Jurnal Kolaboratif Sains, Volume 8 No. 1, Januari 2025, 390-395

Jurnal Kolaboratif Sains
e-ISSN : 2623-2022

Homepage Journal: https://jurnal.unismuhpalu.ac.id/index.php/JKS

Penerapan Konsep Pembuktian Digital dalam Kasus Kejahatan Teknologi Informasi

Application of the Concept of Digital Evidence in Information Technology Crime Cases

Mery Rohana Lisbeth Sibarani[1*], Bambang Supriadi[2], Zabidin[3], Herniwati[4], Ozha Tiwa Hiawananta[5]
[1]Universitas Kristen Indonesia
[2]Universitas Merdeka Malang
[3]Universitas 17 Agustus 1945 Semarang
[4]Sekolah Tinggi ilmu hukum Soelthan M. Tsjafioeddin Singkawang
[5]Universitas Islam Negeri Walisongo
***Corresponding Author**: **E-mail:** merysibaranidosen@gmail.com

Artikel Penelitian

Article History:
Received: 18 Nov, 2024
Revised: 21 Dec, 2024
Accepted: 29 Jan, 2025

Kata Kunci:
Pembuktian Digital, Kejahatan Teknologi Informasi, Bukti Digital, Forensik Digital, Keamanan Siber

Keywords:
Digital Evidence, Technology Crime, Digital Proof, Digital Forensics, Cybersecurity

ABSTRAK

Kejahatan berbasis teknologi juga meningkat seiring dengan berkembangnya teknologi informasi yang sangat pesat. Berbagai pelanggaran yang memanfaatkan perangkat digital termasuk dalam kategori ini: hacking, penipuan online, pencurian identitas, hingga penyebaran informasi yang merugikan. Penerapan konsep pembuktian digital merupakan bagian yang sangat penting dari proses penegakan hukum kejahatan ini. Pengumpulan, penyimpanan, dan analisis bukti dari perangkat atau sistem digital, seperti komputer, ponsel, server, dan jaringan internet, disebut pembuktian digital. Bukti digital ini harus dapat dipertanggungjawabkan secara hukum dan harus menjadi komponen penting dari proses pengadilan. Artikel ini akan membahas lebih lanjut tentang bagaimana konsep pembuktian digital dapat digunakan dalam kasus kejahatan teknologi informasi. Ini akan membahas masalah yang ada dalam proses pembuktian dan solusi untuk masalah tersebut.

ABSTRACT

Technology-based crimes have also increased with the rapid development of information technology. Various offenses that utilize digital devices fall into this category: hacking, online fraud, identity theft, and dissemination of harmful information. The application of digital evidentiary concepts is a very important part of the law enforcement process of these crimes. The collection, storage, and analysis of evidence from digital devices or systems, such as computers, cellphones, servers, and internet networks, is called digital evidence. This digital evidence must be legally admissible and should be an important component of the court process. This article will further discuss how the concept of digital evidence can be used in information technology crime cases. It will discuss the problems that exist in the evidentiary process and solutions to those problems.

DOI: 10.56338/jks.v8i1.6742

PENDAHULUAN

Hampir setiap aspek kehidupan manusia telah sangat dipengaruhi oleh kemajuan teknologi informasi (TI) dalam beberapa dekade terakhir. Beberapa manfaat dari pesatnya transformasi digital termasuk kemudahan akses ke informasi, kemampuan untuk berkomunikasi secara real-time, dan

kemajuan dalam sistem perbankan dan perdagangan online. Namun, tantangan besar muncul di balik kemajuan tersebut: kejahatan yang memanfaatkan teknologi informasi juga dikenal sebagai kejahatan dunia maya. Berbagai pelanggaran ini mencakup berbagai tindak pidana yang dilakukan dengan menggunakan perangkat digital dan internet sebagai alat; ini termasuk peretasan (hacking), pencurian data (data breach), penipuan daring (online fraud), penyebaran malware, dan pelanggaran hak cipta dan kekayaan intelektual.

Seiring dengan semakin mudahnya mendapatkan internet dan perangkat digital, kejahatan teknologi informasi atau cybercrime meningkat dengan cepat. Kejahatan internet ini dapat menargetkan orang, organisasi, atau bahkan negara. Sebagai contoh, serangan siber terhadap infrastruktur penting seperti rumah sakit, bank, dan lembaga pemerintah dapat menyebabkan kerugian finansial, reputasi, dan sosial yang sangat besar. Kejahatan dunia maya juga seringkali sulit untuk ditangani karena bersifat global, dengan pelaku dan korban yang dapat berada di lokasi yang sangat berbeda-beda, dan penggunaan pelaku kejahatan teknologi yang semakin canggih untuk menyembunyikan jejak mereka.

Untuk menangani kejahatan teknologi informasi, salah satu masalah terbesar adalah bagaimana membuktikan adanya kejahatan di pengadilan. Pembuktian digital sangat penting dalam hal ini. Pengumpulan, penyimpanan, dan analisis bukti dari perangkat digital, seperti komputer, ponsel, server, dan sistem jaringan internet, disebut pembuktian digital. Sumber bukti digital dapat berupa file data, log aktivitas sistem, jejak digital di jaringan, atau metadata tentang tindakan pelaku. Dalam kasus ini, bukti digital dapat mencakup bukti yang ditemukan pada perangkat pelaku atau pada server penyedia layanan atau perangkat yang digunakan korban.

Proses pengumpulan dan analisis bukti digital tidak mudah. Penyidik dan penegak hukum menghadapi banyak masalah selama proses ini. Pertama, ada risiko kerusakan atau kehilangan bukti digital selama proses pengumpulan dan penyimpanan jika tidak dilakukan dengan benar. Kedua, karena data digital dapat dengan mudah diubah atau dihapus, pembuktian digital membutuhkan alat dan teknologi yang canggih serta kemampuan untuk menganalisis data yang kompleks dan besar.

Selain masalah tersebut, yurisdiksi hukum masih menghadapi masalah lain. Kejahatan online biasanya melibatkan pelaku dan korban dari berbagai negara. Hal ini menimbulkan kesulitan dalam memperoleh bukti yang sah karena undang-undang dan praktik hukum yang berlaku di setiap negara berbeda. Contohnya, data yang disimpan di server di luar negeri mungkin sulit diakses oleh penegak hukum negara tertentu karena terbatasnya kerjasama internasional atau karena kebijakan perlindungan data pribadi yang ketat di negara tempat server tersebut terletak.

Oleh karena itu, negara-negara di seluruh dunia harus memiliki sistem hukum yang mampu menyesuaikan diri dengan kemajuan teknologi dan bekerja sama dengan negara lain dalam menangani kasus kejahatan dunia maya. Selain itu, penyidik forensik digital dan penegak hukum harus memiliki pengetahuan dan keterampilan yang memadai untuk menangani bukti digital. Untuk memastikan bahwa bukti yang diperoleh dari perangkat digital dapat diterima dan digunakan di pengadilan, pelatihan berkelanjutan dalam prosedur hukum yang berlaku dan teknologi forensik digital sangat penting.

Seiring dengan meningkatnya kompleksitas dan variasi jenis kejahatan yang terjadi di dunia maya, pembuktian digital juga menjadi lebih penting. Serangan siber yang melibatkan ransomware, penipuan online yang menggunakan teknik social engineering, dan pencurian data pribadi yang dilakukan melalui peretasan akun sosial media atau email membutuhkan metode forensik yang lebih khusus. Dengan perkembangan teknologi, pelaku kejahatan juga mengembangkan cara mereka menggunakannya. Oleh karena itu, pembuktian digital yang digunakan dalam menangani kejahatan

teknologi informasi harus mampu mengikuti perkembangan ini dalam hal metodologi, alat yang digunakan, dan kemampuan aparat penegak hukum untuk menangani bukti digital yang semakin kompleks.

Forensik digital menjadi sangat penting dalam konteks ini. Forensik digital adalah bidang ilmu yang berkonsentrasi pada pengumpulan, analisis, dan pelaporan bukti yang terkait dengan tindak kejahatan yang menggunakan teknologi. Proses forensik digital tidak hanya mencakup pengumpulan data, tetapi juga memastikan bahwa bukti yang dikumpulkan dapat digunakan untuk membuktikan kebenaran di pengadilan. Forensik digital melibatkan aspek hukum dan teknis, yang memastikan bahwa bukti yang dikumpulkan dapat dipertanggungjawabkan di pengadilan.

Dengan semakin berkembangnya dunia maya dan berbagai ancaman kejahatan yang muncul, pembuktian digital dalam kasus kejahatan teknologi informasi akan semakin menjadi faktor penting dalam penegakan hukum. Penting bagi penegak hukum, penyidik, dan profesional forensik digital untuk terus memperbarui pengetahuan dan keterampilan mereka, serta bekerja sama secara internasional untuk menciptakan lingkungan digital yang aman.

METODE PENELITIAN

Studi ini menggunakan pendekatan kualitatif deskriptif, yang melibatkan studi pustaka yang mendalam. Penelitian ini mencakup wawancara dengan beberapa ahli forensik digital, praktisi hukum, dan aparat penegak hukum untuk mendapatkan pemahaman tentang masalah dan solusi dalam penggunaan pembuktian digital dalam kasus kejahatan teknologi informasi. Metode ini juga berfokus pada proses pengumpulan dan analisis bukti digital yang sah dan dapat dipertanggungjawabkan di pengadilan.

Studi pustaka mencakup buku, artikel, jurnal ilmiah, dan artikel serta peraturan perundang-undangan tentang pembuktian digital, forensik digital, dan kejahatan teknologi informasi. Selain itu, wawancara juga dilakukan dengan penegak hukum yang langsung menangani kasus kejahatan dunia maya dan praktisi forensik digital.

HASILD DAN PEMBAHASAN

Definisi dan Konsep Pembuktian Digital

Pembuktian digital adalah proses pengumpulan, penyimpanan, dan analisis bukti yang berasal dari perangkat atau sistem digital yang digunakan pelaku atau korban dalam tindak kejahatan. Bukti digital dapat berupa data yang tersimpan di perangkat keras seperti komputer, ponsel, server, atau data yang ada di jaringan internet, seperti log aktivitas, email, pesan instan, rekaman video, atau jejak transaksi digital. Dalam dunia hukum, bukti digital sangat penting untuk mengungkapkan keterlibatan pelaku dalam tindak pidana dan modus operandi yang digunakan.

Beberapa langkah penting dalam pembuktian digital adalah pengumpulan bukti, analisis bukti, dan presentasi bukti di pengadilan. Untuk menghindari kerusakan atau perubahan pada data yang ditemukan, pengumpulan bukti digital harus dilakukan dengan sangat hati-hati. Agar bukti yang diperoleh tetap sah dan dapat dipertanggungjawabkan di pengadilan, proses ini membutuhkan teknik dan prosedur khusus. "Integritas bukti" adalah prinsip utama pembuktian digital, yang berarti bukti digital harus tetap asli dan tidak diubah agar dapat digunakan sebagai alat bukti yang sah.

Selanjutnya, analisis bukti digital dilakukan dengan menggunakan berbagai alat dan teknik forensik digital untuk mengidentifikasi bukti yang relevan, menunjukkan pola-pola yang dapat menghubungkan pelaku dengan kejahatan, dan mengungkapkan waktu dan cara pelaku bertindak. Untuk mendukung proses hukum, hasil analisis ini akan ditulis dalam sebuah laporan yang jelas dan terperinci. Oleh karena itu, bukti digital harus divalidasi dan diakui secara hukum dan teknis agar hakim dapat mempertimbangkannya saat membuat keputusan.

Peran Forensik Digital dalam Pembuktian Kejahatan Teknologi Informasi

Forensik digital sangat penting untuk membuktikan kejahatan teknologi informasi. Forensik digital adalah bidang ilmu yang berkonsentrasi pada identifikasi, pemulihan, dan analisis bukti yang terkait dengan perangkat digital yang terlibat dalam tindak pidana. Keahlian dalam bidang ini memungkinkan penyidik menemukan bukti yang tersembunyi atau dimanipulasi oleh pelaku kejahatan, baik dalam perangkat yang digunakan pelaku maupun korban.

Forensik digital biasanya menggunakan beberapa teknik analisis yang sangat unik, seperti analisis file system (untuk melihat struktur dan data dalam file), rekonstruksi timeline (untuk memahami urutan peristiwa), analisis metadata (untuk menemukan informasi tersembunyi dalam file), dan analisis komunikasi digital (seperti email atau pesan instan) untuk mengidentifikasi hubungan antara orang yang terlibat dalam kejahatan. Alat forensik digital yang digunakan oleh para ahli juga semakin canggih, seperti perangkat lunak untuk menganalisis data tersembunyi (data tersembunyi), perangkat untuk mengidentifikasi jejak digital (jejak digital), dan perangkat untuk memulihkan data yang hilang atau terhapus.

Mengatasi kemungkinan kerusakan atau kehilangan bukti selama proses pengumpulan bukti merupakan tantangan forensik digital. Data digital sangat rentan terhadap perubahan atau penghapusan, baik yang dilakukan secara sengaja oleh individu atau sebagai hasil dari kegagalan sistem atau kerusakan perangkat. Oleh karena itu, penyidik forensik digital harus mengikuti prosedur yang sangat ketat saat mengumpulkan, menyimpan, dan menganalisis data untuk memastikan bahwa bukti tidak berubah atau diubah selama proses analisis. Untuk melakukan ini, penyidik harus menjaga jejak audit yang jelas yang menunjukkan siapa yang dapat mengakses bukti tersebut dan apa yang dilakukan dengannya.

Selain itu, forensik digital menghadapi masalah ketika pelaku menyembunyikan data melalui berbagai metode, seperti enkripsi atau penggunaan perangkat lunak untuk menyembunyikan aktivitas mereka (steganografi). Oleh karena itu, penyidik forensik digital harus memahami dengan baik teknik penyembunyian data ini jika mereka ingin menangani masalah ini dan menemukan bukti yang relevan.

Tantangan dalam Pembuktian Digital pada Kasus Kejahatan Teknologi Informasi

Pembuktian digital menghadirkan banyak masalah yang dapat menghambat proses hukum dalam kasus kejahatan teknologi informasi. Integritas bukti digital merupakan masalah terbesar. Sangat penting untuk memastikan bahwa bukti digital yang dikumpulkan tidak rusak atau diubah karena data digital sangat mudah diubah oleh orang yang ingin menghilangkan jejaknya atau oleh kerusakan teknis pada perangkat penyimpanan. Proses yang ketat untuk mengumpulkan, menyimpan, dan menganalisis bukti diperlukan untuk mencapai hal ini.

Tantangan berikutnya adalah yurisdiksi. Kejahatan teknologi informasi sering melibatkan pelaku dan korban yang berbeda. Ketika bukti yang diperlukan berada di server yang berada di luar negara tempat penyelidikan dilakukan, hal ini menjadi masalah. Negara-negara tertentu memiliki kebijakan yang ketat tentang perlindungan data pribadi, yang menghalangi penyidik dari negara lain untuk mendapatkan data penting. Oleh karena itu, kerjasama internasional sangat penting dalam hal penyelidikan kejahatan dunia maya untuk memastikan bahwa bukti digital dapat diakses secara legal.
Selain itu, perkembangan teknologi yang terus berubah adalah masalah lain. Pelaku kejahatan dunia maya sering menggunakan teknologi terbaru untuk menyembunyikan aktivitas mereka, seperti VPN, enkripsi end-to-end, atau dark web. Selain itu, pelaku kejahatan dapat menggunakan perangkat lunak

yang dapat menghapus jejak aktivitas mereka setelah melakukan tindak pidana, yang membuat proses pencarian bukti lebih sulit. Dalam hal ini, kemampuan dan perangkat penyidik forensik digital harus selalu diperbarui dan ditingkatkan agar mereka dapat mengidentifikasi dan mengatasi metode penyembunyian bukti yang digunakan pelaku.

Sumber daya yang terbatas dan keahlian yang diperlukan untuk penyelidikan forensik digital adalah masalah tambahan. Tidak semua penegak hukum memiliki kemampuan atau sumber daya yang diperlukan untuk menangani bukti digital dengan benar. Oleh karena itu, penting untuk meningkatkan kapasitas penegak hukum dan tenaga forensik digital untuk mengidentifikasi bukti dengan lebih baik. Pengembangan alat forensik digital yang lebih canggih dan mudah digunakan juga sangat penting.

Solusi untuk Mengatasi Tantangan dalam Pembuktian Digital

Beberapa langkah strategis dapat diambil untuk mengatasi berbagai masalah pembuktian digital. Salah satunya adalah dengan meningkatkan kerja sama internasional dalam menangani pelanggaran teknologi informasi. Mengingat bahwa kejahatan dunia maya terjadi di seluruh dunia, sangat penting untuk membangun jaringan kerjasama antarnegara yang memungkinkan pertukaran informasi dan bukti yang sah. Organisasi internasional seperti INTERPOL dan Europol sudah mulai melakukan upaya ini, yang dapat mempercepat akses ke bukti digital yang diperlukan.

Mengembangkan standar yang lebih jelas dan terstruktur juga penting. Negara-negara harus menetapkan undang-undang yang secara rinci mengatur cara mengumpulkan dan menganalisis bukti digital. Untuk memastikan bahwa bukti digital diterima secara sah oleh pengadilan, ada perlunya standar yang jelas untuk praktisi forensik digital dan penyidik dalam mengumpulkan, menganalisis, dan menyajikan bukti di pengadilan.

Untuk menjaga kualitas penyelidikan dan analisis bukti digital, penegak hukum dan ahli forensik digital harus sering dilatih. Pelatihan dapat mencakup dasar teknologi informasi, teknik forensik yang lebih canggih, dan aturan hukum yang berlaku untuk pembuktian digital. Teknologi forensik digital juga harus terus berkembang agar dapat mengikuti teknologi baru yang digunakan oleh pelaku kejahatan. Proses pembuktian akan sangat membantu dengan penggunaan alat forensik terbaru yang dapat mendeteksi dan menganalisis teknik penyembunyian data yang semakin canggih, seperti analisis enkripsi, analisis memori forensik, dan analisis komputasi awan.

KESIMPULAN

Dalam kasus kejahatan teknologi informasi, penerapan konsep pembuktian digital sangat penting untuk keberhasilan penyelidikan dan penuntutan. Pembuktian digital melibatkan beberapa proses yang harus dilakukan dengan hati-hati untuk memastikan bahwa bukti adalah asli dan integritas. Forensik digital sangat penting untuk mengungkap dan menganalisis bukti yang dihasilkan oleh teknologi. Ini juga memastikan bahwa bukti tersebut dapat diterima di pengadilan. Meskipun pembuktian digital menghadapi banyak masalah, seperti masalah integritas bukti, keterbatasan kerja internasional, dan kemajuan teknologi baru, peningkatan kemampuan aparat penegak hukum dan pengembangan peraturan yang lebih baik dapat membantu mengatasi masalah ini. Pembuktian digital yang efektif dapat mempercepat proses penegakan hukum dan membuat pelaku kejahatan teknologi informasi bertanggung jawab.

DAFTAR PUSTAKA

Alfi, M., Yundari, N. P., & Tsaqif, A. (2023). Analisis Risiko Keamanan Siber dalam Transformasi Digital Pelayanan Publik di Indonesia. Jurnal Kajian Stratejik Ketahanan Nasional, 6(2), 5. https://doi.org/10.7454/jkskn.v6i2.10082

Fachmi, A., & Mayesti, N. (2022). Tinjauan literatur argumentatif tentang kepemilikan data arsip digital non-fungible token (NFT) pada teknologi blockchain. Berkala Ilmu Perpustakaan Dan Informasi, 18(1), 144–158. https://doi.org/10.22146/bip.v18i1.3989

Kehista, A. P., Fauzi, A., Tamara, A., Putri, I., Fauziah, N. A., Klarissa, S., & Damayanti, V. B. (2023). Analisis Keamanan Data Pribadi pada Pengguna E-Commerce: Ancaman, Risiko, Strategi Kemanan (Literature Review). Jurnal Ilmu Manajemen Terapan, 4(5), 625–632.

Kristanti, O., & Kuntadi, C. (2022). Literature Review: Pengaruh Audit Forensik, Audit Investigatif, Dan Kompetensi Auditor Terhadap Pengungkapan Fraud. SENTRI: Jurnal Riset Ilmiah, 1(3), 840–848. https://doi.org/10.55681/sentri.v1i3.295

Piter, J., Nainggolan, B. R. M., Indonesia, U. P., Accounting, F., Technology, I., & Audit, I. (2024). LITERATURE REVIEW : METODE WHISTLEBLOWING , TEKNOLOGI INFORMASI , AKUNTANSI FORENSIK DAN AUDIT INVESTIGATIF UNTUK MEMBANTU. 01(01), 16–33.

Ray, S., Das, J., Pande, R., & Nithya, A. (2024). Swati Ray 1 , Joyati Das 2* , Ranjana Pande 3 , and A. Nithya 2. 6(1), 195–222. https://doi.org/10.1201/9781032622408-13

Rizki Kurniarullah, M., Nabila, T., Khalidy, A., Juniarti Tan, V., Widiyani, H., Hukum Universitas Maritim Raja Ali Haji Abstrak, I., & Kunci, K. (2024). Tinjauan Kriminologi Terhadap Penyalahgunaan Artificial Intelligence: Deepfake Pornografi dan Pencurian Data Pribadi. Jurnal Ilmiah Wahana Pendidikan, 10(10), 534–547. https://doi.org/10.5281/zenodo.11448814