Prosiding Seminar Nasional Ilmu Hukum
Volume. 1, Nomor. 2 Desember 2024
e-ISSN: 3064-6332; p-ISSN: 3089-0942, Hal 179-193
DOI: https://doi.org/10.62383/prosemnashuk.v1i2.39
Available online at: https://prosiding.appihi.or.id/index.php/PROSEMNASHUK

Pemanfaatan Digital Forensik dan Teknologi Informasi Dalam Proses Pembuktian Tindak Pidana Pemalsuan Dokumen Elektronik

Edwin Setiawan[1*], Hartiwiningsih[2]
[1,2]Magister Ilmu Hukum, Fakultas Hukum Universitas Sebelas Maret,Indonesia
E-mail : edwins.es14@gmail.com[1],hartiwiningsih@staff.uns.ac.id[2]*

Korespondensi Penulis: edwins.es14@gmail.com[*]

Abstract*. The rapid development of information technology has brought significant changes, particularly in the area of cybercrime, such as electronic document forgery. This research explores the role of digital forensics and information technology in proving electronic document forgery crimes in Indonesia, using a normative legal research approach. The study employs both a statute approach and a conceptual approach to analyze the effectiveness of digital forensics in uncovering electronic crimes. The findings show that while digital forensics plays a crucial role in investigating electronic document forgery, there are several complex challenges in its implementation. One of the major obstacles is the limited number of certified digital forensic experts in Indonesia, with only 147 professionals qualified in this field. Additionally, the existing legal regulations have not kept pace with the rapid advancements in digital technology, which poses significant challenges to enforcement efforts. The study identifies various technical barriers, such as the complexity of forensic technologies, the volatile nature of digital evidence, and the ever-evolving techniques used by cybercriminals. These factors complicate the process of proving electronic crimes and pose difficulties for investigators. In response to these challenges, the research recommends strategic measures such as strengthening the capacity of forensic laboratories, harmonizing legal regulations with technological advancements, and improving the competency of human resources in both technological and legal fields. The study contributes to the development of a conceptual framework for cyber law enforcement, providing a comprehensive perspective on the challenges faced in proving electronic crimes in the digital age. The research aims to inform policymakers in crafting more effective and adaptive law enforcement strategies.*

Keywords*: Cybercrime,Digital Forensics,Electronic Document Forgery,Evidence, Information Technology*

Abstrak. Perkembangan pesat teknologi informasi telah membawa perubahan signifikan, khususnya di bidang kejahatan dunia maya, seperti pemalsuan dokumen elektronik. Penelitian ini mengeksplorasi peran forensik digital dan teknologi informasi dalam membuktikan kejahatan pemalsuan dokumen elektronik di Indonesia, dengan menggunakan pendekatan penelitian hukum normatif. Penelitian ini menggunakan pendekatan perundang-undangan dan pendekatan konseptual untuk menganalisis efektivitas forensik digital dalam mengungkap kejahatan elektronik. Hasil penelitian menunjukkan bahwa meskipun forensik digital memainkan peran penting dalam penyelidikan pemalsuan dokumen elektronik, terdapat berbagai tantangan kompleks dalam pelaksanaannya. Salah satu kendala utama adalah terbatasnya jumlah ahli forensik digital yang bersertifikat di Indonesia, dengan hanya 147 profesional yang memenuhi kualifikasi di bidang ini. Selain itu, peraturan hukum yang ada belum sepenuhnya mengikuti perkembangan pesat teknologi digital, yang menjadi tantangan besar dalam upaya penegakan hukum. Penelitian ini mengidentifikasi berbagai hambatan teknis, seperti kompleksitas teknologi forensik, sifat digital evidence yang mudah berubah, dan teknik-teknik baru yang terus berkembang yang digunakan oleh para pelaku kejahatan dunia maya. Faktor-faktor ini mempersulit proses pembuktian kejahatan elektronik dan menyulitkan penyidik. Sebagai respons terhadap tantangan ini, penelitian ini merekomendasikan langkah-langkah strategis, seperti memperkuat kapasitas laboratorium forensik, menyelaraskan peraturan hukum dengan kemajuan teknologi, dan meningkatkan kompetensi sumber daya manusia di bidang teknologi dan hukum. Penelitian ini berkontribusi dalam pengembangan kerangka konseptual penegakan hukum dunia maya, memberikan perspektif komprehensif mengenai tantangan dalam membuktikan kejahatan elektronik di era digital. Penelitian ini bertujuan untuk memberikan dasar empiris bagi pembuat kebijakan dalam merancang strategi penegakan hukum yang lebih efektif dan adaptif.

Kata kunci*:* Alat Bukti,Forensik Digital,Kejahatan Siber,Pemalsuan Dokumen Elektronik,Teknologi Informasi

Received November 16, 2024; Received November 30, 2024; Accepted Desember 17, 2024; Published; Desember 31, 2024

1. LATAR BELAKANG

Perkembangan teknologi informasi dan komunikasi telah mengalami kemajuan yang sangat pesat dalam beberapa dekade terakhir. Kemajuan ini telah membawa perubahan signifikan dalam berbagai aspek kehidupan masyarakat, termasuk dalam cara berkomunikasi, berbisnis, dan berinteraksi sosial. Teknologi informasi dan komunikasi telah menjadi bagian yang tidak terpisahkan dari aktivitas sehari-hari masyarakat modern. Menurut data dari Asosiasi Penyelenggara Jasa Internet Indonesia (APJII), jumlah pengguna internet di Indonesia pada tahun 2020 mencapai 196,7 juta jiwa atau sekitar 73,7% dari total populasi Indonesia (APJII, 2023). Angka ini menunjukkan tingginya penetrasi internet di Indonesia dan besarnya peran teknologi informasi dalam kehidupan masyarakat.

Namun, di balik berbagai manfaat dan kemudahan yang ditawarkan oleh teknologi informasi, terdapat pula ancaman dan risiko yang perlu diwaspadai. Salah satu ancaman yang semakin marak terjadi adalah kejahatan siber *(cybercrime)* (Banjarnahor, 2023). Kejahatan siber merupakan tindak pidana yang dilakukan dengan menggunakan teknologi informasi dan komunikasi sebagai alat, sasaran, atau tempat terjadinya kejahatan. Berdasarkan data dari Direktorat Tindak Pidana Siber Bareskrim Polri, jumlah laporan kejahatan siber di Indonesia terus meningkat setiap tahunnya. Pada tahun 2020, terdapat 4.250 laporan kejahatan siber yang diterima oleh Polri, meningkat dari 3.411 laporan pada tahun 2019.

Salah satu bentuk kejahatan siber yang menjadi fokus dalam penelitian ini adalah tindak pidana pemalsuan dokumen elektronik. Dokumen elektronik merupakan salah satu jenis informasi elektronik yang memiliki kekuatan hukum dan dapat digunakan sebagai alat bukti yang sah di pengadilan. Hal ini diatur dalam Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) sebagaimana telah diubah dengan Undang-Undang Nomor 19 Tahun 2016. Pasal 1 angka 4 UU ITE mendefinisikan dokumen elektronik sebagai setiap informasi elektronik yang dibuat, diteruskan, dikirimkan, diterima, atau disimpan dalam bentuk analog, digital, elektromagnetik, optikal, atau sejenisnya, yang dapat dilihat, ditampilkan, dan/atau didengar melalui komputer atau sistem elektronik, termasuk tetapi tidak terbatas pada tulisan, suara, gambar, peta, rancangan, foto atau sejenisnya, huruf, tanda, angka, kode akses, simbol atau perforasi yang memiliki makna atau arti atau dapat dipahami oleh orang yang mampu memahaminya.

Pemalsuan dokumen elektronik dapat menimbulkan kerugian yang signifikan bagi individu, organisasi, maupun negara. Dalam konteks individu, pemalsuan dokumen elektronik dapat merugikan pihak-pihak yang terlibat dalam transaksi elektronik, seperti penjual dan pembeli dalam perdagangan elektronik *(e-commerce).* Pemalsuan dokumen transaksi, bukti

pembayaran, atau bukti pengiriman barang dapat menyebabkan kerugian finansial dan menurunkan kepercayaan konsumen terhadap transaksi elektronik. Dalam konteks organisasi, pemalsuan dokumen elektronik dapat merugikan perusahaan atau instansi yang menggunakan sistem elektronik dalam pengelolaan dokumen dan administrasi. Pemalsuan dokumen elektronik seperti surat kontrak, invoice, atau laporan keuangan dapat menyebabkan kerugian finansial, gangguan operasional, dan menurunkan reputasi organisasi. Dalam konteks negara, pemalsuan dokumen elektronik dapat merugikan institusi pemerintah dan mengganggu pelayanan publik. Pemalsuan dokumen elektronik seperti surat keputusan, sertifikat, atau dokumen perizinan dapat menyebabkan kerugian negara, menurunkan kepercayaan publik terhadap pemerintah, dan menghambat pembangunan nasional.

Mengingat besarnya dampak negatif yang dapat ditimbulkan oleh tindak pidana pemalsuan dokumen elektronik, penegakan hukum terhadap tindak pidana ini menjadi sangat penting. Namun, proses penegakan hukum terhadap tindak pidana pemalsuan dokumen elektronik seringkali menghadapi berbagai tantangan dan kendala. Salah satu tantangan utama adalah sulitnya mengungkap dan membuktikan tindak pidana pemalsuan dokumen elektronik secara hukum.

Berbeda dengan pemalsuan dokumen fisik yang dapat dideteksi melalui pemeriksaan fisik dokumen, pemalsuan dokumen elektronik seringkali sulit dideteksi secara kasat mata. Dokumen elektronik yang dipalsukan dapat terlihat sama persis dengan dokumen asli jika dilihat secara visual. Pemalsuan dokumen elektronik juga dapat dilakukan dengan menggunakan teknik-teknik canggih seperti teknik steganografi atau teknik anti-forensik yang dapat menyamarkan atau menghilangkan jejak digital dari aktivitas pemalsuan.

Untuk mengungkap dan membuktikan tindak pidana pemalsuan dokumen elektronik, diperlukan pendekatan yang berbeda dengan pembuktian tindak pidana konvensional. Salah satu pendekatan yang dapat digunakan adalah melalui pemanfaatan ilmu digital forensik. Digital forensik merupakan cabang ilmu forensik yang berkaitan dengan pemulihan dan investigasi materi (data) yang ditemukan pada perangkat digital. Dalam konteks tindak pidana pemalsuan dokumen elektronik, digital forensik berperan dalam mengidentifikasi, mengumpulkan, menganalisis, dan menyajikan bukti-bukti digital yang dapat mendukung proses penyidikan dan pembuktian di pengadilan.

Namun, pemanfaatan digital forensik dalam pembuktian tindak pidana pemalsuan dokumen elektronik juga menghadapi berbagai kendala dan tantangan. Salah satu kendala utama adalah terbatasnya sumber daya manusia yang memiliki kompetensi dan keahlian di bidang digital forensik. Berdasarkan data dari Asosiasi Forensik Digital Indonesia (AFDI),

hingga tahun 2021, jumlah ahli forensik digital yang tersertifikasi di Indonesia baru mencapai 147 orang. Jumlah ini masih sangat kurang jika dibandingkan dengan tingginya kasus kejahatan siber yang terjadi di Indonesia.

Kendala lainnya adalah terbatasnya sarana dan prasarana pendukung digital forensik, khususnya di daerah-daerah. Tidak semua kantor kepolisian atau kejaksaan memiliki laboratorium forensik digital yang memadai untuk melakukan pemeriksaan dan analisis barang bukti digital. Hal ini dapat menghambat proses penyidikan dan pembuktian tindak pidana pemalsuan dokumen elektronik, terutama untuk kasus-kasus yang terjadi di luar kota-kota besar.

Kendala berikutnya adalah cepatnya perkembangan teknologi informasi yang digunakan dalam aktivitas kejahatan siber, termasuk pemalsuan dokumen elektronik. Pelaku kejahatan siber seringkali menggunakan teknik-teknik canggih dan terus berinovasi untuk menghindari deteksi dan menyulitkan proses forensik digital. Hal ini menuntut aparat penegak hukum dan ahli forensik digital untuk terus mengikuti perkembangan teknologi dan meningkatkan kompetensi agar dapat mengungkap tindak pidana pemalsuan dokumen elektronik dengan lebih efektif.

Penelitian terdahulu telah mengkaji berbagai aspek terkait pembuktian tindak pidana siber dan pemanfaatan digital forensik. Penelitian oleh (Manurung & Krisnawati, 2022) membahas mengenai kedudukan alat bukti elektronik dalam sistem pembuktian perkara pidana di Indonesia. Hasil penelitian tersebut menunjukkan bahwa alat bukti elektronik merupakan perluasan dari alat bukti petunjuk berdasarkan KUHAP, namun setelah adanya UU ITE dan putusan MK, alat bukti elektronik diakui sebagai alat bukti yang sah jika bebas dari rekayasa dan dapat dipertanggungjawabkan keasliannya di persidangan.

Penelitian lain oleh Inda Pongantung, (Pongantung, Pangkerego, & Pinangkaan, 2021) membahas mengenai kedudukan alat bukti elektronik dalam pembuktian tindak pidana informasi dan transaksi elektronik berdasarkan UU ITE. Hasil penelitian tersebut menyimpulkan bahwa pembuktian tindak pidana informasi dan transaksi elektronik didasarkan pada alat bukti yang sah dalam Pasal 184 KUHAP serta ketentuan Pasal 5 UU ITE mengenai informasi dan dokumen elektronik sebagai alat bukti hukum yang sah. Alat bukti elektronik berupa informasi dan dokumen elektronik serta hasil cetakannya merupakan perluasan alat bukti yang sah dan memberikan kepastian hukum dalam pembuktian tindak pidana informasi dan transaksi elektronik.

Meskipun penelitian-penelitian sebelumnya telah memberikan pemahaman yang berharga mengenai pembuktian tindak pidana siber dan pemanfaatan digital forensik, masih

terdapat beberapa keterbatasan. Pertama, penelitian-penelitian tersebut belum secara spesifik mengkaji pemanfaatan digital forensik dalam konteks pembuktian tindak pidana pemalsuan dokumen elektronik. Kedua, penelitian-penelitian tersebut belum menganalisis secara komprehensif mengenai kendala-kendala yang dihadapi dalam pemanfaatan digital forensik untuk pembuktian tindak pidana pemalsuan dokumen elektronik. Ketiga, penelitian-penelitian tersebut belum memberikan rekomendasi yang konkret dan operasional untuk mengoptimalkan pemanfaatan digital forensik dalam penegakan hukum terhadap tindak pidana pemalsuan dokumen elektronik di Indonesia.

Penelitian ini bertujuan untuk mengisi celah pengetahuan tersebut dengan mengkaji secara mendalam tentang pemanfaatan digital forensik dan teknologi informasi dalam proses pembuktian tindak pidana pemalsuan dokumen elektronik di Indonesia. Secara khusus, penelitian ini akan menganalisis efektivitas pemanfaatan digital forensik dalam mengungkap dan membuktikan tindak pidana pemalsuan dokumen elektronik, mengidentifikasi kendala dan tantangan yang dihadapi dalam pemanfaatan digital forensik, serta merumuskan rekomendasi kebijakan untuk mengoptimalkan pemanfaatan digital forensik dalam penegakan hukum terhadap tindak pidana pemalsuan dokumen elektronik di Indonesia.

Penelitian ini diharapkan dapat memberikan kontribusi teoritis dan praktis bagi pengembangan ilmu hukum, khususnya di bidang hukum pidana siber dan digital forensik. Secara teoritis, penelitian ini diharapkan dapat memperkaya khazanah pengetahuan tentang pemanfaatan digital forensik dalam pembuktian tindak pidana siber, serta menjadi referensi bagi penelitian-penelitian selanjutnya yang relevan. Secara praktis, penelitian ini diharapkan dapat menjadi masukan bagi aparat penegak hukum, pembuat kebijakan, dan pemangku kepentingan lainnya dalam mengoptimalkan pemanfaatan digital forensik dan teknologi informasi untuk menegakkan hukum terhadap tindak pidana pemalsuan dokumen elektronik di Indonesia.

Berdasarkan latar belakang dan permasalahan yang telah diuraikan, penelitian ini memiliki signifikansi yang tinggi dalam upaya meningkatkan efektivitas penegakan hukum terhadap tindak pidana pemalsuan dokumen elektronik di Indonesia. Dengan mengkaji secara komprehensif mengenai pemanfaatan digital forensik dan teknologi informasi dalam proses pembuktian, penelitian ini diharapkan dapat memberikan solusi konkret untuk mengatasi kendala dan tantangan yang dihadapi, serta mendorong optimalisasi pemanfaatan teknologi dalam mendukung penegakan hukum yang adil, akuntabel, dan responsif terhadap perkembangan kejahatan siber di era digital.

2. METODE PENELITIAN

Bagian Penelitian ini merupakan penelitian hukum normatif yang mengkaji pengaturan hukum terkait tindak pidana pemalsuan dokumen elektronik dan pemanfaatan digital forensik dalam proses pembuktian. Menurut Soerjono Soekanto dan Sri Mamudji, penelitian hukum normatif adalah penelitian hukum yang dilakukan dengan cara meneliti bahan pustaka atau data sekunder belaka (Soekanto & Mamudji, 2021).

Pendekatan yang digunakan dalam penelitian ini meliputi pendekatan perundang-undangan (statute approach) dengan menelaah peraturan perundang-undangan yang relevan seperti Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) dan pendekatan konseptual (conceptual approach) yang mengkaji doktrin dan konsep hukum terkait tindak pidana siber, pembuktian, dan digital forensik. Hal ini sejalan dengan pandangan Peter Mahmud Marzuki yang menyatakan bahwa penelitian hukum dilakukan untuk menghasilkan argumentasi, teori atau konsep baru sebagai preskripsi dalam menyelesaikan masalah yang dihadapi (Marzuki, 2017).

Bahan hukum yang digunakan dalam penelitian ini terdiri dari tiga jenis, yaitu bahan hukum primer, bahan hukum sekunder, dan bahan hukum tersier. Bahan hukum primer merupakan bahan hukum yang bersifat autoritatif, artinya mempunyai otoritas (Marzuki, 2017). Bahan hukum primer dalam penelitian ini antara lain UU ITE, Undang-Undang Nomor 8 Tahun 1981 tentang Hukum Acara Pidana (KUHAP), dan putusan pengadilan terkait kasus pemalsuan dokumen elektronik.

Bahan hukum sekunder berupa semua publikasi tentang hukum yang bukan merupakan dokumen-dokumen resmi (Marzuki, 2017). Bahan hukum sekunder dalam penelitian ini meliputi buku-buku teks, artikel jurnal ilmiah, dan hasil penelitian yang relevan dengan topik penelitian. Sedangkan bahan hukum tersier adalah bahan yang memberikan petunjuk maupun penjelasan terhadap bahan hukum primer dan bahan hukum sekunder (Soekanto & Mamudji, 2021), seperti kamus hukum dan ensiklopedia hukum.

Teknik pengumpulan bahan hukum dalam penelitian ini dilakukan melalui studi kepustakaan dan studi dokumen. Studi kepustakaan dilakukan dengan cara mempelajari, mengidentifikasi, dan menganalisis bahan-bahan hukum yang relevan dengan permasalahan yang diteliti. Sedangkan studi dokumen dilakukan dengan cara mengkaji dan menganalisis dokumen-dokumen hukum yang berkaitan dengan permasalahan yang diteliti, seperti putusan pengadilan, surat dakwaan, atau dokumen-dokumen lainnya.

Setelah bahan-bahan hukum terkumpul, langkah selanjutnya adalah melakukan analisis terhadap bahan-bahan hukum tersebut. Dalam penelitian hukum normatif, analisis bahan hukum dilakukan secara kualitatif. Analisis kualitatif merupakan analisis yang tidak menggunakan angka atau rumus statistik, melainkan menggunakan penalaran hukum (*legal reasoning*) untuk memahami, menafsirkan, dan mengonstruksi bahan-bahan hukum yang ada (Marzuki, 2017).

3. HASIL DAN PEMBAHASAN

Optimalisasi Pemanfaatan Digital Forensik dan Teknologi Informasi dalam Proses Pembuktian Tindak Pidana Pemalsuan Dokumen Elektronik

Pemanfaatan digital forensik dan teknologi informasi memiliki peran yang sangat penting dalam proses pembuktian tindak pidana pemalsuan dokumen elektronik. Melalui pendekatan digital forensik yang terstruktur dan sistematis, bukti-bukti digital terkait pemalsuan dokumen elektronik dapat diungkap dan disajikan sebagai alat bukti yang sah di pengadilan. Hal ini sesuai dengan ketentuan dalam Pasal 5 ayat (1) UU ITE yang menyatakan bahwa informasi elektronik dan/atau dokumen elektronik dan/atau hasil cetaknya merupakan alat bukti hukum yang sah.

Secara lebih spesifik, tindak pidana pemalsuan dokumen elektronik diatur dalam Pasal 35 UU ITE, yang berbunyi:

"Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum melakukan manipulasi, penciptaan, perubahan, penghilangan, pengrusakan Informasi Elektronik dan/atau Dokumen Elektronik dengan tujuan agar Informasi Elektronik dan/atau Dokumen Elektronik tersebut dianggap seolah-olah data yang otentik."

Berdasarkan pasal tersebut, unsur-unsur tindak pidana pemalsuan dokumen elektronik meliputi:

1. Dilakukan dengan sengaja;
2. Tanpa hak atau melawan hukum;
3. Melakukan manipulasi, penciptaan, perubahan, penghilangan, atau pengrusakan informasi elektronik dan/atau dokumen elektronik;
4. Dengan tujuan agar informasi elektronik dan/atau dokumen elektronik tersebut dianggap seolah-olah data yang otentik.

Ancaman pidana bagi pelaku pemalsuan dokumen elektronik diatur dalam Pasal 51 ayat (1) UU ITE, yang menyatakan bahwa:

"Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 35 dipidana dengan pidana penjara paling lama 12 (dua belas) tahun dan/atau denda paling banyak Rp12.000.000.000,00 (dua belas miliar rupiah)."

Untuk mengungkap dan membuktikan tindak pidana pemalsuan dokumen elektronik yang memenuhi unsur-unsur tersebut, diperlukan pemanfaatan digital forensik. Proses digital forensik dalam kasus pemalsuan dokumen elektronik meliputi beberapa tahap, antara lain (Malian, 2024):

1. Identifikasi: melakukan pencarian dan pengumpulan barang bukti digital yang relevan, seperti komputer, smartphone, atau media penyimpanan lainnya yang diduga digunakan dalam pemalsuan.
2. Pelestarian: melakukan pengamanan dan pelestarian integritas barang bukti digital agar tidak rusak, hilang, atau berubah, misalnya dengan teknik imaging forensik atau hashing.
3. Analisis: melakukan pemeriksaan dan analisis mendalam terhadap barang bukti digital untuk menemukan bukti-bukti pemalsuan, seperti file dokumen yang dimanipulasi, log aktivitas, atau jejak digital lainnya.
4. Dokumentasi: melakukan pencatatan dan pelaporan seluruh temuan dan hasil analisis secara terstruktur dan sistematis untuk menjaga chain of custody.
5. Presentasi: menyajikan temuan dan hasil analisis forensik di depan pengadilan atau pihak yang berwenang secara jelas, objektif, dan sesuai aturan hukum.

Namun, pemanfaatan digital forensik dalam pembuktian tindak pidana pemalsuan dokumen elektronik masih menghadapi berbagai kendala. Salah satu kendala utama adalah terbatasnya sumber daya manusia yang kompeten di bidang digital forensik. Berdasarkan data dari Asosiasi Forensik Digital Indonesia (AFDI), hingga tahun 2021, jumlah ahli forensik digital tersertifikasi di Indonesia baru mencapai 147 orang (Asosiasi Forensik Digital Indonesia, 2021). Jumlah ini masih belum sebanding dengan tingginya kasus kejahatan siber yang ditangani.

Untuk mengatasi kendala tersebut, perlu dilakukan langkah-langkah untuk mengoptimalkan pemanfaatan digital forensik, di antaranya:

a. Peningkatan kuantitas dan kualitas SDM forensik digital, baik dari kalangan penegak hukum maupun ahli, melalui pendidikan, pelatihan, dan sertifikasi sesuai standar kompetensi nasional dan internasional.

b. Pengembangan sarana dan prasarana forensik digital yang memadai dan merata di seluruh wilayah, seperti pembangunan laboratorium forensik digital yang terakreditasi dan penyediaan alat-alat forensik yang mutakhir.
c. Penguatan regulasi dan kebijakan yang mendukung penerapan digital forensik, seperti pengaturan tentang standar dan prosedur forensik digital, pengakuan bukti digital sebagai alat bukti yang sah, serta perlindungan privasi dan keamanan data.
d. Peningkatan kerjasama dan kolaborasi antara aparat penegak hukum, ahli forensik, akademisi, dan industri teknologi dalam penelitian, pertukaran informasi, pelatihan bersama, dan pengembangan teknologi forensik digital.

Selain pemanfaatan digital forensik, optimalisasi pembuktian tindak pidana pemalsuan dokumen elektronik juga memerlukan dukungan teknologi informasi yang memadai. Teknologi informasi berperan penting dalam setiap tahapan penanganan perkara, mulai dari pelaporan, penyidikan, hingga persidangan.

Pada tahap pelaporan, ketersediaan sistem pelaporan elektronik (e-reporting) yang terintegrasi dapat memudahkan masyarakat untuk melaporkan dugaan tindak pidana pemalsuan dokumen elektronik. Laporan elektronik tersebut juga lebih mudah dikelola, diteruskan ke unit yang berwenang, dan diawasi progresnya.

Pada tahap penyidikan, sistem manajemen penyidikan berbasis teknologi informasi dapat membantu penyidik dalam mengelola berkas perkara secara digital, memonitor status perkara, dan berkoordinasi dengan pihak-pihak terkait seperti kejaksaan atau pengadilan. Sistem ini juga dapat terhubung dengan database alat bukti digital sehingga memudahkan penelusuran dan pengolahan bukti.

Pada tahap persidangan, penerapan sistem *e-court* yang mencakup *e-filing* (pengajuan dokumen secara elektronik), *e-payment* (pembayaran biaya perkara elektronik), dan *e-litigation* (persidangan elektronik) dapat meningkatkan efisiensi dan transparansi proses persidangan (Mahkamah Agung Republik Indonesia, 2019). Dokumen-dokumen elektronik terkait perkara, termasuk bukti digital hasil forensik, dapat disampaikan dan diperiksa secara elektronik tanpa harus mencetak atau membawanya secara fisik ke ruang sidang.

Namun demikian, pemanfaatan teknologi informasi dalam pembuktian tindak pidana pemalsuan dokumen elektronik juga perlu memperhatikan aspek keamanan siber. Sistem-sistem elektronik yang digunakan harus dijamin keamanan dan integritasnya dari potensi serangan siber yang dapat mengganggu proses penegakan hukum. Oleh karena itu, penegak hukum perlu bekerjasama dengan ahli keamanan siber untuk mengimplementasikan protokol keamanan yang memadai, seperti enkripsi, autentikasi multifaktor, atau audit trail.

Dengan mengoptimalkan pemanfaatan digital forensik dan teknologi informasi melalui langkah-langkah tersebut, diharapkan proses pembuktian tindak pidana pemalsuan dokumen elektronik dapat dilakukan secara lebih efektif, efisien, dan akuntabel. Hal ini sejalan dengan prinsip peradilan yang cepat, sederhana, dan biaya ringan sebagaimana diamanatkan dalam Pasal 2 ayat (4) Undang-Undang Nomor 48 Tahun 2009 tentang Kekuasaan Kehakiman.

Faktor Kendala dalam Pembuktian Tindak Pidana Pemalsuan Dokumen Elektronik

Meskipun pemanfaatan digital forensik dan teknologi informasi menawarkan banyak manfaat dalam pembuktian tindak pidana pemalsuan dokumen elektronik, namun dalam penerapannya masih menghadapi berbagai kendala. Kendala-kendala tersebut dapat dikategorikan menjadi kendala teknis, kendala sumber daya, dan kendala hukum.

Dari segi teknis, kendala yang dihadapi antara lain:

a. Keragaman dan kompleksitas teknologi yang digunakan dalam pemalsuan dokumen elektronik. Pelaku kejahatan dapat memanfaatkan berbagai teknik canggih seperti enkripsi, steganografi, atau anti-forensik untuk menyamarkan atau menghilangkan jejak digital (Yusoff, Dehghantanha, & Mahmod, 2017). Hal ini menyulitkan proses identifikasi dan analisis bukti digital.
b. Tingkat volatilitas dan kerapuhan bukti digital. Tidak seperti bukti fisik, bukti digital mudah berubah, rusak, atau hilang jika tidak ditangani dengan tepat (Shivdas, 2023). Kesalahan dalam proses akuisisi atau pelestarian bukti, seperti mematikan perangkat secara tidak benar, dapat merusak integritas bukti.
c. Keterbatasan alat dan infrastruktur forensik digital. Pemeriksaan forensik untuk kasus pemalsuan dokumen elektronik seringkali membutuhkan perangkat keras dan perangkat lunak khusus yang tidak selalu tersedia, terutama di daerah-daerah (Haris, Abdullah, Rizky, Indah, & others, 2024). Keterbatasan anggaran dan belum meratanya pembangunan laboratorium forensik digital menjadi tantangan.
d. Kesulitan dalam mengamankan dan menganalisis bukti digital dari layanan komputasi awan *(cloud computing).* Banyak dokumen elektronik yang kini disimpan atau diproses menggunakan layanan cloud dari penyedia asing, yang berada di luar yurisdiksi hukum Indonesia (Razaque, Aloqaily, Almiani, Jararweh, & Srivastava, 2021). Hal ini menimbulkan tantangan dalam mengakses dan mengamankan bukti digital dari server-server di luar negeri.

Dari segi sumber daya, kendala yang dihadapi meliputi:

a. Kurangnya kuantitas dan kualitas sumber daya manusia di bidang digital forensik. Sebagaimana dibahas sebelumnya, jumlah ahli forensik digital bersertifikat di Indonesia masih sangat terbatas dibandingkan volume kasus kejahatan siber yang ditangani (Santi, Nopalina, Mahendra, & Alfian, 2024). Keterbatasan SDM ini memperlambat proses pemeriksaan forensik.
b. Kesenjangan kompetensi antara penegak hukum dengan pelaku kejahatan dalam penguasaan teknologi. Pelaku kejahatan siber seringkali lebih mahir dan adaptif dalam menggunakan teknologi terbaru untuk melakukan pemalsuan dokumen elektronik (Sariani, 2024). Di sisi lain, tidak semua penegak hukum memiliki pemahaman yang memadai tentang aspek teknis kejahatan siber.
c. Terbatasnya program pendidikan dan pelatihan yang khusus dan mendalam di bidang digital forensik. Saat ini, hanya sedikit institusi pendidikan tinggi di Indonesia yang menawarkan program studi atau mata kuliah khusus tentang digital forensik (Sakti, 2025). Sebagian besar pelatihan forensik digital juga masih bersifat sporadis atau berjangka pendek.

Dari segi hukum, kendala yang dihadapi antara lain:

a. Keterbatasan pengaturan hukum yang spesifik tentang standar dan prosedur forensik digital. Meskipun UU ITE telah mengakui bukti elektronik, namun belum ada peraturan pelaksana yang secara rinci mengatur mengenai tata cara pengambilan, pengamanan, dan pemeriksaan bukti digital yang sesuai dengan standar forensik (Prayudi & SN, 2025). Hal ini dapat menimbulkan keraguan atau ketidakpastian hukum dalam penerapannya.
b. Belum adanya harmonisasi dan sinkronisasi antara hukum pidana materiil dan formil dalam mengakomodasi bukti elektronik. KUHP dan KUHAP sebagai pedoman utama dalam penegakan hukum pidana belum mengatur secara eksplisit mengenai alat bukti elektronik (Makarim, 2021). Hal ini dapat menimbulkan perbedaan perspektif atau bahkan resistensi dalam mengakui dan menilai alat bukti elektronik di persidangan.
c. Adanya celah hukum atau multi-interpretasi dalam ketentuan pembuktian perkara pidana yang melibatkan bukti elektronik. Misalnya, belum ada ketentuan yang jelas tentang kriteria atau syarat bukti elektronik agar dapat dinyatakan sah dan memiliki nilai pembuktian yang kuat (Ratmaja & Mertha, 2022). Bukti elektronik juga rentan dipersoalkan keotentikannya karena mudahnya bukti tersebut dimanipulasi.
d. Belum optimalnya kerjasama internasional dalam penanganan bukti elektronik lintas yurisdiksi. Seperti dijelaskan sebelumnya, tidak jarang bukti elektronik untuk kasus

pemalsuan dokumen elektronik berada di yurisdiksi negara lain (Purnama Santhi & Nuarta, 2023). Namun, tidak semua negara memiliki perjanjian kerjasama (*mutual legal assistance*) yang memadai untuk mengakses bukti elektronik lintas batas secara sah dan cepat.

Kendala-kendala tersebut perlu segera diatasi agar pemanfaatan digital forensik dan teknologi informasi dalam pembuktian tindak pidana pemalsuan dokumen elektronik dapat berjalan optimal. Upaya yang dapat dilakukan antara lain:

a. Penguatan kapasitas laboratorium forensik digital dan peningkatan kompetensi SDM forensik melalui pengadaan alat forensik yang mutakhir, pelaksanaan pendidikan dan pelatihan yang intensif, serta fasilitasi sertifikasi sesuai standar nasional dan internasional.
b. Percepatan pembentukan peraturan pelaksana UU ITE yang secara spesifik mengatur tentang prosedur dan standar forensik digital yang baku, harmonis dengan hukum pidana dan hukum acara pidana, serta adaptif dengan perkembangan teknologi dan modus kejahatan.
c. Perluasan dan pendalaman kerjasama antara penegak hukum dengan penyedia layanan komunikasi dan teknologi informasi, baik dalam negeri maupun luar negeri, untuk mempermudah proses pengamanan dan penyediaan alat bukti elektronik dengan tetap menghormati kedaulatan hukum dan perlindungan data pribadi.
d. Peningkatan literasi digital dan kesadaran hukum masyarakat, khususnya terkait aspek keamanan informasi dan dokumen elektronik, untuk mencegah dan melaporkan tindak pidana pemalsuan dokumen elektronik.

Dengan upaya-upaya tersebut, diharapkan pemanfaatan digital forensik dan teknologi informasi dapat menjadi solusi efektif dalam menekan angka dan dampak tindak pidana pemalsuan dokumen elektronik di Indonesia. Pembuktian yang didukung oleh temuan dan analisis forensik digital yang mumpuni, ditopang oleh aturan hukum yang akomodatif, dan dilaksanakan oleh penegak hukum yang kompeten, dapat memastikan agar keadilan dan kepastian hukum di ranah siber dapat ditegakkan.

Namun, upaya tersebut juga harus disertai dengan komitmen yang kuat dan tindakan nyata dari para pemangku kepentingan. Optimalisasi pemanfaatan digital forensik dan teknologi informasi tidak dapat dipisahkan dari agenda reformasi hukum dan birokrasi secara menyeluruh. Tanpa adanya daya dukung kelembagaan, anggaran, dan pengawasan yang memadai, maka langkah-langkah strategis yang direkomendasikan akan sulit terwujud.

Selain itu, pemanfaatan digital forensik dan teknologi informasi juga harus diimbangi dengan penghormatan terhadap hak-hak fundamental manusia, termasuk hak privasi, hak atas peradilan yang adil, dan hak untuk mendapatkan pembelaan hukum. Pembuktian dengan digital forensik tidak boleh dilakukan secara eksesif atau abusif sehingga justru kontraproduktif dengan tujuan penegakan hukum yang berkeadilan.

Sebagaimana ditegaskan dalam Pasal 28G ayat (1) UUD NRI Tahun 1945, "Setiap orang berhak atas perlindungan diri pribadi, keluarga, kehormatan, martabat, dan harta benda yang di bawah kekuasaannya, serta berhak atas rasa aman dan perlindungan dari ancaman ketakutan untuk berbuat atau tidak berbuat sesuatu yang merupakan hak asasi." Hak-hak tersebut harus tetap dihormati dan dilindungi dalam proses pembuktian perkara pidana, termasuk yang melibatkan bukti elektronik dan pemeriksaan forensik digital.

Pada akhirnya, efektivitas pemanfaatan digital forensik dan teknologi informasi dalam pembuktian tindak pidana pemalsuan dokumen elektronik akan sangat bergantung pada integritas, profesionalitas, dan koordinasi dari seluruh pihak yang terlibat. Penegak hukum, ahli forensik digital, akademisi, industri, hingga masyarakat harus bersinergi dan berkolaborasi untuk membangun ekosistem penegakan hukum siber yang tangguh, akuntabel, dan responsif di Indonesia.

KESIMPULAN DAN SARAN

Penelitian ini menyimpulkan bahwa pemanfaatan digital forensik dan teknologi informasi memiliki peran krusial dalam mengungkap dan membuktikan tindak pidana pemalsuan dokumen elektronik di Indonesia, namun masih terkendala aspek teknis, sumber daya, dan regulasi. Untuk mengoptimalkannya, diperlukan langkah-langkah strategis yang meliputi penguatan kapasitas forensik, kompetensi SDM, dukungan sarana-prasarana, harmonisasi regulasi, serta perluasan kerjasama antar stakeholder. Temuan dan rekomendasi penelitian ini diharapkan dapat menjadi landasan empiris bagi pengambil kebijakan untuk memperkuat pemanfaatan digital forensik dan teknologi informasi dalam pembuktian, serta menjadi rujukan bagi aparat penegak hukum dan masyarakat untuk meningkatkan kewaspadaan dan partisipasi dalam memerangi tindak pidana pemalsuan dokumen elektronik. Pada akhirnya, sinergi antara teknologi dan nilai-nilai keadilan diharapkan dapat menjadi pilar penegakan hukum siber yang profesional dan bermartabat di Indonesia.

DAFTAR REFERENSI

APJII. (2023). Survei APJII Pengguna Internet di Indonesia. Apjii.or.Id, (March).

Asosiasi Forensik Digital Indonesia. (2021). AFDI Certified Experts. Retrieved from http://afdi.or.id/afdi-certified-experts/

Banjarnahor, J. (2023). Penegakan Cyberlaw Di Indonesia Dalam Mengatasi Cybercrime. Juril AMIK MBP, (1).

Haris, O. K., Abdullah, S. A., Rizky, A., Indah, S. R., & others. (2024). Penggunaan Digital Forensik dalam Pembuktian Tindak Pidana Pencemaran Nama Baik di Media Sosial Berdasarkan UU ITE. Halu Oleo Legal Research, 6(2), 588–603.

Mahkamah Agung Republik Indonesia. (2019). PERMA 01 2019. Peraturan Mahkamah Agung Nomor 1 Tahun 2019, p. 18. Retrieved from https://ecourt.mahkamahagung.go.id/PERMA_01_2019.pdf

Makarim, E. (2021). Kerangka Kebijakan Dan Reformasi Hukum Untuk Kelancaran Perdagangan Secara Elektronik (E-Commerce) Di Indonesia. Jurnal Hukum & Pembangunan, 44(3). https://doi.org/10.21143/jhp.vol44.no3.25

Malian, D. (2024). Penanganan Dan Tantangan Cybercrime Di Era Digital Perspektif Kriminologi. Innovative: Journal Of Social Science Research, 4(6), 7048–7056.

Manurung, T. O., & Krisnawati, I. G. A. A. (2022). Kedudukan Alat Bukti Elektronik Dalam Sistem Pembuktian Perkara Pidana Di Indonesia. Jurnal Kertha Desa, 10(5), 371–381. Retrieved from https://ojs.unud.ac.id/index.php/kerthadesa/article/download/79114/44713

Marzuki, P. M. (2017). Penelitian hukum. Kencana.

Pongantung, I., Pangkerego, O. A., & Pinangkaan, N. (2021). Kedudukan Alat Bukti Elektronik Dalam Pembuktian Tindak Pidana Informasi dan Transaksi Elektronik Berdasarkan Undang-Undang Nomor 19 tahun 2016. Lex Crimen, 10(7), 147–156. Retrieved from https://ejournal.unsrat.ac.id/index.php/lexcrimen/article/view/35007

Prayudi, Y., & SN, A. (2025). Digital Chain of Custody: State of The Art. International Journal of Computer Applications, 114(5). https://doi.org/10.5120/19971-1856

Purnama Santhi, N. N. P., & Nuarta, I. N. (2023). Penguatan Penegakan Hukum Polri dalam Rangka Optimalisasi Penanggulangan Cybercrime di Indonesia. SCIENTIA: Journal of Multi Disciplinary Science, 2(1). https://doi.org/10.62394/scientia.v2i1.40

Ratmaja, I. G. S. D., & Mertha, I. K. (2022). Analisis Dasar Pertimbangan Penerapan Dokumen Elektronik dalam Persidangan Perkara Pidana. Jurnal Komunikasi Hukum (JKH), 8(1). https://doi.org/10.23887/jkh.v8i1.43877

Razaque, A., Aloqaily, M., Almiani, M., Jararweh, Y., & Srivastava, G. (2021). Efficient and reliable forensics using intelligent edge computing. Future Generation Computer Systems, 118. https://doi.org/10.1016/j.future.2021.01.012

Sakti, A. (2025). Pengaruh Pendidikan dan Pelatihan Digital Forensik terhadap Kualitas Penanganan Kasus Kejahatan Siber. Populer: Jurnal Penelitian Mahasiswa, 4(1), 104–109. Retrieved from https://doi.org/10.58192/populer.v4i1.2974

Santi, F., Nopalina, F., Mahendra, D. A., & Alfian, D. (2024). Peran Dokter Forensik dalam Penegakan Hukum: Kontribusi Terhadap Proses Penyidikan dan Pembuktian Pidana. Innovatte: Jurnal of Social Science Research, 4(1), 11645–11660.

Sariani, A. L. (2024). Efektivitas Penegakan Hukum Terhadap Kejahatan Siber di Indonesia. Al-Dalil Jurnal Ilmu Sosial, Politik, Dan Hukum, 2(2), 69–77.

Shivdas, S. (2023). A Complete Handbook for Digital Forensics Investigator. International Journal for Research in Applied Science and Engineering Technology, 11(8). https://doi.org/10.22214/ijraset.2023.55257

Soekanto, S., & Mamudji, S. (2021). Penelitian Hukum Normatif: Suatu Tinjauan Singkat. Jakarta: Raja Grafindo.

Yusoff, M. N., Dehghantanha, A., & Mahmod, R. (2017). Forensic Investigation of Social Media and Instant Messaging Services in Firefox OS: Facebook, Twitter, Google+, Telegram, OpenWapp, and Line as Case Studies. In Contemporary Digital Forensic Investigations of Cloud and Mobile Applications. https://doi.org/10.1016/B978-0-12-805303-4.00004-6