatan siber membutuhkan kemampuan memahami teknologi, jaringan, data, dan teknik digital forensik. Ketimpangan kompetensi dapat menyebabkan sebagian tahapan pemeriksaan lebih bergantung pada personel tertentu yang memiliki pengalaman atau keahlian khusus⁴⁰.

Dari sisi masyarakat, rendahnya literasi digital juga dapat mempengaruhi kualitas pelaporan dan pembuktian. Korban tidak selalu memahami pentingnya mempertahankan tangkapan layar, riwayat komunikasi, bukti transaksi, alamat IP, atau informasi digital lainnya. Akibatnya, sebagian bukti awal dapat hilang atau tidak terdokumentasikan dengan baik sebelum perkara dilaporkan.

Dalam perspektif Friedman, kondisi tersebut menunjukkan bahwa efektivitas hukum tidak cukup dibangun melalui pembentukan peraturan. Substansi hukum yang baik tetap membutuhkan struktur yang mampu menerapkannya dan budaya hukum

yang mendukung kepatuhan serta partisipasi masyarakat⁴¹.

Dengan demikian, temuan penelitian menunjukkan bahwa problem pembuktian elektronik merupakan persoalan sistemik. Kelemahan pada satu dimensi—misalnya standar teknis—dapat mempengaruhi struktur kelembagaan dan pada akhirnya berpengaruh terhadap budaya kerja penyidik maupun kepercayaan masyarakat terhadap proses penegakan hukum.

3.5 Operasionalisasi Integrated Criminal Justice System dalam Penyidikan Siber

Konsep *Integrated Criminal Justice System* (ICJS) digunakan dalam penelitian ini untuk melihat sejauh mana penyidikan tindak pidana akses tanpa hak telah terhubung dengan subsistem peradilan pidana lainnya. Dalam konteks konvensional, keterpaduan tersebut dapat dilihat dari kesinambungan proses penyelidikan, penyidikan, penuntutan, pemeriksaan pengadilan, dan pelaksanaan putusan⁴². Dalam konteks kejahatan siber, keterpaduan tersebut menjadi lebih kompleks karena terdapat dimensi teknis berupa pertukaran dan pemeriksaan data elektronik⁴³.

Temuan penelitian menunjukkan bahwa proses penyidikan telah melibatkan koordinasi antarsubsistem, tetapi belum sepenuhnya

³⁹ Miller, Christa M. "A Survey of Prosecutors and Investigators Using Digital Evidence: A Starting Point." *Forensic Science International: Synergy* 6 (2023): 100296. DOI: 10.1016/j.fsisyn.2022.100296

⁴⁰ Sakti, Abdul. "Pengaruh Pendidikan dan Pelatihan Digital Forensik terhadap Kualitas

Penanganan Kasus Kejahatan Siber." *Populer: Jurnal Penelitian Mahasiswa* 4, no. 1 (2025): 104–109

⁴¹ Friedman, 1975, *Op cit*

⁴² Miller, 2023, *Op cit*

⁴³ Stoykova, 2024, *Op cit*

didukung mekanisme pertukaran data dan prosedur teknis yang seragam. Penyidik dapat memerlukan informasi dari lembaga atau penyelenggara sistem elektronik tertentu, sementara proses pemeriksaan digital forensik memerlukan kapasitas teknis yang tidak selalu berada pada satu unit kelembagaan.

Persoalan tersebut menunjukkan bahwa ICJS dalam konteks cybercrime tidak cukup dipahami sebagai koordinasi administratif antarpenghak hukum. ICJS harus mencakup integrasi informasi, standar pembuktian, prosedur pengelolaan bukti, dan pemahaman bersama mengenai kualitas bukti elektronik.

Stoykova menegaskan bahwa digital evidence memiliki implikasi langsung terhadap prinsip *fair trial*, *equality of arms*, dan *presumption of innocence*. Oleh karena itu, aturan dan praktik mengenai bukti digital harus dirancang sedemikian rupa sehingga seluruh pihak dalam proses peradilan dapat memahami dasar dan reliabilitas bukti yang digunakan⁴⁴.

Dalam konteks penelitian ini, koordinasi ICJS setidaknya perlu mencakup empat hubungan utama. Pertama, hubungan penyidik dengan penuntut umum untuk memastikan bahwa bukti elektronik yang diperoleh pada tahap penyidikan memenuhi kebutuhan pembuktian pada tahap penuntutan. Kedua, hubungan penyidik dengan pengadilan melalui pemenuhan standar pembuktian dan

dokumentasi pemeriksaan. Ketiga, hubungan kepolisian dengan lembaga pendukung yang menguasai data atau memiliki kompetensi teknis. Keempat, integrasi antara unit investigasi dan unit digital forensik agar proses pemeriksaan teknis tetap memiliki keterkaitan dengan konstruksi perkara⁴⁵.

Dengan demikian, temuan penelitian menunjukkan bahwa ICJS pada penyidikan tindak pidana akses tanpa hak masih memerlukan penguatan pada dimensi teknis. Sistem yang terintegrasi bukan hanya sistem yang memungkinkan pertukaran informasi, tetapi sistem yang memastikan bahwa informasi tersebut diperoleh secara sah, dikelola secara aman, dapat diverifikasi, dan dapat digunakan secara konsisten dalam proses pembuktian.

3.6 Perspektif Perbandingan: Standardisasi Digital Evidence dan Cybercrime Investigation

Pengalaman internasional menunjukkan bahwa persoalan bukti elektronik pada dasarnya memiliki dimensi universal, meskipun setiap negara memiliki sistem hukum acara pidana yang berbeda. Salah satu persoalan yang terus muncul adalah bagaimana memastikan reliabilitas proses digital forensik dan bagaimana menghubungkan hasil pemeriksaan teknis dengan kebutuhan pembuktian hukum.

⁴⁴ Stoykova, 2023, *Op cit*

⁴⁵ De Hert, Paul, Cihan Parlan, and Juraj Sajfert. "The Cybercrime Convention Committee's 2017 Guidance Note on Production Orders: Unilateralist

Transborder Access to Electronic Evidence Promoted via Soft Law." *Computer Law & Security Review* 34, no. 2 (2018): 327–336. DOI: 10.1016/j.clsr.2018.01.003

Valjarevic and Venter menekankan pentingnya model investigasi digital forensik yang komprehensif dan harmonis agar tahapan investigasi dapat dilaksanakan secara sistematis. Pendekatan tersebut relevan dengan temuan penelitian di Polda Jawa Timur karena fragmentasi prosedur dapat menghasilkan variasi dalam cara bukti diperoleh, diperiksa, dan didokumentasikan⁴⁶.

Penelitian Stoykova et al. mengenai praktik kepolisian Norwegia memberikan pelajaran penting bahwa keberadaan tenaga ahli dan perangkat digital forensik belum otomatis menjamin reliabilitas pemeriksaan. Dokumentasi tindakan pemeriksaan, keterlacakan proses, justifikasi metode dan alat, serta validasi hasil tetap diperlukan⁴⁷.

Demikian pula, penelitian mengenai standardisasi digital forensic reporting menunjukkan bahwa laporan forensik perlu menjelaskan ruang lingkup pemeriksaan, teknologi dan metode yang digunakan, serta proses yang dilakukan terhadap bukti digital. Transparansi tersebut penting agar pihak lain dapat memahami bagaimana kesimpulan forensik diperoleh dan menilai reliabilitasnya.

Dari perspektif hukum, Stoykova menunjukkan bahwa digital evidence dapat menimbulkan persoalan terhadap fairness apabila penggunaan teknologi tidak disertai prosedur dan standar reliabilitas yang

memadai⁴⁸. Artinya, standardisasi digital forensik bukan hanya persoalan efisiensi investigasi, tetapi juga merupakan bagian dari perlindungan hak dalam proses peradilan pidana.

Perbandingan tersebut memberikan implikasi bagi Indonesia. Standardisasi yang diperlukan bukan berarti mengadopsi satu model asing secara utuh, tetapi membangun standar nasional yang sesuai dengan sistem hukum Indonesia dengan memperhatikan prinsip-prinsip universal digital forensics, antara lain:

1. integritas, yaitu menjamin bahwa bukti tidak mengalami perubahan yang tidak dapat dijelaskan;
2. autentisitas, yaitu memastikan hubungan antara bukti dan sumbernya;
3. keterlacakan, yaitu setiap tindakan terhadap bukti dapat didokumentasikan;
4. reproducibility, yaitu metode pemeriksaan dapat dijelaskan dan, sepanjang memungkinkan, diverifikasi;
5. akuntabilitas, yaitu pemeriksa dapat mempertanggungjawabkan metode dan kesimpulan yang digunakan; dan
6. protection of rights, yaitu proses pemeriksaan tetap menghormati privasi, due process, dan hak pihak yang diperiksa.

Dengan demikian, perspektif perbandingan memperkuat temuan bahwa

⁴⁶ Valjarevic, Aleksandar, and Hein S. Venter. "A Comprehensive and Harmonized Digital Forensic Investigation Process Model." *Journal of Forensic*

Sciences 60, no. 6 (2015): 1467–1483. DOI: 10.1111/1556-4029.12823

⁴⁷ Stoykova et al. 2022, *Op cit*

⁴⁸ Stoykova, 2021, *Op cit*

kebutuhan Indonesia bukan hanya penambahan norma mengenai bukti elektronik, tetapi pembentukan ekosistem prosedural yang menjadikan bukti digital dapat dipercaya secara teknis sekaligus dapat dipertanggungjawabkan secara hukum.

3.7 Sintesis Temuan: Dari *Person-Dependent Investigation* menuju *Integrated Cyber Investigation*

Berdasarkan keseluruhan temuan, problematika penyidikan tindak pidana akses tanpa hak di Polda Jawa Timur tidak dapat dijelaskan hanya melalui keterbatasan teknologi atau belum lengkapnya regulasi. Temuan penelitian menunjukkan adanya hubungan antara empat persoalan utama, yaitu fragmentasi regulasi, ketidakseragaman prosedur digital forensik, kapasitas sumber daya manusia, dan koordinasi antarlembaga.

Pertama, pada tingkat substansi hukum, regulasi mengenai akses tanpa hak, bukti elektronik, perlindungan data, dan penyidikan telah tersedia, tetapi tersebar dalam berbagai instrumen. Kondisi tersebut menyebabkan penyidik harus melakukan interpretasi dan penyesuaian dalam mengoperasionalkan beberapa norma sekaligus.

Kedua, pada tingkat teknis, pemeriksaan bukti elektronik membutuhkan prosedur yang lebih terstandar. Bukti digital tidak cukup hanya dikumpulkan, tetapi harus dapat ditunjukkan asal-usulnya, proses akuisisinya,

integritasnya, metode pemeriksaannya, dan hubungan antara temuan digital dengan unsur tindak pidana. Literatur internasional menunjukkan bahwa kekurangan dokumentasi dan validasi dapat mengurangi kemampuan sistem untuk menilai reliabilitas bukti digital⁴⁹.

Ketiga, pada tingkat struktur, koordinasi antarlembaga belum sepenuhnya terintegrasi dalam satu mekanisme teknis yang memungkinkan pertukaran informasi secara cepat, aman, dan terstandar. Dalam konteks cybercrime, persoalan ini menjadi semakin penting karena data elektronik dapat tersebar pada berbagai sistem dan penyelenggara.

Keempat, pada tingkat budaya hukum, efektivitas penyidikan dipengaruhi oleh kompetensi digital penyidik dan kesadaran masyarakat mengenai pentingnya menjaga bukti elektronik. Kondisi tersebut menunjukkan bahwa penguatan hukum tidak dapat hanya diarahkan pada perubahan peraturan, tetapi juga harus mencakup pembangunan kapasitas manusia dan budaya kerja yang mendukung integritas bukti digital.

Atas dasar itu, temuan penelitian menunjukkan adanya pergeseran persoalan dari “apakah bukti elektronik dapat digunakan?” menuju pertanyaan yang lebih substantif, yaitu “bagaimana bukti elektronik diperoleh, divalidasi, dikelola, dan dinilai secara konsisten dalam seluruh tahapan sistem peradilan pidana?” Pergeseran pertanyaan tersebut penting karena pengakuan normatif

⁴⁹ Stoykova and Franke, 2023, *Op cit*

terhadap bukti elektronik tidak otomatis menjamin reliabilitas proses pembuktiannya.

Dalam konteks ini, istilah *person-dependent investigation* digunakan untuk menggambarkan kondisi ketika kualitas penyidikan sangat bergantung pada kapasitas individual penyidik atau personel digital forensik. Kondisi tersebut tidak berarti bahwa penyidik tidak memiliki kemampuan, tetapi menunjukkan bahwa kemampuan individual belum sepenuhnya dikonversi menjadi standar kelembagaan yang dapat diterapkan secara konsisten.

Temuan tersebut mengarah pada kebutuhan transformasi menuju *integrated cyber investigation*, yaitu model penyidikan yang mengintegrasikan empat komponen utama:

Komponen	Kondisi yang Ditemukan	Arah Penguatan
Legal substance	Regulasi tersebar dalam KUHAP, UU ITE, UU PDP, dan regulasi penyidikan	Harmonisasi dan pedoman pembuktian elektronik
Digital forensic procedure	Belum sepenuhnya seragam	Standar nasional <i>digital forensic protocol</i> dan <i>chain of custody</i>
Legal structure	Koordinasi antarlembaga belum optimal	Mekanisme pertukaran data dan koordinasi lintas lembaga

Legal culture	Kapasitas teknis dan literasi digital tidak seragam	Pelatihan berkelanjutan dan penguatan literasi digital
----------------------	---	--

Model tersebut menunjukkan bahwa reformasi penyidikan siber tidak cukup dilakukan dengan memperkuat satu komponen. Penguatan norma tanpa peningkatan kapasitas struktur dapat menghasilkan aturan yang sulit diterapkan. Sebaliknya, peningkatan kemampuan teknis tanpa standardisasi hukum dapat menghasilkan praktik yang berbeda-beda. Oleh karena itu, penguatan penyidikan harus dilakukan secara simultan antara substansi, struktur, dan budaya hukum.

Sintesis tersebut juga memperkuat argumentasi bahwa ICJS dalam konteks cybercrime harus berkembang dari sekadar koordinasi antaraktor menjadi integrasi prosedural dan teknis. Integrasi tersebut mencakup kesamaan pemahaman mengenai standar bukti, mekanisme pertukaran informasi, dokumentasi digital forensic, serta hubungan antara hasil pemeriksaan teknis dengan kebutuhan pembuktian pada tahap penuntutan dan persidangan.

Dengan demikian, kontribusi utama penelitian ini terletak pada identifikasi *fragmented cyber procedural regime* sebagai persoalan sistemik dalam penyidikan tindak pidana akses tanpa hak. Penelitian menunjukkan bahwa meskipun mekanisme penyidikan pada perkara Nomor 293/Pid.Sus/2023/PN Mjk dapat berjalan dan

bukti elektronik dapat digunakan dalam proses pembuktian, mekanisme tersebut masih membutuhkan standardisasi dan integrasi agar tidak bergantung pada kapasitas individual. Oleh karena itu, model penyidikan siber yang lebih terintegrasi perlu dibangun melalui harmonisasi hukum acara, standardisasi *digital forensic protocol*, penguatan koordinasi lintas lembaga, peningkatan kapasitas penyidik, serta perlindungan hak atas data pribadi.

Pada akhirnya, penguatan penyidikan tindak pidana akses tanpa hak bukan semata-mata persoalan memperluas kewenangan penegak hukum atau memperbanyak instrumen teknologi. Persoalan utamanya adalah membangun sistem yang mampu menjamin bahwa setiap bukti elektronik diperoleh secara sah, dikelola secara dapat ditelusuri, diperiksa melalui metode yang dapat dipertanggungjawabkan, dan dipresentasikan secara konsisten dalam seluruh tahapan sistem peradilan pidana. Kerangka tersebut menjadi dasar bagi pengembangan model integrated cyber investigation yang berorientasi pada autentisitas bukti, konsistensi prosedural, perlindungan hak, dan kepastian hukum.

IV. KESIMPULAN

Penelitian ini menunjukkan bahwa mekanisme penyidikan tindak pidana akses tanpa hak pada Direktorat Reserse Siber Polda Jawa Timur telah dilaksanakan berdasarkan kerangka hukum acara pidana, UU ITE, UU PDP, dan ketentuan teknis penyidikan

kepolisian. Dalam perkara Nomor 293/Pid.Sus/2023/PN Mjk, mekanisme tersebut mampu menghasilkan bukti elektronik yang digunakan dan diterima dalam proses peradilan. Namun, keberhasilan pada tingkat perkara individual belum menunjukkan bahwa sistem pembuktian elektronik telah terstandardisasi secara menyeluruh.

Temuan utama penelitian menunjukkan adanya fragmented cyber procedural regime, yaitu keterpisahan antara norma hukum acara, pengaturan bukti elektronik, perlindungan data pribadi, dan prosedur digital forensik. Fragmentasi tersebut menghasilkan kesenjangan antara norma dan praktik, terutama pada standardisasi akuisisi, preservasi, pemeriksaan, validasi, dan dokumentasi bukti elektronik. Akibatnya, praktik penyidikan masih memiliki karakter *person-dependent* karena kualitas proses sangat dipengaruhi kapasitas dan pengalaman penyidik serta pemeriksa digital forensik.

Dari perspektif ICJS, problem tidak hanya terdapat pada proses internal kepolisian, tetapi juga pada hubungan antarsubsistem penegakan hukum dan lembaga pendukung. Koordinasi penyidik, penuntut umum, pengadilan, serta lembaga yang memiliki kewenangan terhadap data dan infrastruktur digital membutuhkan standar pertukaran informasi dan pemahaman pembuktian yang lebih terpadu. Sementara dari perspektif teori sistem hukum Friedman, persoalan tersebut mencakup tiga dimensi sekaligus: substansi hukum yang belum sepenuhnya operasional,

struktur hukum yang belum terintegrasi secara digital, dan budaya hukum yang masih membutuhkan penguatan kompetensi serta literasi digital.

Penelitian ini memberikan kontribusi pada pengembangan kajian hukum siber dengan menghubungkan pembuktian elektronik, digital forensik, teori sistem hukum, dan ICJS dalam satu kerangka analisis empiris. Kontribusi tersebut memperlihatkan bahwa penguatan substansi hukum saja tidak cukup apabila tidak diikuti reformasi struktur kelembagaan dan standardisasi praktik.

Implikasi penelitian adalah perlunya membangun sistem penyidikan siber yang tidak hanya berbasis kepatuhan terhadap peraturan, tetapi juga berbasis standardisasi proses dan integrasi kelembagaan. Agenda reformasi yang direkomendasikan meliputi: (1) penyusunan pedoman teknis terpadu pembuktian elektronik; (2) pembentukan dan penerapan standar digital forensic protocol; (3) integrasi mekanisme pertukaran data antara lembaga penegak hukum dan lembaga pendukung; dan (4) peningkatan kapasitas penyidik serta pemeriksa digital forensik secara berkelanjutan.

Perkembangan hukum melalui Undang-Undang Nomor 20 Tahun 2025 tentang KUHAP yang secara eksplisit mengakui bukti elektronik merupakan langkah penting dalam memperkuat substansi hukum. Namun, efektivitas perubahan tersebut tetap bergantung pada pembentukan standar teknis dan kelembagaan yang mampu menjamin

otentisitas, integritas, reliabilitas, dan *chain of custody* bukti elektronik. Dengan demikian, arah pembaruan hukum acara pidana digital perlu bergerak dari sekadar pengakuan bukti elektronik menuju sistem pembuktian elektronik yang terintegrasi dan berorientasi pada kepastian hukum.

DAFTAR PUSTAKA

1. Buku

- Casey, Eoghan. *Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet*. 3rd ed. London: Academic Press, 2011.
- Flora, Henny Saida, et al. *Hukum Pidana di Era Digital*. Batam: Rey Media Grafika, 2024.
- Friedman, Lawrence M. *The Legal System: A Social Science Perspective*. New York: Russell Sage Foundation, 1975.
- Hamzah, Andi. *Cyber Crime: Kejahatan Masa Depan*. Jakarta: Sinar Grafika, 2015.
- Rasiwan, Iwan. *Suatu Pengantar Hukum Pembuktian Tindak Pidana*. Bantul: Mitra Edukasi Negeri, 2025.

2. Peraturan Perundang-Undangan Dan Putusan

- Indonesia. *Undang-Undang Nomor 8 Tahun 1981 tentang Hukum Acara Pidana*. Jakarta: Pemerintah Republik Indonesia, 1981.
- Indonesia. *Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik*. Jakarta: Pemerintah Republik Indonesia, 2008.
- Indonesia. *Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik*. Jakarta: Pemerintah Republik Indonesia, 2016.
- Indonesia. *Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data*

Pribadi. Jakarta: Pemerintah Republik Indonesia, 2022.

Indonesia. *Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik*. Jakarta: Pemerintah Republik Indonesia, 2024.

Indonesia. *Undang-Undang Nomor 20 Tahun 2025 tentang Kitab Undang-Undang Hukum Acara Pidana*. Jakarta: Pemerintah Republik Indonesia, 2025.

Kepolisian Negara Republik Indonesia. *Peraturan Kepolisian Negara Republik Indonesia Nomor 6 Tahun 2019 tentang Penyidikan Tindak Pidana*. Jakarta: Kepolisian Negara Republik Indonesia, 2019.

Pengadilan Negeri Mojokerto. *Putusan Nomor 293/Pid.Sus/2023/PN Mjk*.

3. Jurnal

AlBusaidi, Arwa Juma, Laiha Binti Mat Kiah, and Ainuddin Wahid Bin Abdul Waha. "Toward a Unified Methodology for Preliminary Digital Evidence Assessment: Standardizing Forensic Investigations." *Journal of Forensic Sciences* 70, no. 4 (2025): 1571–1583. DOI: 10.1111/1556-4029.70070.

Casey, Eoghan. "Standardization of Forming and Expressing Preliminary Evaluative Opinions on Digital Evidence." *Forensic Science International: Digital Investigation* 32 (2020): 200888. DOI: 10.1016/j.fsidi.2019.200888.

De Hert, Paul, Cihan Parlan, and Juraj Sajfert. "The Cybercrime Convention Committee's 2017 Guidance Note on Production Orders: Unilateralist Transborder Access to Electronic Evidence Promoted via Soft Law." *Computer Law & Security Review* 34, no. 2 (2018): 327–336. DOI: 10.1016/j.clsr.2018.01.003.

Faizah, Fajrini, and Moh. Karim. "Kekuatan Alat Bukti terhadap Pembuktian Tindak

Pidana Cyber Crime." *Jurnal Ilmu Hukum Wijaya Putra* 3, no. 1 (2025): 46–53.

Hardianto, Aris, Barda Nawawi Arief, and Joko Setiyono. "The Significance of Computer Forensics in Electronic Documents as Evidence in Criminal Law." *Jurnal Cakrawala Hukum* 14, no. 2 (2023): 155–166. DOI: 10.26905/idjch.v14i2.10820.

Horsman, Graeme. "Standardizing Digital Forensic Examination Procedures: A Look at Windows 10 in Cases Involving Images Depicting Child Sexual Abuse." *WIREs Forensic Science* 3, no. 6 (2021): e1417. DOI: 10.1002/wfs2.1417.

Ismail, Muh. Akbar, H. Thalib, and A. Arief. "Efektivitas Penyidikan terhadap Pelaku Tindak Pidana Illegal Access di Kepolisian Resor Soppeng." *Journal of Lex Philosophy* 5, no. 1 (2024): 143–159.

July, Wiarti. "Legality of Electronic Evidence in Cyber Crime Cases." *Ahmad Dahlan Indonesian Law Journal* 1, no. 2 (2023): 11–19. DOI: 10.12928/adil.v1i1.572.

Karie, N. M., H. S. Venter, and J. H. P. Eloff. "The Stages of Cybercrime Investigations: Bridging the Gap between Technology Examination and Law Enforcement Investigation." *Computer Law & Security Review* 27, no. 1 (2011): 61–67. DOI: 10.1016/j.clsr.2010.11.001.

Miller, Christa M. "A Survey of Prosecutors and Investigators Using Digital Evidence: A Starting Point." *Forensic Science International: Synergy* 6 (2023): 100296. DOI: 10.1016/j.fsisyn.2022.100296.

Mustika, Julia, et al. "Urgensi Digital Forensik untuk Pembuktian Tindak Pidana Siber dalam Konteks Merusak Data dan Sistem Elektronik." *JAITS: Journal of Applied Information Technology Solution* 2, no. 1 (2025): 1–6.

- Pribadi, Insan. "Legalitas Alat Bukti Elektronik dalam Sistem Peradilan Pidana." *Lex Renaissance* 3, no. 1 (2019). DOI: 10.20885/JLR.vol3.iss1.art4.
- Sakti, Abdul. "Pengaruh Pendidikan dan Pelatihan Digital Forensik terhadap Kualitas Penanganan Kasus Kejahatan Siber." *Populer: Jurnal Penelitian Mahasiswa* 4, no. 1 (2025): 104–109.
- Santosa, Dewa Gede Giri, and Karell Mawla Ibnu Kamali. "Acquisition and Presentation of Digital Evidence in Criminal Trial in Indonesia." *Jurnal Hukum dan Peradilan* 11, no. 2 (2022): 195–218. DOI: 10.25216/jhp.11.2.2022.195-218.
- Sitanggang, A. S., F. Darmawan, and D. Saputra. "Hukum Siber dan Penegakan Hukum di Indonesia: Tantangan dan Solusi Memerangi Kejahatan Siber." *Jurnal Pendidikan dan Teknologi Indonesia* 4, no. 3 (2024): 79–83.
- Stoykova, Radina. "A New Right to Procedural Accuracy: A Governance Model for Digital Evidence in Criminal Proceedings." *Computer Law & Security Review* 55 (2024): 106040. DOI: 10.1016/j.clsr.2024.106040.
- Stoykova, Radina. "Digital Evidence: Unaddressed Threats to Fairness and the Presumption of Innocence." *Computer Law & Security Review* 42 (2021): 105575. DOI: 10.1016/j.clsr.2021.105575.
- Stoykova, Radina. "The Right to a Fair Trial as a Conceptual Framework for Digital Evidence Rules in Criminal Investigations." *Computer Law & Security Review* 49 (2023): 105801. DOI: 10.1016/j.clsr.2023.105801.
- Stoykova, Radina, and Katrin Franke. "Reliability Validation Enabling Framework (RVEF) for Digital Forensics in Criminal Investigations." *Forensic Science International: Digital Investigation* 45 (2023): 301554. DOI: 10.1016/j.fsidi.2023.301554.
- Stoykova, Radina, Stig Andersen, Katrin Franke, and Stefan Axelsson. "Reliability Assessment of Digital Forensic Investigations in the Norwegian Police." *Forensic Science International: Digital Investigation* 40 (2022): 301351. DOI: 10.1016/j.fsidi.2022.301351.
- Sumardiana, Benny, Pujiyono, Irma Cahyaningtyas, and Cahya Wulandari. "Evaluation of Electronic Evidence in Criminal Justice in the Era of Advanced Artificial Intelligence Technology." *Indonesian Journal of Criminal Law Studies* 9, no. 2 (2024). DOI: 10.15294/ijcls.v9i2.36634.
- Tully, Gillian, Neil Cohen, David Compton, Gareth Davies, Roy Isbell, and Tim Watson. "Quality Standards for Digital Forensics: Learning from Experience in England & Wales." *Forensic Science International: Digital Investigation* 32 (2020): 200905. DOI: 10.1016/j.fsidi.2020.200905.
- Valjarevic, Aleksandar, and Hein S. Venter. "A Comprehensive and Harmonized Digital Forensic Investigation Process Model." *Journal of Forensic Sciences* 60, no. 6 (2015): 1467–1483. DOI: 10.1111/1556-4029.12823.
- Wu, Hong, and Guan Zheng. "Electronic Evidence in the Blockchain Era: New Rules on Authenticity and Integrity." *Computer Law & Security Review* 36 (2020): 105401. DOI: 10.1016/j.clsr.2020.105401.
- Yar, Majid, and Kevin F. Steinmetz. "The Contemporary Cybercrime Ecosystem: A Multi-Disciplinary Overview of the State of Affairs and Developments." *Computer Law & Security Review* 34, no. 6 (2018): 1180–1196. DOI: 10.1016/j.clsr.2018.08.005.