Journal of Innovative and Creativity
Journal Homepage: https://joecy.org/index.php/joecy
e-mail: journaljoecy@gmail.com

Faculty of Education
University of Pahlawan Tuanku Tambusai
ISSN 2775-771X (Online)
ISSN 2962-570X **(Printed)**
5 (2) 2025, Page: 4377-4384

Eksaminasi Terhadap Bukti Digital Dalam Kasus Kejahatan Cyber

Mhd Ilham Nasution[1], Bambang Fitrianto [2], Gian Randa Juangsah[3], Muhammad Haykal[4], M. Adnan[5]
[1,2,3,4,5]Universitas Pembangunan Panca Budi
Corresponding Author: Mhd Ilham Nasution, e-mail: ilhamnasution123@gmail.com

Published: May, 2025

ABSTRAK

Perkembangan teknologi informasi dan komunikasi telah membawa tantangan serius dalam sistem hukum, khususnya terkait pembuktian dalam perkara kejahatan siber. Karakteristik bukti digital yang tidak berwujud, mudah dimanipulasi, dan tersebar lintas yurisdiksi memerlukan pendekatan hukum dan teknis yang spesifik. Penelitian ini bertujuan untuk mengkaji mekanisme eksaminasi bukti digital dalam konteks hukum pidana di Indonesia, serta mengevaluasi kesiapan instrumen hukum dan kapasitas penegak hukum dalam menanganinya. Dengan menggunakan metode kajian literatur, penelitian ini menemukan bahwa meskipun secara normatif bukti digital telah diakui melalui UU ITE, implementasinya masih menghadapi berbagai kendala, termasuk keterbatasan sumber daya manusia, infrastruktur teknologi, dan harmonisasi regulasi lintas batas. Digital forensik menjadi instrumen krusial dalam memastikan validitas dan keabsahan bukti elektronik dalam proses pembuktian. Oleh karena itu, penguatan kapasitas investigasi digital serta penegakan standar forensik harus menjadi prioritas guna menjamin due process of law dan keadilan substantif dalam penanganan kejahatan siber di Indonesia.

Kata Kunci: Kejahatan cyber, bukti digital

ABSTRACT

The rapid development of information and communication technology has introduced significant challenges to the legal system, particularly in the realm of evidentiary procedures in cybercrime cases. The intangible, easily manipulated, and cross-jurisdictional nature of digital evidence necessitates both legal and technical approaches tailored to its unique characteristics. This study aims to examine the mechanisms of digital evidence examination within the framework of Indonesia's criminal law, while also evaluating the readiness of legal instruments and the capacity of law enforcement in addressing these challenges. Using a literature review method, the study finds that although digital evidence has been normatively recognized through the Electronic Information and Transactions Law (ITE Law), its practical implementation still faces various obstacles, including limited human resources, inadequate technological infrastructure, and insufficient cross-border regulatory harmonization. Digital forensics emerges as a crucial tool in ensuring the validity and admissibility of electronic evidence in legal proceedings. Therefore, strengthening digital investigative capacity and enforcing forensic standards must become a priority to ensure due process of law and substantive justice in handling cybercrime in Indonesia.

***Keywords**: Cybercrime, digital evidence*

© The Author(s). 2021 Open Access This article is licensed under a Creative Commons Atibution 4.0 International License, which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons licence, and indicate if changes were made. The images or other third party material in this article are included in the article's Creative Commons licence, unless indicated otherwise in a credit line to the material. To view a copy of this licence, visit http://creativecommons.org/licenses/by/4.0

PENDAHULUAN

Perkembangan pesat teknologi informasi dan komunikasi dalam beberapa dekade terakhir telah membawa dampak signifikan terhadap berbagai aspek kehidupan manusia. Kemudahan akses informasi, efisiensi dalam berkomunikasi, serta inovasi dalam berbagai sektor ekonomi dan sosial menjadi beberapa manfaat utama dari kemajuan teknologi digital. Namun, di balik manfaat tersebut, muncul pula tantangan serius berupa kejahatan siber (cybercrime) yang semakin kompleks dan meresahkan. Kejahatan siber mencakup berbagai tindak pidana yang dilakukan melalui atau terhadap sistem

komputer dan jaringan internet, seperti peretasan (hacking), pencurian identitas, penipuan online, penyebaran virus, serta penyalahgunaan data pribadi (Aini & Lubis, 2024)

Di Indonesia, fenomena kejahatan siber menunjukkan tren yang meningkat seiring dengan semakin meluasnya penggunaan teknologi digital di masyarakat. Berdasarkan data dari Badan Siber dan Sandi Negara (BSSN), pada tahun 2022 tercatat lebih dari 400 juta anomali trafik siber yang terdeteksi, menunjukkan eskalasi ancaman digital yang mengkhawatirkan (Widatama, 2019).

Salah satu tantangan utama dalam penegakan hukum terhadap kejahatan siber adalah persoalan pembuktian. Berbeda dengan kejahatan konvensional yang melibatkan barang bukti fisik, kejahatan siber bergantung pada bukti digital yang bersifat elektronik, tidak berwujud, mudah dimanipulasi, dan sering kali tersebar dalam berbagai lokasi digital yang tidak terikat oleh batas yurisdiksi geografis. Bukti digital dapat berupa log aktivitas pengguna, data perangkat, rekaman komunikasi, transaksi elektronik, dokumen digital, hingga metadata yang berkaitan dengan peristiwa kriminal yang terjadi di ruang maya (Anggraeni & Salsabila, 2024)

Validitas, keabsahan, serta integritas bukti digital menjadi isu sentral dalam proses peradilan. Pengumpulan, pelestarian (preservation), analisis, dan presentasi bukti digital harus dilakukan dengan metode dan standar tertentu yang mengacu pada prinsip-prinsip forensik digital. Kegagalan dalam mengikuti prosedur hukum dan teknis yang sah dapat berakibat pada ditolaknya bukti digital oleh pengadilan, yang pada akhirnya berpengaruh terhadap pembuktian dan keadilan dalam proses hukum (Dewa Gede Giri Santosa, 2022).

Di Indonesia, meskipun Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE) yang diperbarui dengan Undang-Undang Nomor 19 Tahun 2016 telah mengakui eksistensi bukti elektronik sebagai alat bukti yang sah, praktik di lapangan masih menunjukkan berbagai kelemahan. Aparat penegak hukum sering kali belum memiliki kapasitas yang memadai dalam melakukan investigasi berbasis digital, dan keterbatasan infrastruktur teknologi di beberapa daerah juga menjadi penghambat utama dalam penegakan hukum berbasis bukti digital. Selain itu, tantangan dari sisi keterbukaan data, kolaborasi lintas negara, serta keterbatasan regulasi menjadi hambatan lain yang perlu segera diatas (Iman et al., 2020)

Sejatinya kajian mengenai tema ini sudah banyak dilakukan, salah satunya penelitian yang dilakukan oleh (Riadi et al., 2020) menunjukkan hasil analisis TRIM enable metode penghapusan shift delete tidak ditemukan bukti digital yang sesuai nilai hash dengan bukti digital asli. Sedangkan metode penghapusan delete, delete recycle bin bukti digital dapat dikembalikan dengan prosentase keberhasilan menggunakan tool Autopsy sebesar 90% dan 10% nilai hash bukti digital tidak valid, sedangkan tool Recuva 80% bukti digital berhasil dikembalikan dan 20% tidak berhasil dikembalikan, dapat disimpulkan hasil recovery penghapusan delete, delete recycle bin pada SSD NVME TRIM enable dapat dijadikan bukti digital yang sah menurut hukum.

Melanjutkan penelitian sebelumnya, penelitian yang dilakukan oleh (Anshori et al., 2020) Hasil yang didapatkan dari penelitian ini adalah MOBILedit Forensic Express mendapatkan bukti digital berupa 2 akun, 11 chat dan 26 gambar dengan persentase berupa 100% dalam mendapatkan akun, 55% dalam mendapatkan chat dan 86% dalam mendapatkan gambar. Dapat disimpulkan bahwa MOBILedit Forensic Express memiliki kinerja yang baik dalam mendapatkan bukti digital.

Melihat hasil penelitian sebelumnya, penelitian yang dilakukan oleh (Anwar & Riadi, 2017) bahwa penanganan tindak kejahatan yang melibatkan piranti digital perlu ditekankan sehingga dapat membantu proses peradilan akan efek yang ditimbulkannya. Investigasi Forensika Digital turut berperan serta terhadap penindakan penyalahgunaan fitur layanan pesan instan WhatsApp diantaranya langkah investigasi penanganan kasus penyadapan percakapan WhatsApp melalui serangkaian tahapan baku sesuai prosedur forensika digital. Eksplorasi barang bukti (digital evidence) percakapan WhatsApp akan menjadi acuan akan tindak kejahatan penyadapan telekomunikasi yang selanjutnya akan dilakukan report investigation forensics yang melibatkan barang bukti smartphone dan komputer korban.

Dengan demikian, eksaminasi terhadap bukti digital menjadi aspek yang krusial dalam menjamin keadilan dalam penanganan kasus kejahatan siber. Eksaminasi bukan hanya menyangkut keabsahan bukti dari sisi teknis forensik, tetapi juga dari aspek hukum, prosedural, dan etika. Penelitian ini bertujuan untuk mengkaji secara mendalam bagaimana bukti digital diperoleh, diuji, dan dipertanggungjawabkan secara hukum dalam konteks penanganan kejahatan siber di Indonesia, serta untuk mengidentifikasi tantangan-tantangan yang muncul dalam implementasinya. Diharapkan bahwa hasil kajian ini dapat memberikan kontribusi pada penguatan sistem hukum pidana nasional dalam menghadapi era digital yang semakin kompleks dan dinamis.

METODOLOGI PENELITIAN

Penelitian ini menggunakan metode kajian literatur (library research) yang bertujuan untuk mengkaji berbagai referensi yang relevan terkait dengan eksaminasi bukti digital dalam kasus kejahatan cyber. Data yang digunakan dalam penelitian ini berasal dari berbagai sumber tertulis, seperti jurnal ilmiah, artikel, buku, serta laporan dari lembaga-lembaga yang berkompeten dalam bidang kejahatan cyber dan hukum. Analisis dilakukan dengan pendekatan deskriptif-analitik untuk menggambarkan, memahami, dan mengkritisi permasalahan yang ada seputar bukti digital dalam sistem peradilan di Indonesia (Juni Sahla Nasution et al., 2024).

HASIL DAN PEMBAHASAN

Pengaturan Hukum Digital Forensik dalam Pembuktian Tindak Pidana di Indonesia

Pemanfaatan teknologi informasi dan komunikasi telah memberikan dampak signifikan terhadap sektor hukum di Indonesia, khususnya dalam aspek penegakan hukum terhadap tindak pidana. Fenomena ini menjadi perhatian serius seiring dengan meningkatnya angka kejahatan yang memanfaatkan media digital sebagai sarana dalam menjalankan aksinya. Dalam konteks ini, konsep digital forensik memegang peranan penting karena menjadi salah satu metode utama dalam proses pengumpulan, analisis, dan penyajian bukti digital di hadapan pengadilan.

Digital forensik sendiri merupakan cabang dari ilmu forensik yang berfokus pada proses identifikasi, akuisisi, pengolahan, analisis, dan pelaporan data elektronik yang memiliki relevansi hukum. Bukti-bukti digital tersebut diperlukan dalam penanganan perkara yang memerlukan pembuktian melalui data elektronik. Dalam tahapan penyelidikan dan penyidikan, digital forensik berfungsi sebagai alat bantu yang krusial bagi penyidik, sebagaimana telah diatur dalam Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik, serta Kitab Undang-Undang Hukum Acara Pidana (KUHAP).

Dalam kerangka hukum acara pidana, peran bukti digital menjadi bagian integral dari proses pembuktian di persidangan, di mana hakim melakukan pemeriksaan perkara berdasarkan bukti yang diajukan dan diakui secara sah menurut hukum untuk menilai kebenaran suatu peristiwa hukum. Peristiwa yang dilaporkan dalam suatu perkara pidana akan melalui tahap pembuktian, yang merupakan inti dari proses persidangan. Dalam konteks ini, Jaksa Penuntut Umum memiliki kewajiban untuk menyajikan bukti-bukti yang relevan guna meyakinkan Majelis Hakim terhadap validitas dan keabsahan atas kejadian yang dituduhkan. Pembuktian memiliki posisi yang sangat krusial karena menjadi landasan bagi hakim dalam menentukan kesalahan atau ketidakbersalahan terdakwa.

Menurut (Hiariej., 2012) proses pembuktian dalam perkara pidana erat kaitannya dengan pencarian kebenaran sejati (materiil), yaitu kebenaran yang sesuai dengan kenyataan peristiwa hukum yang terjadi. Berdasarkan teori pembuktian, hakim dalam menjatuhkan putusan harus dilandasi oleh keyakinan yang dibentuk melalui bukti-bukti yang sah menurut ketentuan hukum. Hal ini ditegaskan dalam Pasal 183 Undang-Undang Nomor 8 Tahun 1981 tentang Hukum Acara Pidana (KUHAP), yang menyatakan bahwa hakim hanya dapat menjatuhkan pidana apabila sekurang-kurangnya didukung oleh dua alat bukti yang sah dan disertai keyakinan bahwa terdakwa benar-benar bersalah melakukan tindak pidana tersebut.

Alat bukti memiliki peran sentral dalam membentuk keyakinan hakim. KUHAP dalam Pasal 184 ayat (1) menyebutkan lima jenis alat bukti yang sah dalam hukum acara pidana, yakni: (1) keterangan saksi, (2) keterangan ahli, (3) surat, (4) petunjuk, dan (5) keterangan terdakwa (Auli, 2023). Meskipun tidak tercantum secara eksplisit dalam pasal tersebut, informasi elektronik dan/atau dokumen

elektronik beserta hasil cetaknya kini telah diakui sebagai alat bukti hukum yang sah berdasarkan Pasal 5 Ayat (1) Undang-Undang Nomor 11 Tahun 2008 jo. Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik (UU ITE), yang menyatakan bahwa: *"Informasi Elektronik dan/atau Dokumen Elektronik dan/atau hasil cetaknya merupakan alat bukti hukum yang sah."*

Selanjutnya, Pasal 5 Ayat (2) UU ITE menegaskan bahwa alat bukti elektronik merupakan bentuk perluasan dari alat bukti sah yang dapat digunakan dalam proses peradilan sesuai dengan hukum acara yang berlaku di Indonesia. Dengan demikian, dapat disimpulkan bahwa alat bukti elektronik memiliki kekuatan hukum yang setara dengan alat bukti konvensional sebagaimana tercantum dalam KUHAP. Hal ini telah diperkuat melalui berbagai putusan pengadilan, salah satunya Putusan Mahkamah Konstitusi Nomor 20/PUU-XIV/2016 yang secara eksplisit mengakui status dan legalitas alat bukti elektronik dalam proses peradilan pidana di Indonesia.

Peran Digital Forensik dalam Pembuktian Tindak Pidana di Indonesia

Pembuktian merupakan unsur yang sangat esensial dalam proses persidangan pidana, karena menjadi tahapan krusial dalam mengungkap kebenaran atas suatu peristiwa hukum. Proses ini melibatkan penyajian bukti-bukti yang dapat memberikan dasar keyakinan bagi hakim untuk menilai apakah suatu tindak pidana benar-benar terjadi dan apakah terdakwa bertanggung jawab atas perbuatan tersebut. Pada tahap ini, baik Jaksa Penuntut Umum maupun pihak terdakwa diberikan kesempatan yang seimbang untuk membuktikan dalil masing-masing.

Dalam pelaksanaannya, proses pembuktian harus tunduk pada ketentuan hukum yang berlaku, termasuk tata cara penyampaian bukti, jenis alat bukti yang sah, dan prinsip-prinsip dasar dalam hukum acara pidana. Berdasarkan sistem pembuktian yang dianut dalam hukum acara pidana Indonesia, yakni *negatief wettelijk bewijstheorie* (Medeline et al., 2023), pembuktian tidak hanya didasarkan pada jumlah alat bukti yang sah, tetapi juga pada keyakinan hakim yang diperoleh dari alat bukti tersebut. Hal ini secara tegas diatur dalam Pasal 183 Kitab Undang-Undang Hukum Acara Pidana (KUHAP), yang menyatakan bahwa: *"Hakim tidak boleh menjatuhkan pidana kepada seseorang kecuali apabila dengan sekurang-kurangnya dua alat bukti yang sah ia memperoleh keyakinan bahwa suatu tindak pidana benar-benar terjadi dan bahwa terdakwalah yang bersalah melakukannya."*

Ketentuan dalam pasal tersebut secara jelas menegaskan bahwa seorang hakim tidak diperkenankan untuk menjatuhkan pidana kepada terdakwa apabila perbuatannya tidak dapat dibuktikan sekurang-kurangnya dengan dua alat bukti yang sah. Sebaliknya, apabila hakim memperoleh keyakinan yang didasarkan pada dua alat bukti yang sah, maka ia berwenang menjatuhkan putusan pidana terhadap terdakwa. Dalam praktik peradilan, meskipun keyakinan hakim merupakan unsur subjektif, unsur tersebut tidak dapat berdiri sendiri tanpa didukung alat bukti yang sah menurut hukum. Namun demikian, terdapat kondisi di mana pembuktian yang cukup kuat dan meyakinkan dapat

mendorong hakim untuk mengesampingkan keraguannya dan menyimpulkan bahwa perbuatan terdakwa terbukti secara sah sebagai suatu tindak pidana (Harahap, 2009).

Bukti elektronik memiliki karakteristik yang unik karena bersifat tidak kasat mata, mudah diubah, serta rentan terhadap kerusakan dan manipulasi. Oleh karena itu, proses pengumpulan bukti elektronik harus dilakukan oleh tenaga ahli yang memiliki kompetensi khusus di bidang digital forensik. Digital forensik sendiri merupakan cabang dari ilmu forensik yang berfokus pada identifikasi, analisis, dan interpretasi data digital yang terdapat dalam berbagai perangkat elektronik sebagai bagian dari proses penyelidikan dan penyidikan hukum. Peran digital forensik sangat signifikan dalam tahap pembuktian tindak pidana, tidak hanya untuk memperkuat dakwaan yang diajukan oleh Jaksa Penuntut Umum, tetapi juga sebagai instrumen penting dalam mengungkap identitas serta menjerat pelaku kejahatan berbasis teknologi (RACHMIE, 2020).

Ilmu digital forensik memiliki peran yang sangat signifikan dalam proses pembuktian perkara pidana, khususnya yang berkaitan dengan kejahatan berbasis teknologi. Secara umum, tahapan dalam digital forensik terdiri atas lima proses utama, yaitu: identifikasi, preservasi, analisis, reduksi dan penyaringan data, serta pelaporan. Tahap awal, yakni identifikasi, bertujuan untuk menemukan lokasi penyimpanan bukti digital serta memahami bentuk dan karakteristik data tersebut. Setelah bukti berhasil diidentifikasi, proses dilanjutkan dengan preservasi, yaitu upaya menjaga integritas dan keaslian data agar tidak mengalami perubahan, kerusakan, atau manipulasi sejak pertama kali ditemukan (Holt, T. J., Bossler, A. M., & Seigfried-Spellar, 2022).

Tahap berikutnya adalah analisis, yang merupakan proses penafsiran dan rekonstruksi data untuk memperoleh pemahaman menyeluruh mengenai relevansi dan keterkaitan bukti dengan peristiwa pidana yang sedang diselidiki. Selanjutnya, dilakukan reduksi dan penyaringan data, yaitu proses penyederhanaan dan seleksi terhadap kumpulan data yang ada guna memperoleh subset data yang paling relevan dan signifikan secara hukum. Proses ini penting untuk meningkatkan efisiensi serta fokus dalam kajian forensik.

Tahap terakhir adalah pelaporan, yakni penyusunan dokumen resmi yang memuat hasil temuan forensik secara komprehensif. Laporan ini harus disusun dengan transparan, sistematis, dan rinci untuk memastikan kejelasan serta akuntabilitas dalam setiap tahapan investigasi, sekaligus menghindari munculnya keraguan di kemudian hari. Dengan melalui seluruh tahapan tersebut, digital forensik menjadi instrumen yang esensial dalam menemukan, mengamankan, serta menilai validitas bukti elektronik untuk kemudian diajukan secara sah dalam proses persidangan.

KESIMPULAN

Kejahatan siber merupakan tantangan nyata dalam era digital yang menuntut penyesuaian menyeluruh dalam sistem hukum pidana, terutama pada aspek pembuktian. Bukti digital, sebagai

instrumen utama dalam pembuktian perkara siber, memiliki sifat yang kompleks dan memerlukan pendekatan khusus dalam pengumpulan, pelestarian, dan analisisnya. Meskipun Undang-Undang ITE telah mengakui legalitas bukti elektronik, tantangan dalam praktik masih signifikan, baik dari sisi teknis, yuridis, maupun kapasitas kelembagaan. Penegakan hukum terhadap kejahatan siber belum sepenuhnya efektif akibat keterbatasan sumber daya penegak hukum, kurangnya infrastruktur digital forensik, serta belum optimalnya koordinasi lintas sektor dan lintas negara. Oleh karena itu, diperlukan reformasi struktural dan peningkatan kapasitas SDM dalam bidang digital forensik, serta harmonisasi regulasi yang mampu menjawab dinamika kejahatan digital lintas yurisdiksi. Tanpa langkah konkret dalam memperkuat eksaminasi bukti digital, sistem peradilan pidana dikhawatirkan tidak mampu memberikan perlindungan hukum yang adil dan responsif terhadap tantangan era digital.

DAFTAR PUSTAKA

Aini, N., & Lubis, F. (2024). Tantangan Pembuktian Dalam Kasus Kejahatan Siber. *Judge: Jurnal Hukum*, *05*(02), 55–63. http://www.journal.cattleyadf.org/index.php/Judge/article/view/566%0Ahttp://www.journal.cattleyadf.org/index.php/Judge/article/download/566/433

Anggraeni, D. R., & Salsabila, M. (2024). Analisis Yuridis Peran Digital Forensik Dalam Pembuktian Tindak Pidana di Indonesia. *Media Hukum Indonesia (MHI)*, *2*(2), 593–600.

Anshori, I., Setya Putri, K. E., & Ghoni, U. (2020). Analisis Barang Bukti Digital Aplikasi Facebook Messenger Pada Smartphone Android Menggunakan Metode NIJ. *IT Journal Research and Development*, *5*(2), 118–134. https://doi.org/10.25299/itjrd.2021.vol5(2).4664

Anwar, N., & Riadi, I. (2017). Analisis Investigasi Forensik WhatsApp Messanger Smartphone Terhadap WhatsApp Berbasis Web. *Jurnal Ilmiah Teknik Elektro Komputer Dan Informatika*, *3*(1), 1. https://doi.org/10.26555/jiteki.v3i1.6643

Auli, R. C. (2023). *Alat Bukti Sah Menurut Pasal 184 KUHAP*.

Dewa Gede Giri Santosa, K. M. I. K. (2022). Acquisition and Presentation of Digital Evidence in Criminal Trial in Indonesia. *Jurnal Hukum Dan Peradilan*, *Vol. 11*, *N*.

Harahap, M. Y. (2009). *Pembahasan Permasalahan dan Penerapan KUHAP: Pemeriksaan Sidang Pengadilan, Banding, Kasasi dan Peninjauan Kembali*. Jakarta: Sinar Grafika.

Hiariej., E. O. S. (2012). *Teori & Hukum Pembuktian*. Jakarta: Penerbit Erlangga.

Holt, T. J., Bossler, A. M., & Seigfried-Spellar, K. C. (2022). *Cybercrime and Digital Forensics*. Routledge: An Introduction.

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

Juni Sahla Nasution, Dinah Nadhifah, Wahyu Azhari, & Abdal Rizky Munthe. (2024). Peningkatan Keterampilan Menulis Teks Prosedur Melalui Penggunaan Media Video. *Sinar Dunia: Jurnal Riset Sosial*

Humaniora Dan Ilmu Pendidikan, *3*(2), 228–235. https://doi.org/10.58192/sidu.v3i2.2196

Medeline, F., Rusmiati, E., & Ramadhani, R. H. (2023). Forensik Digital dalam Pembuktian Tindak Pidana Ujaran Kebencian di Media Sosial. *PAMPAS: Journal of Criminal Law*, *3*(3), 310–325. https://doi.org/10.22437/pampas.v3i3.19691

RACHMIE, S. (2020). Peranan Ilmu Digital Forensik Terhadap Penyidikan Kasus Peretasan Website. *Litigasi*, *21*(21), 104–127. https://doi.org/10.23969/litigasi.v21i1.2388

Riadi, I., Sunardi, S., & Hadi, A. (2020). Analisis Bukti Digital TRIM Enable SSD NVMe Menggunakan Metode Static Forensics. *JUITA: Jurnal Informatika*, *8*(1), 65. https://doi.org/10.30595/juita.v8i1.6584

Widatama, K. (2019). Sistem Monitoring Bukti Digital Untuk Meningkatkan Kontrol Terhadap Kasus Cybercrime Di Indonesia. *INTEK: Jurnal Informatika Dan Teknologi Informasi*, *2*(1), 39–46. https://doi.org/10.37729/intek.v2i1.88