Investigasi Forensik Dalam Proses Pencarian Bukti Digital Dengan Menggunakan Metode NIJ (National Institute of Justice)

I Putu Dharma Aditya[1a)], Ni Kadek Sukerti[2b)], I Ketut Putu Suniantara[2c)]
[1)]Sistem Komputer, Institut Teknologi dan Bisnis STIKOM Bali, Bali, Indonesia
[2)]Sistem Informasi, Institut Teknologi dan Bisnis STIKOM Bali, Bali, Indonesia
e-mail: [a)]200010025@stikom-bali.ac.id, [b)]nikadek_sukerti@stikom-bali.ac.id, [c)]suniantara@stikom-bali.ac.id

Abstrak

Perkembangan teknologi informasi mempermudah distribusi data digital, namun juga meningkatkan potensi kejahatan siber seperti penyebaran konten pornografi. Penelitian ini bertujuan menganalisis penerapan Metode National Institute of Justice (NIJ) dalam pencarian bukti digital serta efektivitas FTK Imager dan Autopsy dalam mengungkap kasus penyebaran konten pornografi pada FlashDisk SanDisk Ultra 3.0 berkapasitas 16 GB. Penelitian menggunakan pendekatan forensik digital eksperimental dengan tahapan identifikasi, akuisisi, analisis, dan pelaporan. Pada tahap akuisisi, pembuatan forensic image dilakukan dengan FTK Imager menggunakan tiga variasi image fragment size (0 MB, 16.000 MB, dan 1.500 MB), lalu diverifikasi menggunakan algoritma MD5 dan SHA-256. Analisis dilanjutkan dengan Autopsy untuk mengekstraksi file aktif, file terhapus, dan artefak digital lainnya. Hasil penelitian menunjukkan proses akuisisi berjalan efisien dan aman, dengan kecepatan rata-rata 20,7 MB/s dan integritas data yang terjaga. Autopsy mampu memulihkan berbagai file penting terkait kasus. Dengan demikian, penerapan Metode NIJ dengan kombinasi FTK Imager dan Autopsy terbukti efektif, cepat, dan akurat dalam pengungkapan bukti digital kasus penyebaran konten pornografi.

Kata kunci: *Digital Forensik, Metode NIJ, FTK Imager, Autopsy, FlashDisk.*

1. Pendahuluan

Perkembangan teknologi informasi dan komunikasi yang pesat telah membawa dampak signifikan terhadap banyak aspek kehidupan, termasuk dalam bidang kriminalitas. Salah satu kejahatan yang semakin marak terjadi adalah kejahatan *cyber*, yang mencakup berbagai tindakan ilegal yang dilakukan melalui perangkat digital, seperti penyebaran konten pornografi. Penyebaran pornografi melalui media penyimpanan portabel, seperti *FlashDisk,* telah menjadi masalah serius dalam dunia maya, yang tidak hanya merusak moral masyarakat tetapi juga menimbulkan berbagai dampak negatif bagi individu dan institusi [1].

Dalam menangani kejahatan *cyber,* forensik digital menjadi salah satu pendekatan yang sangat penting. Forensik digital bertujuan untuk mengidentifikasi, memulihkan, dan menganalisis bukti digital yang dapat digunakan dalam proses hukum. Salah satu metode yang digunakan dalam investigasi forensik digital adalah metode National Institute of Justice (NIJ), yang berfokus pada pengumpulan bukti yang bersifat data akan tetap tersimpan meskipun perangkat dimatikan. Studi kasus dalam penelitian ini mengacu pada penyebaran konten pornografi yang telah disebarkan, beberapa di antaranya disimpan dan didistribusikan menggunakan media penyimpanan *FlashDisk* [2]. Keberadaan *FlashDisk* sebagai sarana penyimpanan dan distribusi konten pornografi menunjukkan bahwa bukti digital tidak hanya berasal dari media sosial, tetapi juga dari perangkat fisik yang dapat dengan mudah dipindahkan atau disembunyikan. Oleh karena itu, metode National Institute of Justice (NIJ) sangat diperlukan untuk mengidentifikasi dan mengamankan data digital dari perangkat seperti *FlashDisk* secara cepat dan tepat tanpa merusak bukti asli.

Metode National Institute of Justice (NIJ) memiliki peran yang sangat penting dalam penyelidikan kasus penyebaran pornografi melalui *FlashDisk. FlashDisk,* sebagai perangkat penyimpanan portabel yang mudah digunakan dan dibawa, sering menjadi media untuk memindahkan, menyebarkan, dan menyimpan konten illegal. Oleh karena itu, penting untuk dapat mengakses data yang ada pada *FlashDisk* dengan tepat dan efektif, terutama dalam kondisi dimana data dapat terhapus atau tersembunyi, sehingga bukti dapat ditemukan dan digunakan dalam proses hukum [3].

Penelitian yang dilakukan oleh S. Soni, Y. Fatma, dan R. Anwar berfokus pada akuisisi dan analisis bukti digital pada aplikasi pesan instan Bip dengan menerapkan metode National Institute of Justice (NIJ) sebagai kerangka kerja forensik digital. Penelitian ini dilatarbelakangi oleh semakin meningkatnya penggunaan aplikasi pesan instan sebagai sarana komunikasi yang berpotensi dimanfaatkan dalam tindak kejahatan digital, sehingga diperlukan metode forensik yang terstandarisasi untuk mengamankan dan mengolah barang bukti digital. Dalam pelaksanaannya, peneliti menerapkan tahapan Metode National Institute of Justice (NIJ) yang meliputi proses identifikasi sumber bukti digital, pengumpulan data, pemeriksaan, analisis, hingga pelaporan hasil investigasi forensik. Melalui proses akuisisi forensik yang dilakukan pada aplikasi Bip, penelitian ini berhasil memperoleh berbagai artefak digital, seperti data percakapan, informasi akun pengguna, serta metadata yang berkaitan dengan aktivitas komunikasi. Penelitian ini juga menekankan pentingnya menjaga integritas dan keaslian data selama proses akuisisi agar bukti digital yang diperoleh tidak mengalami perubahan dan dapat dipertanggungjawabkan secara hukum. Hasil penelitian menunjukkan bahwa metode National Institute of Justice (NIJ) efektif digunakan dalam proses investigasi forensik pada aplikasi pesan instan Bip karena mampu menghasilkan bukti digital yang relevan, valid, dan tersusun secara sistematis, sehingga dapat mendukung proses penegakan hukum dan pembuktian dalam kasus kejahatan siber [4].

Penelitian yang dilakukan oleh I. Wahyudi, A. Muntasa, M. Yusuf, dan A. Hamzah membahas proses pengungkapan dan pengujian keaslian bukti digital dalam penanganan kasus kejahatan siber *(cybercrime)* dengan menerapkan metode Digital Forensic Research Workshop (DFRWS) sebagai kerangka kerja forensik digital. Penelitian ini dilatarbelakangi oleh meningkatnya tindak kejahatan siber yang menuntut adanya penanganan bukti digital secara profesional dan terstandarisasi agar bukti yang diperoleh tidak hanya dapat mengungkap peristiwa kejahatan, tetapi juga memiliki kekuatan hukum. Metode DFRWS digunakan untuk mengelola tahapan forensik digital yang meliputi identifikasi sumber bukti, proses akuisisi dan pengumpulan data, pemeriksaan, analisis, hingga penyajian hasil investigasi. Dalam pelaksanaannya, penelitian ini menekankan pentingnya menjaga integritas, keaslian, dan keutuhan bukti digital selama proses investigasi forensik. Peneliti melakukan analisis terhadap barang bukti digital guna menemukan jejak aktivitas yang berkaitan dengan tindak kejahatan siber, sekaligus melakukan pengujian untuk memastikan bahwa data tersebut tidak mengalami perubahan sejak pertama kali diakuisisi. Hasil penelitian menunjukkan bahwa penerapan metode DFRWS mampu membantu investigator dalam mengungkap bukti digital secara sistematis dan akurat serta memastikan keaslian bukti digital, sehingga hasil investigasi dapat dipertanggungjawabkan secara teknis maupun hukum dan mendukung proses pembuktian dalam penanganan kasus *cybercrime* [5].

Penelitian yang dilakukan oleh R. Umar, A. Yudhana, dan M. N. Fadillah [6] berfokus pada perbandingan kinerja dan kemampuan beberapa *tools* forensik digital dalam menangani bukti digital pada aplikasi dompet digital. Penelitian ini dilatarbelakangi oleh semakin meningkatnya penggunaan dompet digital dalam transaksi keuangan yang berpotensi menimbulkan permasalahan hukum dan tindak kejahatan siber, sehingga diperlukan *tools* forensik yang andal untuk mengamankan serta menganalisis bukti digital. Dalam penelitian ini, penulis melakukan pengujian terhadap beberapa *tools* forensik dengan menilai kemampuannya dalam melakukan proses akuisisi data, pemeriksaan, dan analisis artefak digital yang tersimpan pada aplikasi dompet digital [7]. Melalui proses perbandingan tersebut, penelitian ini mengevaluasi efektivitas masing-masing *tools* dalam mengungkap informasi penting, seperti data transaksi, informasi akun pengguna, dan artefak digital lainnya yang relevan dengan proses investigasi. Penelitian ini juga menekankan aspek keakuratan hasil, kelengkapan data yang diperoleh, serta kemudahan penggunaan *tools* forensik yang diuji [8]. Hasil penelitian menunjukkan adanya perbedaan kemampuan antar *tools* forensik digital dalam menangani aplikasi dompet digital, sehingga penelitian ini memberikan rekomendasi mengenai *tools* yang paling sesuai dan efektif untuk digunakan dalam proses investigasi forensik digital pada kasus yang melibatkan aplikasi dompet digital.

Tujuan dilakukannya penelitian ini, dapat mengkaji lebih dalam bagaimana metode National Institute of Justice (NIJ) diterapkan dalam proses pencarian bukti digital, khususnya dalam kasus penyebaran konten pornografi melalui media *FlashDisk.* Penelitian ini mengevaluasi efektivitas metode tersebut, tantangan yang muncul dalam praktiknya, serta prosedur yang diperlukan untuk menjamin keabsahan dan integritas bukti digital. Diharapkan hasil penelitian ini dapat memberikan kontribusi terhadap pengembangan standar dan praktik investigasi forensik digital di Indonesia.

2. Metode Penelitian

Penelitian ini didasarkan pada metode pengumpulan barang bukti forensik dari National Institute of Justice (NIJ) metode ini menjelaskan bagaimana tahapan – tahapan penelitian yang dilakukan, sehingga

alur penelitian dapat diselesaikan secara sistematis dan dapat dijadikan pedoman untuk memecahkan permasalahan yang ada. Menurut penelitian yang telah dilakukan oleh Yudharta Arif pengumpulan data forensic mencapai hasil hampir 100% jika teknik dan analisis forensik dilakukan berdasarkan metode yang tepat [9].

Metodologi pada National Institute of Justice (NIJ) ini dibagi menjadi lima fase yaitu: tahapan *identification, collection, examination, analysis* dan *reporting* [10].

a. Tahapan *Identification*
   Tahap *identification* meliputi pengklasifikasian barang bukti digital yang bertujuan untuk mengenali, menentukan, serta memastikan bentuk, jenis, dan lokasi bukti digital yang relevan dengan kasus yang sedang diselidiki.
b. Tahapan *Collection*
   Tahap *collection* merupakan sebuah rangkaian kegiatan dalam mengumpulkan data guna mendukung dari proses penyelidikan pencarian barang bukti digital. Dalam fase ini informasi yang diperoleh berdasarkan sumber data yang relevan.
c. Tahapan *Examination*
   Tahap *examination* merupakan tahap dimana data yang dikumpulkan baik secara otomatis ataupun secara manual, bertujuan untuk dilakukannya pembacaan, penelusuran, dan pemeriksaan struktur data yang terdapat di dalam *image file* guna menemukan bukti digital yang relevan dengan kasus yang diselidiki [11].
d. Tahapan *Analysis*
   Tahap *analysis* merupakan fase lanjutan yang berfungsi untuk menafsirkan, mengelompokkan, dan menarik makna dari data hasil pemeriksaan *(examination)* yang telah dilakukan sebelumnya. Serta untuk menghubungkan antara artefak digital dengan aktivitas pengguna yang berpotensi mengarah pada tindakan pelanggaran hukum.
e. Tahapan *Reporting*
   Tahap *reporting* merupakan tahap akhir dalam metodologi investigasi forensik digital berbasis model National Institute of Justice (NIJ). Pada tahap ini, seluruh hasil kegiatan mulai dari identifikasi, akuisisi, pemeriksaan, hingga analisis disusun secara sistematis dalam bentuk laporan forensik yang bersifat ilmiah, objektif, dan dapat dipertanggungjawabkan secara hukum [12].

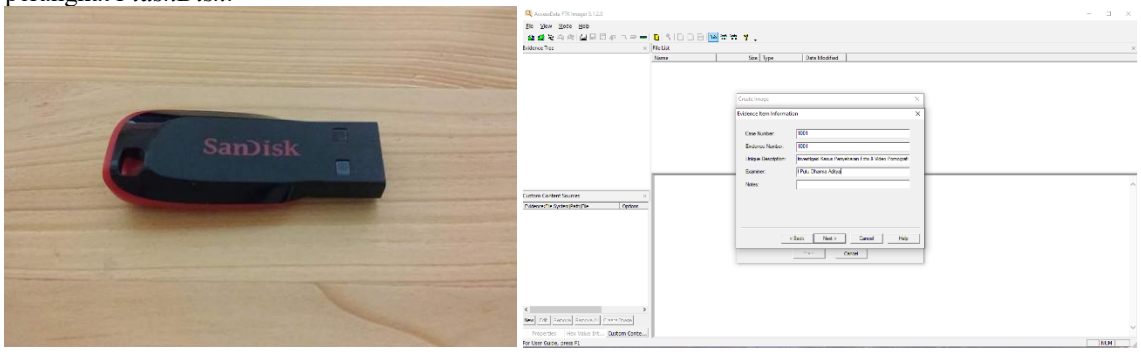
3. Hasil dan Pembahasan

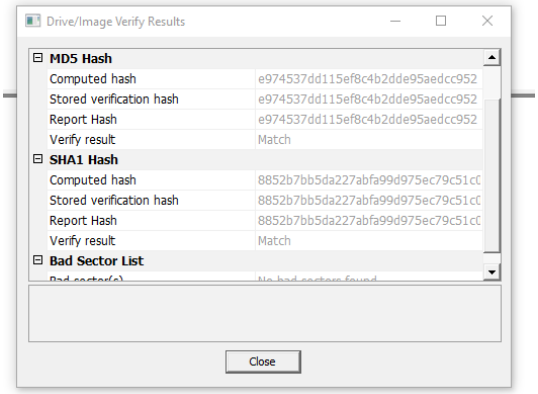
3.1 *Identification*

Pada tahap identifikasi ini penyidik melakukan proses pengumpulan barang bukti pada sebuah perangkat *FlashDisk* serta menyiapkan alat dan bahan yang dipergunakan dalam proses pengumpulan barang bukti forensik seperti 1 Unit laptop, dan 2 *tools* forensik yaitu FTK Imager dan Autopsy.

3.2 *Collection*

Tahap selanjutnya adalah tahap dimana barang bukti dikumpulkan guna menjaga keaslian dari barang bukti *FlashDisk* yang ditemukan untuk menghindari adanya kerusakan atau hilangnya barang bukti pada kasus tersebut. Gambar 1 menunjukan proses pengumpulan barang bukti yang digunakan berupa perangkat *FlashDisk*.

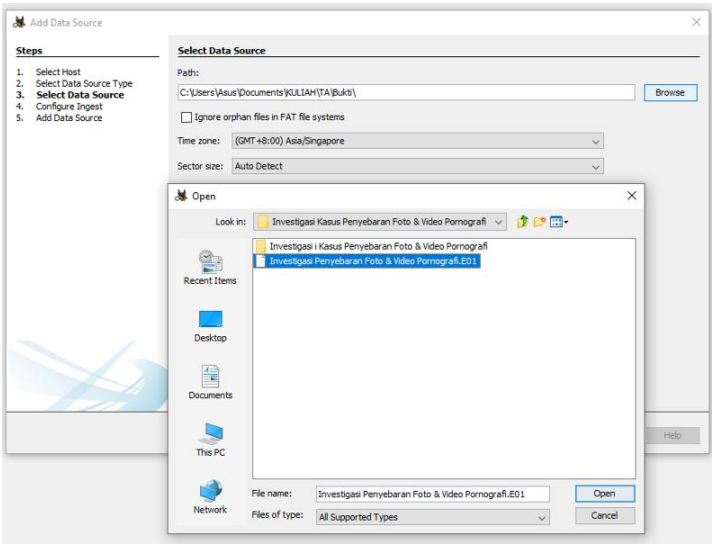




Gambar 1. Proses pengumpulan barang bukti berupa *FlashDisk* menggunakan *tools* FTK Imager

3.3 *Examination*

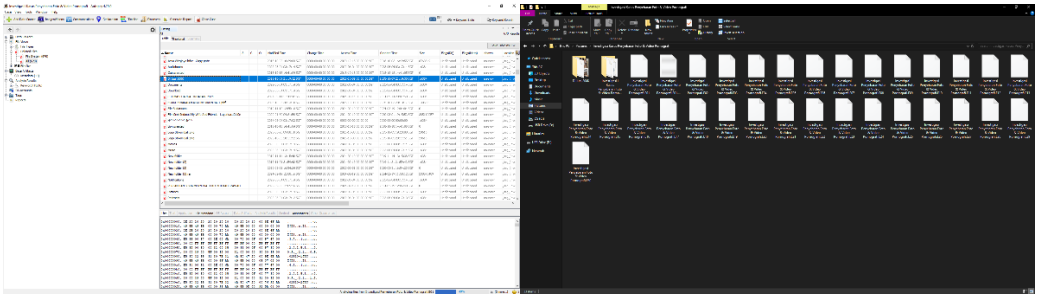
Tahap examination merupakan tahap pemeriksaan data digital yang sudah diperoleh sebelumnya pada barang bukti *FlashDisk* SanDisk 16GB dengan menggunakan *tools* Autopsy. Selanjutnya Gambar 2 menunjukan proses pemeriksaan data menggunakan *tools* Autopsy dan menemukan sebuah file yang diduga didalam file tersebut berisi foto dan video.

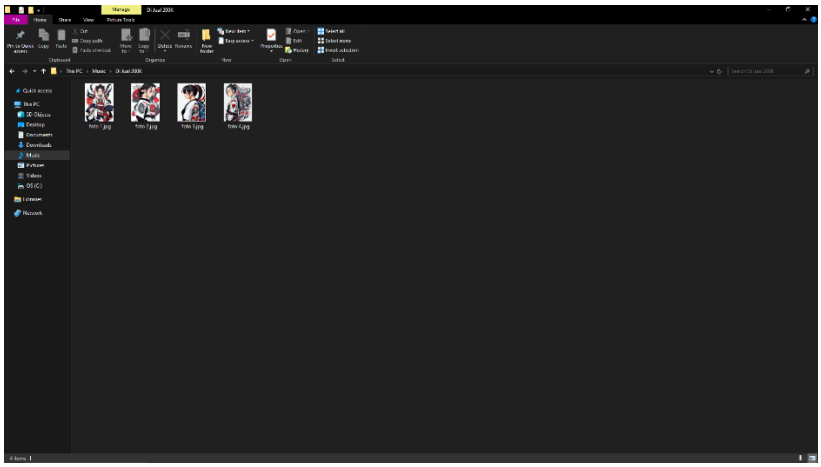


Gambar 2. Proses Pemeriksaan data digital menggunakan *tools* Autopsy

3.4 Analysis

Setelah dilakukannya hasil ekstraksi data digital menggunakan *tools* FTK Imager, ditemukan sebuah file foto dan video yang mencurigakan, diduga kasus dari pelaku yang memiliki barang bukti tersebut. Pada Gambar 3 menunjukan proses hasil ekstraksi data digital yang diperoleh.





Gambar 3. Proses hasil ekstraksi data digital menggunakan *tools* FTK Imager

Hasil dari ekstraksi data digital menggunakan *tools* FTK Imager, ditemukan adanya foto dan video pada file yang sengaja dihapus pada *FlashDisk* pelaku untuk menghilangkan jejak digital. Dengan dilakukannya proses ekstraksi ditemukan sejumlah foto dan video yang memiliki unsur pornografi.

3.5 Reporting

Setelah dilakukannya proses akuisisi pada barang bukti yang ditemukan, dapat disimpulkan bahwa melakukan proses forensik pada *FlashDisk* berhasil dikumpulkan. Berdasarkan hasil simulasi yang dilakukan, telah berhasil menemukan bukti digital penyebaran dan unggahan foto dan video yang dilakukan oleh pelaku. Setelah dilakukan proses akuisisi terhadap *FlashDisk* dengan menggunakan *tools* Autopsy dan FTK Imager diketahui memiliki efisiensi yang tinggi pada hasil ekstraksi dan mendapatkan barang bukti digital pada *FlashDisk* pelaku.

Tabel 1. Hasil Ekstraksi

Barang Bukti	Nama Barang Bukti	Keterangan
FlashDisk	SanDisk 16GB	Barang bukti ditemukan disebuah meja pada saat proses simulasi investigasi dilakukan.
Folder berisi File	Dijual 200K	Bukti digital tersebut setelah dilakukan analisa menggunakan *tools* Autopsy dan FTK Imager berhasil ditemukan penyebaran foto dan video pornografi oleh pelaku.

4. Kesimpulan

Berdasarkan hasil penelitian dan pembahasan yang telah dilakukan, dapat disimpulkan bahwa metode National Institute of Justice (NIJ) dapat diterapkan secara efektif dalam proses investigasi forensik digital pada media penyimpanan *FlashDisk* yang digunakan dalam kasus penyebaran konten pornografi. Penerapan tahapan NIJ yang meliputi *identification, collection, examination, analysis,* dan *reporting* mampu memberikan alur kerja investigasi yang sistematis, terstruktur, serta menjaga keutuhan dan keaslian barang bukti digital. Proses akuisisi barang bukti menggunakan FTK Imager berhasil dilakukan dengan baik tanpa mengubah data asli pada *FlashDisk,* sedangkan proses analisis menggunakan Autopsy mampu mengekstraksi serta memulihkan file digital, termasuk file foto dan video yang telah dihapus oleh pelaku. Hasil analisis menunjukkan bahwa tools FTK Imager dan Autopsy memiliki tingkat efisiensi dan akurasi

yang tinggi dalam menemukan artefak digital yang relevan dengan kasus, sehingga mendukung proses pengungkapan bukti digital secara optimal.

Daftar Pustaka

[1] Aidil Wijaya Kusuma, Erick Irawadi Alwi, and Ramdaniah Ramdaniah, "Analisis Bukti Digital Pada Media Penyimpanan Flash Disk Menggunakan *Metode National Institute Of Standards And Technology (NIST)*," *Cyber Secur. dan Forensik Digit.*, vol. 7, no. 1, pp. 18–24, Nov. 2024, doi: 10.14421/csecurity.2024.7.1.4345.

[2] M. Syaiful Huda Mubarok, A. Ardiansyah, R. Novrianda Dasmen, V. Pranata, and M. A. Januarta, "Digital Analysis of Forensic Data Recovery on Flash Drive Using National Institute Of Justice (NIJ) Method," J. Ilm. Inform., vol. 12, no. 01, pp. 75–79, 2024.

[3] R. A. Ramadhan, Abdul Kudus Zaini, and Jerika Mardafora, "Pelatihan Investigasi Digital Forensik," J. Pengabdi. Masy. dan Penerapan Ilmu Pengetah., vol. 3, no. 2, pp. 1–6, 2022, doi: 10.25299/jpmpip.2022.11003.

[4] S. Soni, Y. Fatma, and R. Anwar, "Akuisisi Bukti Digital Aplikasi Pesan Instan 'Bip'Menggunakan Metode National Institute Of Justice (NIJ)," J. CoSciTech (Computer Sci. Inf. Technol., vol. 3, no. 1, pp. 34–42, 2022, doi: 10.37859/coscitech.v3i1.3694.

[5] I. Wahyudi, A. Muntasa, M. Yusuf, and A. Hamzah, "Mengungkap Dan Menguji Keaslian Bukti Digital Pada Kejahatan Cybercrime Dengan Metode Digital Forensic Research Workshop," J. Apl. Teknol. Inf. dan Manaj., vol. 2, no. 2, pp. 120–127, 2021, doi: 10.31102/jatim.v2i2.1068.

[6] R. Umar, A. Yudhana, and M. N. Fadillah, "Perbandingan Tools Forensik Pada Aplikasi Dompet Digital," JIKO (Jurnal Inform. dan Komputer), vol. 6, no. 2, p. 242, 2022, doi: 10.26798/jiko.v6i2.621.

[7] I. Anshori, K. E. Setya Putri, and U. Ghoni, "Analisis Barang Bukti Digital Aplikasi Facebook Messenger Pada Smartphone Android Menggunakan Metode NIJ," IT J. Res. Dev., vol. 5, no. 2, pp. 118–134, 2020, doi: 10.25299/itjrd.2021.vol5(2).4664.

[8] Elsya indah Fitria, "Penerapan Digital Forensics Research Workshop Dalam Akuisisi Evidence Forensik Snack Video," J. Komput. Teknol. Inf. dan Sist. Inf., vol. 2, no. 2, pp. 390–399, 2023, doi: 10.62712/juktisi.v2i2.108.

[9] R. T. Amanah, F. Fachri, and T. Informatika, "Identifikasi Bukti Digital Sistem Property Pada Instagram Menggunakan Live Forensik," JATI (Jurnal Mhs. Tek. Inform., vol. 9, no. 1, pp. 1197–1201, 2025.

[10] F. Medeline, E. Rusmiati, and R. H. Ramadhani, "Forensik Digital dalam Pembuktian Tindak Pidana Ujaran Kebencian di Media Sosial," PAMPAS J. Crim. Law, vol. 3, no. 3, pp. 310–325, May 2023, doi: 10.22437/pampas.v3i3.19691.

[11] E. Koisin and F. Melania Lalamafu, "Sistem Komputer Dalam Pelaporan Pengunaan Dana Desa," Cerdika J. Ilm. Indones., vol. 1, no. 2, pp. 103–113, 2021, doi: 10.59141/cerdika.v1i2.22.

[12] K. Fadhlil Khaliq, "Pengamanan Data Akta Dengan Metode Aes Berbasis Cloud Computing," J. Teknol. Dan Ilmu Komput. Prima, vol. 4, no. 1, pp. 509–512, 2021, doi: 10.34012/jutikomp.v4i1.1555.