SENTRI:
Jurnal Riset Ilmiah
ejournal.nusantaraglobal.ac.id/index.php/sentri

Vol. 4, No. 8, 2025
e-ISSN: 2963-1130
pp. 1346-1360

Transformasi Modus Kejahatan Ekonomi Transnasional di Era Digital: Analisis Hukum Pidana dan Teknik Forensik Siber

Arief Agus Djunarjanto[1*], Ani Purwati[2], Liza Marina[2]
[1]Mahasiswa Magister Hukum Sekolah Pasca Sarjana Universitas Sahid
[2]Dosen Magister Hukum Sekolah Pasca Sarjana Universitas Sahid

*Corresponding Author's e-mail: arief.agus.d@gmail.com

Article History:
Received: August 10, 2025
Revised: August 18, 2025
Accepted: August 20, 2025

Keywords:
Transnational Economic Crime, Digital Era, Cyber Forensics, Money Laundering, International Collaboration

Abstract: *The transformation of transnational economic crime in the digital era has fundamentally changed the way perpetrators commit crimes, presenting new challenges for criminal law enforcement. This study adopts a normative juridical approach, utilizing statutory analysis, case studies, and comparative law to examine the evolution of digital economic crimes and the strategic role of cyber forensics. Case studies such as money laundering through crypto assets using chain hopping techniques and Business Email Compromise (BEC) schemes reveal the complexity of cross-border jurisdiction, legal gaps in defining digital assets like cryptocurrency and NFTs, and evidentiary challenges in presenting digital proof in court. Cyber forensics, through techniques such as network forensics, malware analysis, and blockchain analysis, has proven crucial in collecting and validating digital evidence. However, law enforcement continues to face obstacles, including limited regulations, insufficient human resource capacity, and increasingly sophisticated anti-forensic techniques. This research recommends regulatory updates, enhanced training for law enforcement personnel, strengthened international cooperation, and public education to raise awareness of digital crime risks. Synergy between criminal law, forensic technology, and cross-border collaboration is essential for effectively combating digital economic crimes.*

How to cite: Djunarjanto, A. A., Purwati, A., & Marina, L. (2025). Transformasi Modus Kejahatan Ekonomi Transnasional di Era Digital: Analisis Hukum Pidana dan Teknik Forensik Siber. *SENTRI: Jurnal Riset Ilmiah*, *4*(8), 1346–1360. https://doi.org/10.55681/sentri.v4i8.4448

PENDAHULUAN

Transformasi modus kejahatan ekonomi transnasional di era digital telah mengakibatkan perubahan signifikan dalam modus kejahatan yang dilakukan dan berdampak besar pada penegakan hukum. Berbagai jenis kejahatan seperti pencurian data, penipuan, dan cybercrime lainnya kini telah menggunakan teknologi sebagai alat utama. Dalam konteks ini, hukum pidana dan teknik forensik siber menjadi dua hal mendasar yang saling terkait dan sangat penting untuk ditelaah lebih lanjut.

Dalam analisis kejahatan ekonomi transnasional, salah satu metode yang sangat relevan adalah digital forensics, yang dikenal sebagai forensik digital. Digital forensics membantu dalam mengevaluasi dan menyelidiki jejak digital yang ditinggalkan oleh pelaku kejahatan, memungkinkan penegak hukum untuk mengumpulkan bukti yang diperlukan dalam proses peradilan. Sebagai contoh, penelitian menunjukkan bahwa aplikasi digital forensik seperti Autopsy mampu melakukan pengembalian data yang telah dihapus, yang seringkali menjadi tantangan bagi penyidik kejahatan digital (Julian & Sutabri, 2023). Dalam banyak insiden, pelaku menggunakan teknik untuk menghapus data

dengan tujuan menghilangkan jejak, sehingga forensik digital menjadi sangat penting untuk menyelidiki kasus-kasus semacam itu (Iman et al., 2020; Riadi et al., 2019) .

Selain itu, tantangan dalam penegakan hukum terhadap kejahatan digital semakin kompleks karena modus operandi pelaku yang terus berevolusi. Kasus-kasus yang melibatkan aplikasi media sosial dan layanan cloud sering kali membutuhkan pendekatan investigasi khusus, karena setiap platform dapat memiliki arsitektur teknis yang berbeda dan tantangan tersendiri dalam hal keandalan data serta aksesibilitas informasi yang diperlukan untuk forensik (Ramansyah et al., 2021). Keberadaan platform gaming dan aplikasi chat yang memberikan kemudahan akses informasi membuat penegakan hukum menjadi lebih sulit, sehingga teknik forensik harus selalu diperbarui dan disesuaikan dengan perkembangan teknologi terbaru(Faridi, 2019).

Kemajuan dalam alat dan server cloud memberikan kesempatan bagi penjahat untuk menyembunyikan jejak kejahatannya dengan lebih efisien. Sebagai contoh, analisis terhadap aplikasi cloud seperti Owncloud menunjukkan bahwa data yang sudah dihapus dapat dibuktikan kembali melalui teknik yang sesuai, meningkatkan peluang penegakan hukum dalam menyelidiki dan mengumpulkan informasi yang relevan (Jayanti, 2020).Meskipun terdapat banyak kemampuan dalam digital forensics, masih ada kebutuhan untuk pengembangan dan penelitian lebih lanjut mengenai teknik dan aplikasi yang berlainan agar didapat hasil yang lebih baik dan akurat (Andria, 2021).

Setiap bukti digital yang dikumpulkan harus diperlakukan dengan mengikuti metode yang sudah distandarisasi, yang sering kali mengacu pada praktik terbaik dalam digital forensics. Penegakan hukum diharuskan memperhatikan semua detail dalam pengumpulan dan analisis bukti, dan memanfaatkan alat yang tepat untuk memastikan hasil yang dihasilkan dapat dipertanggungjawabkan di pengadilan ((Riadi et al., 2019) ;(Sunardi et al., 2020). Oleh karena itu, pengembangan alat forensik dan kemampuan penegak hukum untuk memahami dan mengimplementasikan teknik baru menjadi kunci sukses dalam menangani kejahatan ekonomi transnasional di era digital.

Pentingnya edukasi mengenai kejahatan digital dan forensik tidak dapat diabaikan. Dengan meningkatnya penggunaan teknologi di kalangan masyarakat, pengetahuan dan kesadaran tentang risiko yang ada, serta cara untuk menghindari atau menghadapinya harus menjadi prioritas. Upaya ini tidak hanya akan membantu dalam pencegahan kejahatan, tetapi juga memperkuat proses forensik dengan memberi pembelajaran yang lebih baik kepada segenap masyarakat tentang bagaimana bukti digital dapat digunakan dalam proses hukum.

Kejahatan ekonomi transnasional di era digital merupakan fenomena yang semakin kompleks dan menuntut adanya kolaborasi erat antara perangkat hukum, teknik forensik, dan edukasi masyarakat. Perubahan pola kejahatan yang semakin canggih menjadikan investigasi berbasis bukti digital sebagai pilar penting dalam meningkatkan kualitas penegakan hukum. Sejalan dengan itu, inovasi dalam bidang digital forensics harus terus berkembang guna mengimbangi kecepatan perubahan modus operandi para pelaku. Untuk mencapai efektivitas dalam pemberantasan kejahatan ekonomi transnasional berbasis digital, diperlukan sinergi yang kuat antara pemerintah, lembaga penegak hukum, serta institusi pendidikan sebagai pemangku kepentingan utama dalam membangun kerangka kerja yang terpadu.

Rumusan permasalahan yang diajukan dalam penelitian ini mencakup tiga hal pokok. Pertama, bagaimana transformasi modus operandi kejahatan ekonomi transnasional di era digital. Kedua, apa saja tantangan serta problematika hukum pidana,

baik dari aspek materiil maupun formil, dalam menjerat pelaku kejahatan ekonomi transnasional digital. Ketiga, bagaimana peran strategis serta teknik forensik siber dapat dioptimalkan guna mendukung proses pembuktian dalam penegakan hukum pidana.

Adapun tujuan penelitian ini adalah untuk menganalisis serta memetakan bentuk-bentuk transformasi modus operandi kejahatan ekonomi transnasional digital, mengidentifikasi serta mengkritisi kelemahan kerangka hukum pidana Indonesia maupun internasional, serta merumuskan peran ideal forensik siber sebagai alat bukti yang sah dan meyakinkan dalam sistem peradilan pidana.

Signifikansi penelitian ini terletak pada kontribusi akademis maupun praktisnya, karena mengkaji interkoneksi antara hukum pidana, teknologi, dan hukum internasional, sekaligus memberikan rekomendasi bagi legislator dan aparat penegak hukum. Kebaruan penelitian ini ada pada pendekatan terintegrasi yang menghubungkan kajian yuridis dengan aspek teknis forensik siber, di mana analisis teknis dipandang sebagai bagian tak terpisahkan serta menjadi prasyarat mutlak bagi keberhasilan penegakan hukum terhadap kejahatan siber modern.

LANDASAN TEORI

2.1 Konsep Kejahatan Ekonomi Transnasional

Kejahatan ekonomi transnasional dapat diartikan sebagai kegiatan ilegal yang melibatkan pelanggaran hukum di beberapa negara demi keuntungan finansial. Konsep ini telah disusun dalam kerangka hukum internasional yang tidak hanya mencakup aspek legalitas tetapi juga dampak sosial dan ekonomi dari kejahatan tersebut. Salah satu instrumen penting dalam kerangka hukum internasional adalah Konvensi PBB Menentang Kejahatan Terorganisir Transnasional (UNTOC), yang diadopsi pada November 2000, menyediakan mekanisme hukum untuk memerangi kejahatan transnasional dan memperkuat kolaborasi optimal antar lembaga penegak hukum di seluruh dunia, (Tennant, 2021).

Ruang lingkup UNTOC mencakup berbagai kejahatan, termasuk perdagangan manusia, penyelundupan migran, dan kejahatan keuangan yang bersifat lintas negara. UNTOC memberikan perangkat hukum bagi negara-negara untuk melawan berbagai bentuk kejahatan transnasional sekaligus mendorong penelitian lebih lanjut dalam bidang kriminalitas ini (Tennant, 2021). Sebagai bagian dari upaya internasional yang lebih besar, konvensi ini mendorong partisipasi aktif dari 190 negara, menjadikannya salah satu instrumen paling luas yang mengatur kejahatan transnasional.

2.2 Karakteristik Kejahatan Ekonomi Transnasional

Kejahatan ekonomi transnasional memiliki beberapa karakteristik penting: terorganisir, melintasi batas negara, bermotif ekonomi, dan memanfaatkan teknologi modern. Pertama, sifat terorganisir dari kejahatan ini memungkinkan kelompok kriminal untuk mengkoordinasikan aktivitas ilegal dengan baik, memanfaatkan jaringan internasional, serta beroperasi dengan strategi yang kompleks (Khan et al., 2024). Kegiatan kriminal ini biasanya melibatkan sekelompok individu atau organisasi yang memiliki struktur hierarkis, memperkuat kemampuan mereka untuk menghindari penegakan hukum di berbagai negara.

Kedua, karakter lintas batas menempatkan kejahatan ini dalam konteks yang lebih luas, di mana aktivitas ilegal terjadi di beberapa negara sekaligus. Contoh kasus adalah kejahatan siber, di mana semakin banyak transaksi finansial berpindah ke platform daring,

memungkinkan pelaku berpindah dari satu yurisdiksi ke yurisdiksi lain tanpa hambatan yang signifikan. Hal ini turut menambah kompleksitas dalam upaya penegakan hukum.

Motif ekonomi menjadi pendorong utama pelaku kejahatan transnasional, di mana keuntungan finansial menjadi fokus utama. Penelitian oleh Popko dan Popko menegaskan bahwa penghasilan dari kejahatan transnasional seringkali sangat besar, menciptakan insentif bagi kelompok kriminal untuk terus melakukan aktivitas ilegal (Popko & Popko, 2021). Kejahatan seperti pencucian uang, penipuan, dan korupsi dapat terjadi karena celah hukum yang ada di berbagai negara, di mana regulasi yang berbeda memungkinkan terjadinya eksploitasi.

Pakar hukum internasional juga mengamati evolusi kejahatan ini. Khususnya, Khan et al. mencatat bahwa selama dua dekade terakhir, terjadi perkembangan dramatis dalam bentuk dan metode kejahatan transnasional, di mana banyak dari kejahatan ini kini disusun berdasarkan kemajuan teknologi informasi (Khan et al., 2024). Ini mengharuskan peradaban hukum internasional untuk menyesuaikan diri dengan realitas baru ini, termasuk penerapan hukum berbasis teknologi dan penyelidikan forensik digital yang semakin penting (Khan et al., 2024).

2.3 Teori Hukum Pidana dan Yurisdiksi Siber

2.3.1 Teori Hukum Pidana dan Yurisdiksi Siber

Dalam konteks hukum pidana, yurisdiksi merujuk pada kewenangan suatu negara untuk menetapkan dan menerapkan hukum pidana yang berlaku di wilayahnya. Yurisdiksi ini dapat dibagi dalam beberapa asas, seperti asas teritorial, nasionalitas aktif, nasionalitas pasif, universal, dan perlindungan. Asas teritorial mengacu pada penerapan hukum pidana kepada setiap tindakan kriminal yang terjadi dalam batas wilayah suatu negara, tanpa mempedulikan kewarganegaraan pelaku atau korbannya. Hal ini merupakan asas yang paling umum diterapkan dalam hukum pidana, di mana hukum negara berlaku bagi kejahatan yang dilakukan di dalam wilayahnya, seperti tertuang dalam Pasal 2 KUHP Indonesia yang menyatakan bahwa "Hukum pidana yang berlaku di Indonesia adalah hukum pidana yang dikenal sebagai hukum positif nasional".

Asas nasionalitas aktif memberikan yurisdiksi kepada negara untuk mengadili warganya sendiri atas kejahatan yang dilakukan di luar wilayahnya. Contohnya, jika seorang warga negara Indonesia melakukan tindak pidana kejahatan di luar negeri, negara Indonesia berhak untuk mengadili berdasarkan hukum yang berlaku di dalam negeri. Sedangkan asas nasionalitas pasif mengizinkan suatu negara untuk mengadili pelaku yang melakukan kejahatan terhadap warganya di negara lain. Misalnya, jika seorang warga negara Indonesia menjadi korban tindak pidana kejahatan di luar negeri, negara Indonesia dapat campur tangan dengan menyelidiki dan meminta pertanggungjawaban pelaku secara hukum berdasarkan hukum Indonesia (Indriati, 2009).

Asas universal berlaku untuk kejahatan tertentu yang dianggap sangat serius, seperti kejahatan terhadap kemanusiaan, pencucian uang, dan terorisme. Dalam hal ini, setiap negara berhak melakukan penuntutan tanpa memandang asal pelaku, lokasi, atau korbannya. Penerapan asas ini berkontribusi pada upaya internasional untuk melawan kejahatan global dan memperkuat kerjasama antarnegara dalam bidang hukum (Yoserwan, 2023).

2.3.2 Tantangan Penerapan Asas Teritorialitas

Dalam dunia maya, lokasi fisik dari server dan pelaku sering kali sulit ditentukan, sehingga tindakan kriminal yang dilakukan dalam ruang siber dapat melintasi batas-batas

negara tanpa terlihat. Sebagai contoh, pencurian data atau penipuan daring dapat dilakukan oleh pelaku yang berada di satu negara, sementara korbannya ada di negara lain, dan server yang digunakan dapat dihosting di negara ketiga. Hal ini menciptakan kesulitan nyata bagi penegakan hukum untuk menemukan akses yurisdiksi yang tepat.

Di samping itu, ketidakpastian mengenai kapan dan di mana kejahatan sebenarnya terjadi menyebabkan tumpang tindih yurisdiksi, sehingga dapat memicu konflik hukum antara negara-negara yang berbeda dalam menangani kasus kejahatan siber. Misalnya, serangan DDoS (Distributed Denial of Service) dapat dilakukan dari beberapa lokasi di seluruh dunia sekaligus, menyulitkan negara-negara untuk menentukan siapa yang seharusnya memiliki yurisdiksi atas kasus tersebut (Djanggih & Qamar, 2018).

2.3.3 Teori Ubiquity dan Teori Dampak

Beberapa teori telah dikembangkan untuk membantu menentukan yurisdiksi dalam kasus yang melibatkan kejahatan di ruang siber. Teori ubiquity berargumen bahwa kejahatan dapat diadili di mana saja, dan setiap negara memiliki hak untuk mengadili pelanggaran yang terjadi dalam ruang sibernya, terlepas dari lokasi fisik pelakunya (Djanggih & Qamar, 2018). Dengan kata lain, jika suatu tindakan ilegal berdampak pada pengguna di negara tersebut, negara itu memiliki hak untuk menerapkan hukum pidana, terlepas dari lokasi pelaku.

Selanjutnya, teori dampak (effects doctrine) menyatakan bahwa negara memiliki yurisdiksi jika tindakan pelanggaran yang dilakukan memiliki dampak nyata di wilayahnya. Sebagai contoh, jika seorang pelaku kejahatan siber di luar negeri meninggalkan jejak yang menyebabkan kerugian bagi individu atau bisnis di dalam negeri, negara tersebut berhak untuk menerapkan hukum (Hiariej, 2020). Teori ini menjadi relevan terutama dalam konteks teknologi digital yang canggih, karena dapat memvalidasi tanggung jawab pelaku meskipun mereka beroperasi dari negara lain.

2.3.4 Pengaruh Teori dalam Penegakan Yurisdiksi

Kedua teori ini menjadi krusial dalam menentukan yurisdiksi pengadilan, terutama ketika berhadapan dengan kejahatan yang ada di ruang siber. Penegakan hukum terhadap kejahatan siber menjadi semakin rumit ketika mempertimbangkan kerangka hukum yang ada saat ini, seperti perjanjian internasional dan kerjasama bilateral dalam penegakan hukum. Sebagai contoh, Mutual Legal Assistance Treaties (MLATs) berfungsi sebagai instrumen untuk memfasilitasi kerjasama hukum antarnegara dalam penyelidikan dan peradilan kasus kejahatan transnasional (Indriati, 2009). Dengan adanya perjanjian ini, diharapkan dapat menciptakan sinergi dalam menangani kasus-kasus kejahatan lintas batas yang melibatkan teknologi digital.

2.4 Kerangka Hukum Terkait dalam Penanganan Kejahatan Ekonomi Transnasional

Dalam konteks penanganan kejahatan ekonomi transnasional, terdapat dua aspek utama dalam kerangka hukum: Hukum Pidana Materiil dan Hukum Pidana Formil. Keduanya memiliki peranan penting dalam mengatur dan memberikan sanksi terhadap tindakan kriminal yang dilakukan, terutama yang berkaitan dengan kejahatan siber dan kejahatan lintas batas.

Hukum Pidana Materiil

Hukum Pidana Materiil mencakup ketentuan-ketentuan dalam Kitab Undang-Undang Hukum Pidana (KUHP) Indonesia serta regulasi yang lebih spesifik, seperti UU No 8 Tahun 2010 tentang Tindak Pidana Pencucian Uang (TPPU).

Pasal-pasal dalam KUHP memberikan dasar hukum bagi penegakan hukum terhadap kejahatan, dengan jelas mendefinisikan berbagai jenis tindak pidana dan menetapkan hukuman yang sesuai. Khususnya, UU TPPU dirancang untuk memberantas praktik pencucian uang, yang sering kali terkait dengan aktivitas kejahatan terorganisir dan kejahatan ekonomi transnasional lainnya.

Sementara itu, Undang-Undang ITE (Informasi dan Transaksi Elektronik) memberikan kerangka hukum yang lebih spesifik untuk kasus-kasus kejahatan siber, termasuk penipuan elektronik, pencurian identitas, dan penyalahgunaan data pribadi.

Hukum Pidana Formil

Hukum Pidana Formil berkaitan dengan prosedur dan alat bukti yang digunakan dalam penegakan hukum. Sesuai dengan ketentuan yang diatur dalam UU ITE, yang mencakup pasal-pasal tentang validitas dan keabsahan alat bukti elektronik, peradilan kini memiliki praktik yang lebih modern dan memperhitungkan elemen digital dari kejahatan. Misalnya, kehadiran e-mail, dokumen digital, dan rekaman digital sebagai alat bukti kini diakui dan dapat diterima di pengadilan.

Kerja Sama Internasional

Mekanisme Mutual Legal Assistance (MLA) dan ekstradisi menjadi alat penting dalam upaya penegakan hukum tindak pidana kejahatan lintas batas negara. MLA adalah perjanjian antarnegara yang memungkinkan pertukaran bukti dan data yang diperlukan untuk penyelidikan hukum. Dalam konteks Budapest Convention on Cybercrime, yang merupakan perjanjian internasional pertama yang mengatur kejahatan siber, telah ada upaya untuk mendorong kerja sama memberantas kejahatan tersebut secara lebih efektif di tingkat internasional.. Ekstradisi juga memainkan peran penting ketika pelaku kejahatan berada di negara lain; tanpa adanya ekstradisi, pelaku seringkali dapat menghindari hukum.

2.5 Konsep Dasar Forensik Siber

2.5.1 Definisi, Tujuan, dan Prinsip-Prinsip Forensik Siber

Forensik siber adalah cabang ilmu forensik yang mentitikberatkan pada pengumpulan, analisa, dan penyajian bukti digital dalam konteks yuridis. Definisinya mencakup prosedur teknis dan metode ilmiah yang diterapkan untuk menyelidiki insiden yang melibatkan perangkat digital dan jaringan. Tujuan utama dari forensik siber adalah untuk mengidentifikasi, menjaga, menganalisis, dan menyajikan bukti dalam cara yang dapat diterima di pengadilan, sehingga memfasilitasi keadilan serta mendukung proses hukum (Alotaibi et al., 2022) (FFaizal & Luthfi, 2024).

Prinsip-prinsip forensik siber mencakup empat tahap utama:

1.Identifikasi: Proses mengenali jenis dan lokasi bukti digital yang relevan dalam suatu kasus.

2. Preservasi: Memastikan bahwa bukti yang ditemukan disimpan dengan aman, sehingga tidak mengalami perubahan atau kerusakan. Ini sering melibatkan penggunaan teknik yang menjamin integritas data, seperti membuat salinan 'forensically sound' (FFaizal & Luthfi, 2024).

3. Analisis: Melakukan analisis mendalam terhadap bukti yang telah disimpan untuk menemukan informasi yang relevan dan menggali setiap detail yang dapat mendukung kasus. Analisis ini harus dilakukan menggunakan teknik yang telah diverifikasi dan mengikuti standar yang ada (Makura et al., 2021).

4. Presentasi: Menyajikan temuan dalam konteks yang jelas dan dapat dipahami dalam pengadilan, seringkali melalui laporan tertulis atau kesaksian ahli. Hasil analisis disampaikan dengan objektivitas dan akurasi untuk meningkatkan kredibilitas di depan hukum (Wilson-Kovacs & Wyatt, 2023).

2.5.2 Standar dan Metodologi

Standar internasional seperti ISO/IEC 27043:2015 memberikan kerangka kerja yang penting untuk forensik siber. Standar ini menetapkan prinsip-prinsip untuk menangani bukti digital, termasuk prosedur untuk identifikasi, pengumpulan, dan pelestarian bukti. Ini bertujuan untuk meningkatkan kesiapsiagaan forensik dan meminimalkan risiko kerusakan data sebelum terjadi insiden (FFaizal & Luthfi, 2024). Misalnya, standar ini menjadi panduan bagi penyelidik untuk mengikuti langkah-langkah yang terstruktur dalam melakukan investigasi digital yang efektif dan efisien.

Metodologi yang diusulkan di dalam standar ini juga menyertakan panduan untuk menjamin keamanan proses pengolahan dan pelaporan bukti, memastikan bahwa semua langkah konsisten dan dapat diulang oleh penyelidik mana pun di masa mendatang (Wilson-Kovacs & Wyatt, 2023). Ini sangat penting agar investigasi dapat diaudit dan hasilnya dapat diterima di pengadilan.

2.5.3 Posisi Hasil Forensik Siber sebagai Alat Bukti

Hasil dari forensik siber memiliki posisi krusial sebagai alat bukti dalam hukum acara pidana. Dalam konteks hukum, bukti digital dapat dikategorikan sebagai alat bukti petunjuk atau alat bukti ahli. Alat bukti petunjuk mengacu pada informasi yang dapat memberikan petunjuk tentang kejahatan atau pelaku, sementara alat bukti ahli melibatkan testimoni dari penyelidik forensik atau ahli yang menjelaskan dan memvalidasi proses serta hasil analisis yang dilakukan.

Hasil forensik juga harus memenuhi kriteria untuk diterima sebagai bukti di pengadilan. Ini mencakup ketepatan, relevansi, dan keandalan dari teknik yang digunakan untuk mengumpulkan, memvalidasi dan menganalisis bukti digital. Dalam beberapa kasus, pengadilan memerlukan ahli forensik untuk memberikan penjelasan yang memungkinkan majelis hakim atau juri untuk memahami metode yang digunakan dan mendukung kredibilitas dari hasil investigasi yang disajikan

Dalam sistem hukum yang berlaku, penting bagi praktisi forensik untuk mengikuti perkembangan standar dan praktik terbaik agar bukti yang disajikan tetap relevan dan dapat dipertanggungjawabkan secara hukum. Dengan demikian, forensik siber bukan hanya tugas teknis tetapi juga harus dilakukan dengan pemahaman yang kuat tentang konteks hukum yang relevan, termasuk persyaratan seringkali ketat yang ditetapkan oleh pengadilan (Kurii & Opirskyy, 2023).

METODE PENELITIAN

Penelitian ini bersifat yuridis normatif yang menganalisis norma, prinsip, dan doktrin hukum terkait isu penelitian. Untuk kelengkapan analisis, digunakan empat pendekatan: perundang undangan untuk menilai kesesuaian dan harmonisasi regulasi; kasus melalui kajian putusan dan perkara penting guna melihat penerapan norma; komparatif untuk membandingkan ketentuan Indonesia dengan sistem hukum negara lain serta standar internasional; dan konseptual untuk mendalami doktrin serta konsep sebagai landasan teoretis norma.

Sumber bahan hukum dibagi tiga: primer (UUD 1945, KUHP, KUHAP, UU ITE, UU TPPU, UU KIP, dan konvensi internasional relevan); sekunder (jurnal ilmiah nasional

dan internasional, buku, disertasi, penelitian terdahulu, artikel investigatif media); dan tersier (kamus dan ensiklopedia hukum, glosarium teknis siber). Bahan sekunder dan tersier memperkaya penjelasan atas bahan primer serta memberi definisi dan pemahaman istilah yang jelas.

Pengumpulan dilakukan melalui studi kepustakaan dengan tahapan inventarisasi, identifikasi, dan klasifikasi bahan relevan. Analisis dilakukan secara kualitatif menggunakan penalaran hukum serta tiga teknik penafsiran: gramatikal (arti harfiah), sistematis (keterkaitan antar norma), dan teleologis (ratio legis/tujuan). Pendekatan ini diarahkan untuk menyusun argumen yang sistematis, logis, dan koheren dalam menjawab pertanyaan penelitian.

HASIL DAN PEMBAHASAN

Dalam era digital saat ini, modus kejahatan ekonomi telah berevolusi seiring dengan kemajuan teknologi. Dalam analisis ini, akan dibahas dua studi kasus utama, yaitu pencucian uang melalui aset kripto dan skema Business Email Compromise (BEC).

4.1 Studi Kasus 1: Pencucian Uang (Money Laundry) melalui Aset Kripto

Pencucian uang dengan aset kripto telah menjadi salah satu modus operandi kejahatan yang signifikan dalam beberapa tahun terakhir. Salah satu teknik utama yang digunakan oleh pelaku ialah chain hopping. Chain hopping merujuk pada praktik berpindah dari satu blockchain ke blockchain lain untuk mengaburkan jejak transaksi keuangan. Dengan melakukannya, pelaku dapat memperumit proses pelacakan transaksi oleh pihak berwenang (Saputra et al., 2024). Tindakan ini sering dilakukan dengan berinteraksi dengan berbagai bursa kripto yang beroperasi di berbagai negara, beberapa di antaranya memiliki regulasi yang lemah dalam hal Know Your Customer (KYC) dan Anti-Money Laundering (AML).

Penggunaan mixers atau tumblers juga merupakan teknik populer dalam pencucian uang berbasis kripto. Mixers bertujuan untuk menggabungkan dana dari berbagai sumber dalam satu transaksi, untuk kemudian mendistribusikannya kembali ke alamat baru dengan cara yang sulit dilacak oleh penegak hukum. Hal ini pada gilirannya menciptakan kebingungan dan mengganggu upaya untuk mengidentifikasi asal usul dana.

Pelaku yang mengeksploitasi bursa kripto dengan regulasi yang longgar seringkali dapat melewati batasan yang ada pada KYC dan AML tanpa risiko yang signifikan. Bursa-bursa yang tidak menerapkan prosedur KYC dan AML yang ketat merupakan sasaran empuk bagi para pencuci uang. Mereka memanfaatkan ketidakpahaman atau keterbatasan pengetahuan para operator bursa mengenai aktivitas ilegal yang sedang berlangsung di platform mereka.

4.2 Studi Kasus 2: Skema Business Email Compromise (BEC)

Business Email Compromise (BEC) adalah skema penipuan yang melibatkan rekayasa sosial untuk menyamarkan identitas pelaku agar tampak seperti otoritas yang sah dalam perusahaan. Pelaku biasanya menggunakan teknik spoofing untuk mengubah alamat email agar terlihat dari sumber yang dapat dipercaya, seperti pimpinan atau mitra bisnis, untuk menipu karyawan agar mentransfer dana ke rekening yang telah ditentukan (Ramadhan et al., 2020). Teknik ini sangat merugikan, karena sering kali karyawan tidak mencurigai bahwa email tersebut adalah penipuan.

Proses alur transfer dana dalam kasus BEC dapat sangat kompleks, seringkali melibatkan beberapa negara sebelum akhirnya dana mencapai tujuannya. Para pelaku

dengan cermat merancang alur ini agar menyulitkan otoritas untuk melacak asal usul dana. Keterlibatan dalam transfer lintas negara ini sangat berpotensi menimbulkan tantangan bagi penegak hukum karena masalah yurisdiksi.

Skema BEC kerap kali melibatkan kolaborasi pelaku dengan individu yang berada di negara tujuan, menciptakan saluran yang terorganisir dan terencana dengan baik. Hal ini menunjukkan betapa beragam dan terjadinya transformasi metode kejahatan ekonomi di era digital ini (Pantow, 2025).

4.3 Analisis Kritis terhadap Kerangka Hukum Pidana Saat Ini

Analisis terhadap kerangka hukum pidana saat ini menunjukkan bahwa meskipun terdapat beberapa landasan hukum yang telah ada, masih ada banyak celah yang mengakibatkan kesulitan dalam penegakan hukum. Penelitian ini akan mengeksplorasi dua aspek utama dari kerangka hukum pidana: hukum materiil dan hukum formil.

4.3.1 Aspek Hukum Materiil

Kekosongan Hukum dalam Mendefinisikan Aset Virtual

Satu permasalahan utama dalam hukum materiil adalah kekosongan hukum (legal vacuum) yang terdapat dalam mendefinisikan aset virtual baru, seperti Non-Fungible Tokens (NFT), sebagai objek dalam Tindak Pidana Pencucian Uang (TPPU). Meskipun aset virtual semakin populer, peraturan yang ada tidak menjelaskan secara rinci mengenai aset-aset ini, sehingga menimbulkan kesulitan dalam menerapkan norma-norma hukum yang ada. Pengaturan NFT dan peruntukannya dalam konteks pencucian uang menjadi ambigu, karena tidak ada ketentuan hukum yang secara eksplisit mencakup karakteristik dan mekanisme fungsional dari aset ini.

Akibat kekosongan hukum ini, para pelaku kejahatan sering kali mengeksploitasi celah yang ada untuk melindungi aktivitas ilegal mereka. Dengan tidak adanya definisi yang jelas mengenai aset digital, penegak hukum menghadapi tantangan dalam mengidentifikasi transaksi mencurigakan yang melibatkan NFT. Misalnya, banyak transaksi NFT digunakan untuk membantu pencucian uang karena sifat anonimitas yang melekat pada teknologi blockchain. Hal ini menunjukkan perlunya segera ada pembaruan dalam regulasi yang ada untuk mencakup definisi aset virtual dan implikasinya dalam TPPU.

Kesulitan Perumusan Unsur "Kesalahan"

Aspek lain yang mengkhawatirkan adalah kesulitan dalam perumusan unsur "kesalahan" pada kejahatan yang melibatkan kecerdasan buatan (AI). Dalam konteks AI, penegakan hukum sering mengalami kebingungan mengenai siapa yang harus disalahkan untuk tindakan yang diambil oleh mesin. Dalam banyak kasus, sulit untuk menentukan apakah perilaku suatu sistem AI adalah akibat dari desain oleh manusia atau autonomi yang dihasilkannya. Dengan kata lain, apakah kesalahan tersebut ada di tingkat pengembang, pengguna, atau AI itu sendiri?

Situasi ini membuat penerapan prinsip-prinsip hukum pidana yang sudah ada menjadi sulit dan kompleks. Pertanyaan tentang tanggung jawab hukum menjadi lebih mendesak, terlebih ketika AI digunakan untuk tujuan ilegal. Oleh karena itu, diperlukan peninjauan kembali terhadap asas hukum yang ada agar dapat mengakomodasi skenario baru yang muncul akibat perkembangan teknologi ini.

4.3.2 Aspek Hukum Formil

Problematika Yurisdiksi

Satu tantangan utama dalam hukum formil berkaitan dengan yurisdiksi. Dalam kasus di mana server, pelaku, dan korbannya berada di negara yang berbeda, menentukan mana yang memiliki wewenang untuk mengadili kejahatan tersebut menjadi rumit. Hal ini bisa menyebabkan jurisdiksi tumpang tindih, di mana beberapa negara merasa memiliki hak untuk mengambil tindakan hukum, tetapi tidak ada yang benar-benar secara efektif dapat melaksanakannya.

Kondisi ini diperparah oleh praktik penegakan hukum yang berbeda-beda di tiap negara. Tanpa adanya kerjasama internasional yang baik, kasus di ranah siber sering kali dapat lolos dari penegakan hukum. Dengan situasi yang demikian, diperlukan mekanisme penegakan hukum internasional yang lebih solid untuk menangani kejahatan yang melibatkan pihak-pihak dari berbagai yurisdiksi yang berbeda.

Tantangan Pembuktian

Tantangan lain yang signifikan dalam kerangka hukum formil adalah masalah pembuktian. Bukti yang diperoleh dari yurisdiksi lain tidak selalu dapat diterima di pengadilan karena kesulitan dalam membuktikan legalitas dan keaslian dari alat bukti tersebut. Misalnya, ketidakpastian tentang chain of custody digital dapat membahayakan validitas bukti digital saat dibawa ke pengadilan. Proses mengamankan dan melacak perangkat keras (hardware) dan perangkat lunak (software) sangat penting untuk memastikan bahwa bukti tidak mengalami perubahan atau manipulasi sebelum digunakan dalam kasus hukum.

Selain itu, volatilitas data yang melekat pada banyak bentuk bukti digital dapat membuat penegakan hukum menjadi sulit. Data yang bisa berubah atau hilang seiring berjalannya waktu mengakibatkan perhatian yang lebih terhadap cara bagaimana data tersebut dikumpulkan dan disimpan. Oleh karena itu, penting untuk memiliki prosedur yang jelas dalam pengumpulan dan penyimpanan bukti digital agar dapat diterima dalam hukum.

4.3.3 Perbandingan Internasional

Dalam konteks penyelesaian isu terkait yurisdiksi dan akses data, pendekatan internasional sering dipertimbangkan. Amerika Serikat, misalnya, telah mengadopsi Clarifying Lawful Overseas Use of Data Act (CLOUD Act) yang memberikan kerangka hukum untuk aktivitas pengumpulan dan pemanfaatan data yang melibatkan entitas di luar negeri. Undang-undang ini memperbolehkan otoritas penegak hukum untuk mengakses data yang disimpan di luar negeri di bawah ketentuan tertentu, mengatasi beberapa isu yurisdiksi yang dihadapi saat ini.

Sementara itu, Uni Eropa melalui General Data Protection Regulation (GDPR) memberikan kerangka yang ketat dalam hal perlindungan data pribadi, tetapi juga menyajikan peraturan mengenai transfer data internasional. GDPR tidak hanya memberikan hak kepada individu atas data mereka tetapi juga memberikan kejelasan mengenai hukum yang berlaku ketika data diolah di luar Eropa. Dengan demikian, terdapat sebuah model yang bisa dipelajari untuk meningkatkan kerjasama dan penegakan hukum lintas negara dalam menghadapi tantangan yang dihadapi oleh negara-negara di seluruh dunia terhadap kejahatan siber.

4.4 Optimalisasi Peran Forensik Siber dalam Penegakan Hukum

Optimalisasi forensik siber dalam penegakan hukum adalah aspek yang sangat penting untuk meningkatkan efektivitas penyelidikan dan penegakan hukum terhadap kejahatan digital. Dalam kajian ini, akan dibahas beberapa teknik investigasi digital, bagaimana mengintegrasikan hasil forensik ke dalam Berita Acara Pemeriksaan (BAP), serta analisis kasus untuk memahami keberhasilan dan tantangan yang dihadapi oleh forensik siber.

4.4.1Teknik Investigasi Digital

1. Network Forensics: Teknik ini mencakup pengumpulan dan analisis data dari jaringan untuk menyelidiki insiden keamanan. Network forensics membantu dalam melacak aktivitas mencurigakan, menganalisis pola penggunaan, dan mengidentifikasi pelanggaran keamanan dengan memeriksa log aktivitas jaringan (Qureshi et al., 2021). Dengan menggunakan metode yang tepat, penyelidik dapat menemukan jejak pelaku kejahatan siber, termasuk analisis packet capture untuk mengidentifikasi komunikasi yang terjadi selama insiden.

2. Malware Analysis: Teknik ini melibatkan studi tentang perangkat lunak berbahaya (malware) untuk memahami cara kerjanya, bagaimana penyebarannya, dan potensi kerusakannya. Melalui analisis statis dan dinamis, penyelidik dapat mengidentifikasi perilaku malware, memberi mereka wawasan tentang siapa yang mungkin berada di belakang serangan dan bagaimana cara menghindarinya di masa depan (Al-Dhaqm et al., 2021). Dengan informasi yang tepat, penyelidikan dapat memberikan bukti yang kuat dalam pengadilan.

3. Blockchain Analysis: Teknik ini sangat berguna dalam menangani kejahatan yang melibatkan cryptocurrency. Analisis blockchain memungkinkan penyelidik untuk melacak dan mengidentifikasi transaksi serta pemilik wallet coin dengan cara yang transparan. Metode ini sangat penting dalam kasus pencucian uang dan kejahatan finansial lainnya, di mana banyak transaksi dilakukan secara anonim namun tetap dapat dipantau dalam rantai transaksi yang ada (Albrecht et al., 2019; Ruiz & Angelis, 2021). Analisis juga mencakup penggunaan alat seperti Chainalysis untuk mengidentifikasi pola transaksi yang mencurigakan.

4.4.2 Integrasi Hasil Forensik ke dalam Berita Acara Pemeriksaan (BAP)

Integrasi hasil forensik ke dalam Berita Acara Pemeriksaan (BAP) adalah langkah krusial untuk memastikan bahwa hasil penyelidikan dapat diterima di pengadilan. Langkah pertama adalah menerjemahkan temuan teknis yang kompleks ke dalam bahasa yang dapat dipahami oleh hakim serta pihak-pihak lain yang terlibat dalam proses hukum. Hal ini memerlukan pengetahuan mendalam tentang aspek hukum yang relevan dan kemampuan untuk menjelaskan informasi teknis dengan jelas.

Penyelidik forensik harus dapat mendokumentasikan temuan mereka dalam format yang sesuai, menjelaskan teknik yang digunakan, serta interpretasi data yang ditemukan. Menyusun laporan yang rinci dan terstruktur dapat membantu mengurangi kebingungan dan memberikan gambaran yang jelas mengenai proses investigasi, sehingga hasil forensik dapat diterima sebagai bukti yang sah (Alansari, 2023; Canhoto, 2021).

4.4.3 Studi Kasus Penerapan Forensik Siber

Analisis studi kasus penerapan forensik siber menunjukkan peningkatan keberhasilan dalam penggunaan bukti forensik yang telah menghasilkan putusan yang menguntungkan bagi penegakan hukum. Misalnya, dalam kasus pencucian uang melalui cryptocurrency, bukti yang diperoleh dari analisis blockchain dan penyelidikan yang mendalam terhadap jaringan transaksi telah menyebabkan penangkapan sejumlah tersangka dan pemulihan dana yang hilang (Albrecht et al., 2019; Wronka, 2021). Namun, ada juga kegagalan yang terjadi, terutama ketika bukti tidak disiapkan dengan benar, atau ketika pihak-pihak tertentu tidak mengizinkan akses ke data penting yang dibutuhkan untuk analisis.

Penting juga untuk dicatat bahwa keberhasilan tidak hanya bergantung pada keakuratan teknik forensik tetapi juga pada integrasi hasil tersebut ke dalam sistem hukum yang ada dan bagaimana bukti tersebut dapat diterima di pengadilan. Pada kasus lain, ketika bukti tidak jelas atau tidak bisa diverifikasi melalui metode yang sah, keputusan pengadilan bisa mengakibatkan kegagalan dalam penuntutan (Gyamfi, 2022; Nanyun & Nasiri, 2020).

4.4.4 Tantangan Forensik

Meskipun terdapat kemajuan dalam teknik forensik siber, beberapa tantangan masih ada yang perlu diatasi:

1. Biaya Tinggi: Investigasi forensik sering kali memerlukan investasi yang besar dalam hal hardware dan software, serta SDM yang terampil. Biaya ini dapat membatasi kapasitas lembaga penegak hukum, terutama di negara-negara dengan sumber daya terbatas.

2. Kebutuhan SDM Ahli: Terdapat kekurangan tenaga ahli yang terlatih dalam bidang forensik siber. Untuk mengatasi tantangan ini, diperlukan upaya untuk meningkatkan pendidikan dan pelatihan di bidang forensik siber untuk menciptakan lebih banyak profesional yang kompeten (Qureshi et al., 2021).

3. Teknik Anti-Forensik: Pelaku kejahatan kini sering menggunakan metode anti-forensik seperti enkripsi dan steganografi untuk mengaburkan jejak mereka dan melindungi diri dari analisis forensik. Teknik-teknik ini merupakan tantangan besar bagi penegak hukum yang berusaha mengumpulkan bukti yang sah dan dapat diterima di pengadilan.

KESIMPULAN

Transformasi kejahatan ekonomi ke ranah digital yang sangat pesat telah mengubah tidak hanya modus operandi kejahatan, tetapi juga menantang pilar-pilar fundamental hukum pidana, yaitu yurisdiksi, pembuktian, dan pertanggungjawaban pidana. Kejahatan digital membawa dampak besar bagi struktur hukum yang ada, di mana ancaman baru muncul dengan cepat dan kompleks. Hal ini menuntut perhatian serius dari pembuat kebijakan dan penegak hukum untuk merespons perubahan ini secara efektif.

Pertama, dengan beragamnya teknik dan metode yang digunakan oleh pelaku kejahatan siber, yurisdiksi menjadi semakin kabur dan sulit diterapkan. Forensik siber, yang sebelum ini hanya dipandang sebagai alat bantu, kini telah dinyatakan sebagai komponen inti dalam upaya penegakan hukum. Analisis teknis yang dihasilkan dapat membimbing proses penyelidikan dan memberikan bukti yang valid di pengadilan. Namun, masuknya bukti digital dalam ruang lingkup hukum juga memunculkan

tantangan baru terkait dengan kesulitan dalam pembuktian dan integrasi hasil forensik ke dalam Berita Acara Pemeriksaan (BAP).

Kedua, terdapat kesenjangan (gap) yang signifikan antara kecepatan inovasi kejahatan teknologi dan lambatnya adaptasi kerangka hukum serta kapasitas penegak hukum. Di banyak negara, kerangka hukum yang ada belum mencakup semua aspek kejahatan baru yang muncul dari kemajuan teknologi. Kesulitan dalam menghasilkan regulasi yang relevan serta kekurangan SDM yang ahli di bidang ini menghambat penegakan hukum yang efektif. Oleh karena itu, diperlukan kerjasama internasional untuk mencari solusi kolektif dalam menghadapi kejahatan yang melintasi batas-batas negara.

Dengan demikian, penting bagi sistem hukum untuk segera beradaptasi dan memperbarui peraturan yang ada agar selaras dengan perubahan yang diakibatkan oleh kejahatan digital. Investasi dalam forensik siber sebagai sarana penegakan hukum harus diprioritaskan, termasuk pelatihan sumber daya manusia dan pengembangan kapasitas teknis. Semua langkah ini diperlukan untuk menjaga integritas sistem hukum dan melindungi masyarakat dari ancaman kejahatan ekonomi transnasional di era digital ini.
Untuk mengatasi kejahatan ekonomi digital, legislator direkomendasikan untuk mengamandemen UU TPPU dan ITE agar secara eksplisit mencakup aset digital seperti cryptocurrency dan NFT, serta memperjelas yurisdiksi siber. Selain itu, perlu didorong ratifikasi protokol tambahan Budapest Convention untuk mempermudah kerja sama internasional dan akses bukti elektronik lintas batas.

Dari sisi operasional, aparat penegak hukum membutuhkan peningkatan anggaran dan pelatihan berkelanjutan di bidang investigasi siber dan forensik digital. Kerja sama internasional juga harus diperkuat melalui jalur informal, seperti police-to-police cooperation, untuk mempercepat pertukaran intelijen awal sebelum proses formal seperti Bantuan Hukum Timbal Balik (MLA).

Sementara itu, akademisi diharapkan dapat mengembangkan kajian interdisipliner yang memadukan ilmu hukum, teknologi informasi, dan ekonomi. Penelitian harus fokus pada dampak perubahan teknologi yang cepat untuk menghasilkan rekomendasi kebijakan yang holistik, relevan, dan aplikatif bagi praktik hukum.

DAFTAR REFERENSI

Alansari, I. (2023). A Detection and Investigation Model for the Capture and Analysis of Network Crimes. Engineering Technology & Applied Science Research, 13(5), 11871–11877. https://doi.org/10.48084/etasr.6316

Albrecht, C., Duffin, K. M., Hawkins, S. R., & Morales-Rocha, V. (2019). The Use of Cryptocurrencies in the Money Laundering Process. Journal of Money Laundering Control, 22(2), 210–216. https://doi.org/10.1108/jmlc-12-2017-0074

Al-Dhaqm, A., Ikuesan, R. A., Kebande, V. R., Razak, S. A., Grispos, G., Choo, K. R., Al-rimy, B. A. S., & Alsewari, A. A. (2021). Digital Forensics Subdomains: The State of the Art and Future Directions. Ieee Access, 9, 152476–152502. https://doi.org/10.1109/access.2021.3124262

Alotaibi, F., Al-Dhaqm, A., & Al-Otaibi, Y. D. (2022). A Novel Forensic Readiness Framework Applicable to the Drone Forensics Field. Computational Intelligence and Neuroscience, 2022, 1–13. https://doi.org/10.1155/2022/8002963

Andria, A. (2021). Forensik Digital Sistem Informasi Berbasis Web. Jami Jurnal Ahli Muda Indonesia, 2(2), 33–44. https://doi.org/10.46510/jami.v2i2.73

Canhoto, A. I. (2021). Leveraging Machine Learning in the Global Fight Against Money Laundering and Terrorism Financing: An Affordances Perspective. Journal of Business Research, 131, 441–452. https://doi.org/10.1016/j.jbusres.2020.10.012

Djanggih, H., & Qamar, N. (2018). Penerapan Teori-Teori Kriminologi Dalam Penanggulangan Kejahatan Siber (Cyber Crime). Pandecta Research Law Journal, 13(1), 10–23. https://doi.org/10.15294/pandecta.v13i1.14020

Faridi, M. K. (2019). Kejahatan Siber Dalam Bidang Perbankan. Cyber Security Dan Forensik Digital, 1(2), 57–61. https://doi.org/10.14421/csecurity.2018.1.2.1373

FFaizal, A., & Luthfi, A. (2024). Comparison Study of NIST SP 800-86 and ISO/IEC 27037 Standards as a Framework for Digital Forensic Evidence Analysis. Journal of Information Systems and Informatics, 6(2), 701–718. https://doi.org/10.51519/journalisi.v6i2.717

Gyamfi, L. O. (2022). Effective Ways of Carrying Out Network Autopsy. Advances in Multidisciplinary & Scientific Research Journal Publication, 1(1), 329–333. https://doi.org/10.22624/aims/crp-bk3-p52

Hiariej, E. O. (2020). Korupsi Di Sektor Swasta Dan Tanggung Jawab Pidana Korporasi. Masalah-Masalah Hukum, 49(4), 333–344. https://doi.org/10.14710/mmh.49.4.2020.333-344

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

Indriati, N. (2009). MUTUAL LEGAL ASSISTANCE TREATIES (MLATs) SEBAGAI INSTRUMEN PEMBERANTASAN KEJAHATAN INTERNASIONAL. Jurnal Dinamika Hukum, 9(2). https://doi.org/10.20884/1.jdh.2009.9.2.218

Jayanti, D. E. (2020). Analisis Forensik Digital Storage Pada Owncloud Drive. Jurnal Repositor, 2(8). https://doi.org/10.22219/repositor.v2i8.96

Julian, D., & Sutabri, T. (2023). Analisa Kinerja Aplikasi Digital Forensik Autopsy Untuk Pengembalian Data Menggunakan Metode NIST SP 800-86. Jurnal Informatika Terpadu, 9(2), 136–142. https://doi.org/10.54914/jit.v9i2.984

Khan, S. H., Zakir, M. H., Tayyab, A., & Ibrahim, S. (2024). The Role of International Law in Addressing Transnational Organized Crime. J. Asian Dev. Studies, 13(1), 283–294. https://doi.org/10.62345/jads.2024.13.1.24

Kurii, Y., & 0pirskyy, I. (2023). Iso 27001: Analysis of Changes and Compliance Features of the New Version of the Standard. Cybersecurity Education Science Technique, 3(19), 46–55. https://doi.org/10.28925/2663-4023.2023.19.4655

Makura, S. M., Venter, H. S., Kebande, V. R., Karie, N. M., Ikuesan, R. A., & Alawadi, S. (2021). Digital Forensic Readiness in Operational Cloud Leveraging <scp>ISO</Scp>/<scp>IEC</Scp> 27043 Guidelines on Security Monitoring. Security and Privacy, 4(3). https://doi.org/10.1002/spy2.149

Nanyun, N. M., & Nasiri, A. (2020). Role of FATF on Financial Systems of Countries: Successes and Challenges. Journal of Money Laundering Control, 24(2), 234–245. https://doi.org/10.1108/jmlc-06-2020-0070

Pantow, R. T. (2025). Tindak Pidana Penipuan Dalam Transaksi Online Sebagai Kejahatan Terorganisir Dan Kaitannya Dengan Pencucian Uang. Peshum, 4(3), 4604–4615. https://doi.org/10.56799/peshum.v4i3.8971

Popko, V., & Popko, Y. (2021). Theoretical and Legal Characteristics of Economic Crimes of a Transnational Nature. Baltic Journal of Economic Studies, 7(1), 93–101. https://doi.org/10.30525/2256-0742/2021-7-1-93-101

Qureshi, S., Li, J., Akhtar, F., Tunio, S., Khand, Z. H., & Wajahat, A. (2021). Analysis of Challenges in Modern Network Forensic Framework. Security and Communication Networks, 2021, 1–13. https://doi.org/10.1155/2021/8871230

Ramadhan, M., Ariyanti, D. O., & Ariyani, N. (2020). Pencurian E-Money Pada E-Commerce Dalam Tindak Pidana Cybercrime Sebagai Tindak Pidana Ekonomi. Reformasi Hukum, 24(2), 169–188. https://doi.org/10.46257/jrh.v24i2.179

Ramansyah, R., Prayudi, Y., & Riadi, I. (2021). Deteksi Bukti Digital Game Online Pada Platform Skyegrid Menggunakan Framework FRED. Jatisi (Jurnal Teknik Informatika Dan Sistem Informasi), 8(2), 794–804. https://doi.org/10.35957/jatisi.v8i2.793

Riadi, I., Sunardi, S., & Sahiruddin, S. (2019). Analisis Forensik Recovery Pada Smartphone Android Menggunakan Metode National Institute of Justice (NIJ). Jurnal Rekayasa Teknologi Informasi (Jurti), 3(1), 87. https://doi.org/10.30872/jurti.v3i1.2292

Ruiz, E. P., & Angelis, J. (2021). Combating Money Laundering With Machine Learning – Applicability of Supervised-Learning Algorithms at Cryptocurrency Exchanges. Journal of Money Laundering Control, 25(4), 766–778. https://doi.org/10.1108/jmlc-09-2021-0106

Saputra, A., Kristiawanto, K., & Ismed, M. (2024). Rekonstruksi Penegakan Hukum Tindak Pidana Siber Di Indonesia. Seikat Jurnal Ilmu Sosial Politik Dan Hukum, 3(1), 63–70. https://doi.org/10.55681/seikat.v3i1.1186

Sunardi, S., Riadi, I., & Akbar, Muh. H. (2020). Steganalisis Bukti Digital Pada Media Penyimpanan Menggunakan Metode Static Forensics. Jurnal Nasional Teknologi Dan Sistem Informasi, 6(1), 1–8. https://doi.org/10.25077/teknosi.v6i1.2020.1-8

Tennant, I. (2021). Fulfilling the Promise of Palermo? A Political History of the UN Convention Against Transnational Organized Crime. Journal of Illicit Economies and Development, 2(1), 53–71. https://doi.org/10.31389/jied.90

Wilson-Kovacs, D., & Wyatt, D. (2023). The Long Journey of Resistance Toward Acceptance: Understanding Digital Forensic Accreditation in England and Wales From a Social Science Perspective. Wiley Interdisciplinary Reviews Forensic Science, 6(1). https://doi.org/10.1002/wfs2.1501

Wronka, C. (2021). "Cyber-Laundering": The Change of Money Laundering in the Digital Age. Journal of Money Laundering Control, 25(2), 330–344. https://doi.org/10.1108/jmlc-04-2021-0035

Yoserwan, Y. (2023). Eksistensi Hukum Pidana Adat Dalam Hukum Pidana Nasional Setelah Pengesahan Kuhp Baru. Unes Law Review, 5(4), 1999–2013. https://doi.org/10.31933/unesrev.v5i4.577