

# AKUSISI FORENSIK DIGITAL PADA APLIKASI GOOGLE DRIVE SEBAGAI BUKTI DIGITAL DALAM PENYELIDIKAN KASUS PORNOGRAFI

Pande Aditya Pratama Putra<sup>1)</sup>, Ni Kadek Sukerti<sup>2)</sup>, I Ketut Putu Suniantara<sup>3)</sup>

Program Studi Sistem Komputer

Institut Teknologi dan Bisnis STIKOM Bali

Denpasar, Indonesia

e-mail: 200010024@stikombali.ac.id<sup>1)</sup>, dektisamuh@gmail.com<sup>2)</sup>, suniantara@stikom-bali.ac.id<sup>3)</sup>

## Abstrak

*Ponsel pintar merupakan salah satu bukti teknologi digital. Perkembangan ponsel pintar juga sangat pesat terutama menjadi media penyimpanan awan atau cloud. Penyimpanan cloud yang tersedia di android dan merupakan aplikasi bawaan dari sebuah ponsel pintar atau smartphone salah satunya adalah aplikasi Google Drive. Perkembangan media penyimpanan awan ini bisa saja membuat dampak negative pada penggunaannya untuk tindakan kejahatan seperti cybercrime dan pornografi. Penelitian ini menggunakan skenario pada kondisi pengguna aplikasi yang digunakan, termasuk menghapus data pada aplikasi tersebut. Eksperimen pengambilan data menggunakan metode National Institute of Justice (NIJ). Data yang didapatkan akan dikumpulkan dan dilakukan analisis menggunakan software MOBILEdit Forensic Express dan Magnet AXIOM, setelah itu, dilakukan analisis lebih lanjut untuk menunjukkan bahwa data tersebut bisa digunakan dalam menyelesaikan sebuah kasus. Setelah data tersebut diperoleh, dilakukan analisis perbandingan terhadap bukti digital yang terkait dengan penelitian, perangkat, dan aplikasi cloud storage. Penelitian ini memiliki tujuan untuk menanggapi dampak negative penyebaran konten pornografi melalui aplikasi Google Drive pada perangkat berbasis Android. Hasil dari penelitian ini adalah untuk mendapatkan kembali barang bukti yang telah terhapus oleh pelaku guna memperkuat bukti dan menghukum pelaku. Penelitian ini juga menekankan aspek etika dan privasi harus menjadi perhatian utama ketika menggunakan bukti digital dalam konteks kasus konten pornografi.*

**Kata kunci:** *Forensik Digital, Google Drive, National Institute of Justice (NIJ), Penyebaran konten Pornografi*

## 1. Pendahuluan

Pada era digital yang terus berkembang, aplikasi seluler berbasis *android*, seperti *Google Drive*, telah menjadi bagian penting dari kehidupan masyarakat. *Google Drive* memungkinkan penggunaannya untuk menyimpan, berbagi, dan mengakses berbagai jenis informasi dengan mudah, termasuk foto, video, dan dokumen. Namun, seperti halnya dengan teknologi lainnya, *Google Drive* juga dapat disalahgunakan, contohnya seperti menyebarkan konten pornografi, yang memiliki dampak negatif yang signifikan bagi masyarakat. Penegakan hukum dan penyelidikan kasus pornografi memerlukan bukti yang kuat untuk menghukum pelaku tersebut.

Forensik digital dengan menggunakan *Google Drive* di *Android* sangat penting untuk mengumpulkan dan menganalisis bukti digital terkait kasus pornografi. Penyebaran konten pornografi seringkali menggunakan *Google Drive*, yang digunakan oleh banyak orang dengan jumlah pengguna aktif mencapai 800 juta. Oleh karena itu, banyak orang yang memanfaatkannya untuk melakukan kejahatan, seperti kasus *Dea OnlyFans* yang menyebarkan 76 video pornografi melalui *Google Drive* [1].

Penelitian ini dilakukan untuk mengumpulkan bukti forensik adanya kegiatan kriminal menyebarluaskan konten pornografi pada *Google Drive*. Metode penyelidikan yang digunakan mengacu pada *National Institute of Justice (NIJ)*, yang dikenal karena reputasinya dalam mengembangkan metode forensik digital yang handal. Melalui tahapan *identification, collection, examination, analysis, dan reporting* yang disediakan oleh *NIJ*, diharapkan bukti digital yang diperoleh akan memiliki tingkat keandalan dan integritas tinggi dalam proses penyelidikan yang efektif dan adil.

Penelitian yang dilakukan oleh Ikhwan Anshori, melibatkan analisis terhadap barang bukti digital yang terkait dengan aplikasi *Facebook Messenger* pada perangkat berbasis *android*. Dalam penelitian ini, penulis menerapkan metode *National Institute of Justice (NIJ)*. Hasil penelitian menunjukkan bahwa

*MOBILedit Forensic Express* dan *Magnet AXIOM* menunjukkan kinerja yang memuaskan dalam pengambilan bukti digital dari aplikasi *Facebook Messenger*. Namun, *Oxygen Forensic Suite 2014* menunjukkan kinerja yang kurang memuaskan, terutama dalam hal pengambilan data percakapan (*chat*). Penelitian yang dilakukan oleh Anton Yudhana mengenai proses pengumpulan data digital dari aplikasi *Google Drive* pada perangkat *Android* dengan menggunakan metodologi *National Institute of Justice (NIJ)*. Hasil penelitian ini menghasilkan bukti yang signifikan terkait penggunaan metode *NIJ* dalam membrantas kejahatan digital. Hasil proses akuisisi data tersebut dianalisis melalui proses dekripsi kode-kode hexsa yang dihasilkan, dengan tujuan menghasilkan bukti digital yang dapat dipahami dan diajukan kepada hakim sebagai bagian dari proses peradilan. Penelitian yang dilakukan oleh I Putu Denny Indra Putra, dalam penelitian ini, digunakan metode *National Institute of Justice (NIJ)* untuk menyelidiki platform *WhatsApp Messenger* yang digunakan untuk *cyberbullying*. Metode *NIJ* memiliki 5 tahap untuk melaksanakan proses forensik, yaitu Persiapan, Pengumpulan, Pemeriksaan, Analisis, dan Pelaporan. Penelitian ini juga menggunakan bantuan dari 3 perangkat lunak, yaitu *MOBILedit Forensic*, *DB Browser for SQLite*, dan *Odin3*. Penelitian yang dilakukan oleh Desti Muallifah, dalam Penelitian ini, membahas proses *digital forensic* untuk mencari bukti digital yang dihapus pada aplikasi *TamTam Messenger*, menggunakan *MobileEdit forensic* dan metode *National Institute of Justice*. Hasilnya menunjukkan bahwa alat tersebut berhasil mengembalikan bukti digital yang dihapus oleh pelaku pada aplikasi *Tam Tam Messenger* [2]–[5].

Penelitian yang dilakukan oleh I Gusti Ngurah Guna Wicaksana, dalam Penelitian ini menjelaskan langkah-langkah untuk menyelidiki kasus kejahatan dunia maya yang terjadi pada aplikasi desktop Telegram. Metodologi yang digunakan dalam penelitian ini mengacu pada langkah investigasi yang dilakukan pada penelitian sebelumnya, termasuk penggunaan metodologi *National Institute of Justice (NIJ)*. Media yang digunakan dalam penelitian ini adalah aplikasi desktop Telegram. Selama proses ini, lokasi file log, cache, dan file gambar bukti digital akan diperoleh dalam percakapan aplikasi desktop Telegram. Penelitian yang dilakukan oleh Syifa Riski Ardiningtias, dengan judul *Investigasi digital pada Facebook Messenger Menggunakan National Institute of Justice*. Hasil penyidikan dapat dijadikan alat bukti untuk membantu penyidik dalam menangani perkara pidana dan sebagai acuan saat penyidik mencari alat bukti dalam kasus penyebaran konten pornografi melalui aplikasi *Facebook Messenger*. *MobilEdit* menerima hampir semua bukti dengan tingkat keberhasilan 85,71%, sedangkan *Wondershare Dr.fone* hanya mendapat 28,57%. Pengujian yang dilakukan oleh Hijrah Nurhairan, dalam penelitian ini, memberikan perbandingan antara bukti dengan *smartphone* yang sudah di-root dan *smartphone* yang belum di-root. Kondisi *smartphone* yang sudah di-root ditemukan dalam bentuk 2 partisipan pengguna, 3 pesan obrolan, dan 1 gambar, lokasi, dan profil pelaku, sedangkan pada *smartphone* yang belum di-root hanya mendapatkan 1 file *APK*. Bukti berupa percakapan yang diperoleh dari *smartphone* yang belum di-root membuktikan adanya ujaran kebencian antara pelaku dan korban [6]–[8].

Penelitian yang dilakukan oleh Aries Suharso, [9] dengan judul *Akuisisi Bukti Digital Dan Deteksi Keaslian Citra Pada Whatsapp Menggunakan Metode NIST Dan ELA*. Hasil dari penelitian ini mengungkapkan bahwa *Magnet Axiom* berhasil menemukan beberapa barang bukti, diantaranya pesan percakapan, kontak korban, riwayat panggilan, serta foto profil dari pelaku, dan gambar pelaku. Dengan bantuan *tools ForensicallyBeta* gambar struk yang diperoleh dapat dianalisis dan menentukan bahwa telah terjadi modifikasi pada bukti struk tersebut.

Penelitian yang dilakukan oleh Yuyun Dwi Lestari, [10] dengan judul *Analisis Perbandingan Kinerja Root Explorer dan Oxygen Forensic Detective Pada Forensic Digital*. Hasil pengujian menunjukkan bahwa *Oxygen Forensic Detective* bekerja lebih unggul daripada Aplikasi *Root Explorer* dalam pengujian yang dilakukan. Meskipun keduanya berhasil menemukan semua informasi pengguna dan data yang dihapus, *Oxygen Forensic Detective* memberikan output yang lebih sesuai dengan harapan. *Software Root Explorer* tidak dapat membagikan gambar dan menemukan gambar dalam format *JPG*.

Penelitian yang dilakukan oleh Andi Muh Afdal, [11] dengan judul *Analisis Bukti Digital Forensik pada Discord Menggunakan Metode National Institute of Standards Technology*. Hasil penelitian ini menunjukkan bahwa saat menggunakan *tool FTK Imager*, didapatkan hanya gambar dengan presentase 38,46%, untuk video didapatkan presentase 15,38%. Selain itu teks percakapan, waktu, identitas tidak ditemukan.

Berdasarkan dari penelitian diatas ini, Terdapat variasi *tools* forensik yang dapat digunakan dalam pencarian barang bukti digital, memudahkan *investigator* dalam mengidentifikasi bukti yang telah dihapus oleh pelaku kejahatan. Setiap *tools* memiliki tingkat keberhasilan pemulihan barang bukti digital yang berbeda, Oleh karena itu, penelitian ini difokuskan pada kasus pornografi dengan membandingkan dua

---

*tools*, yaitu *MobilEdit Forensics* dan *Magnet AXIOM*, bertujuan memberikan wawasan lebih mendalam tentang efektivitas keduanya dalam pengumpulan barang bukti digital.

Tujuan penelitian ini adalah untuk menanggapi dampak negatif penyebaran konten pornografi melalui aplikasi *Google Drive* pada perangkat *Android* dengan melakukan penegakan hukum dan penyelidikan kasus-kasus pornografi. Penelitian ini bertujuan untuk mengumpulkan bukti forensik digital yang kuat guna mengidentifikasi dan menghukum pelaku kejahatan tersebut.

## 2. Metode Penelitian

Penggunaan metode penelitian ini didasarkan pada metode pengumpulan bukti forensik dari *National Institute of Justice (NIJ)*. Metode ini digunakan untuk menjelaskan bagaimana tahapan – tahapan penelitian dilakukan, sehingga alur penelitian dapat diselesaikan secara sistematis dan dapat dijadikan pedoman untuk memecahkan permasalahan yang ada. Menurut penelitian yang dilakukan Roni Anggara pengumpulan data forensik mencapai hasil hampir 100% bila teknik dan analisis forensik dilakukan berdasarkan metode yang tepat.[12].

Metodologi dari *National Institute of Justice* ini dibagi menjadi lima fase yaitu : *identification*, *collection*, *examination*, *analysis*, dan *reporting* [13].

### a. Tahapan Identification

Tahap identifikasi meliputi pengklasifikasian barang bukti dan data kriminal digital untuk mendukung proses penyelidikan dalam pencarian bukti kriminal digital. Fase ini meliputi proses identifikasi, pelabelan, dan pencatatan barang bukti.

### b. Tahapan Collection

Tahap *collection* atau tahap pengumpulan merupakan rangkaian kegiatan pengumpulan data guna mendukung proses penyelidikan pencarian barang bukti kejahatan digital. Pada fase ini, informasi diperoleh dari sumber data yang relevan dan integritas bukti perubahan dipertahankan [14].

### c. Tahapan Examination

Tahap *examination* adalah tahap dimana data yang dikumpulkan, baik secara otomatis atau manual, diperiksa secara forensik dan memastikan bahwa data yang diperoleh sebagai file adalah asli dan sesuai dengan data yang diperoleh dari TKP komputer, itulah sebabnya *file* digital dibuat, diidentifikasi dan diverifikasi *file* menggunakan teknik hashing.

### d. Tahapan Analysis

Tahap penyelidikan ini dilakukan setelah menerima file atau bukti digital yang ditemukan dari proses penyelidikan sebelumnya, dan bukti tersebut dilakukan analisis secara rinci dengan menggunakan metode pembuktian informasi yang dibenarkan secara teknis dan hukum. [15].

### e. Tahapan Reporting

Tahapan ini merupakan tahap pelaporan hasil yang diperoleh selama analisis, yang meliputi deskripsi penelitian yang dilakukan, menjelaskan alat forensik yang digunakan, urutan langkah yang dipilih, dan kemudian menentukan langkah selanjutnya. Serta memberikan saran dan rekomendasi terhadap penelitian akhir guna memperbaiki prosedur, alat forensik, praktik dan aspek ilmu forensik lainnya [16].

## 3. Hasil dan Pembahasan

### 3.1 Identification

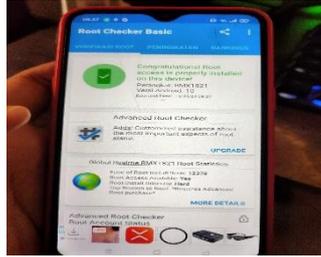
Tahap identifikasi ini dilakukan dengan menyiapkan peralatan dan alat yang akan dipergunakan oleh penyidik untuk melakukan proses pengumpulan bukti forensik. Alat dan bahan yang dipergunakan dalam proses pengumpulan bukti forensik seperti 1 buah komputer, 1 buah *smartphone*, kabel data *USB*, *Google Drive*, dan 2 *tools* forensik yaitu *MOBILedit Forensic Express*, *Magnet AXIOM*.

### 3.2 Collection

Tahap selanjutnya adalah tahap dimana bukti elektronik yang diperlukan untuk membantu dalam melakukan penelitian dalam mengumpulkan bukti digital yang diharapkan. Penelitian ini menggunakan

---

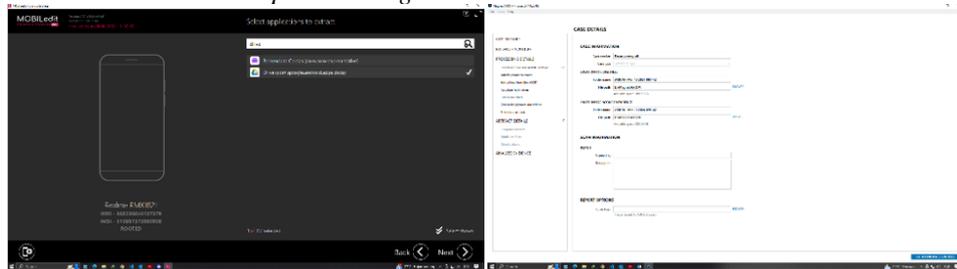
barang bukti elektronik yaitu *smartphone* Realme 3, *android* versi 10. Gambar 1 menunjukkan proses *rooting* merupakan proses pada digital forensik untuk mendapatkan akses secara penuh pada ponsel pintar pelaku.



Gambar 1. Proses *Rooting*.

### 3.3 Examination

Tahap *examination* adalah pemeriksaan bukti digital. Bukti kejahatan diperoleh dengan memeriksa data yang dikirim dari *smartphone* Android ke PC melalui kabel data. Proses ini menggunakan software *MobilEdit Forensics Express & Magnet AXIOM*.



Gambar 2. Proses Eksaminasi pada aplikasi *MobilEdit Forensics & Magnet AXIOM*.

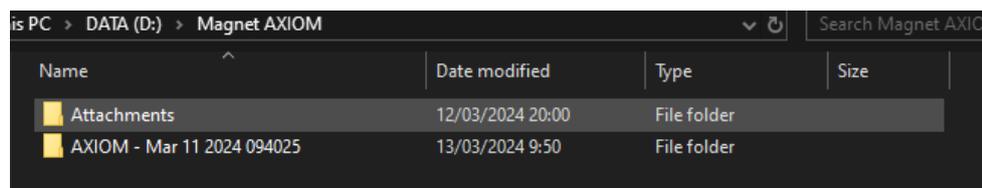
### 3.4 Analysis

Hasil ekstraksi data digital menggunakan aplikasi *MobilEdit Forensics* dan *Magnet AXIOM* ditemukan pada penyimpanan ponsel pelaku.



Gambar 3. Hasil dari proses Ekstrak aplikasi *MobileEdit Forensics*

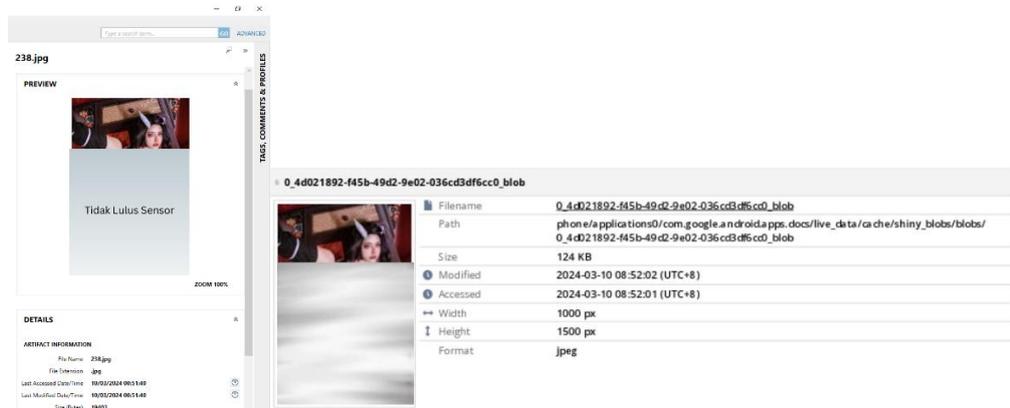
Proses ekstrak menggunakan *MobileEdit Forensics Express* menghasilkan bukti berupa file dan direktori *folder* yang tersimpan pada penyimpanan *ponsel*, data tersebut meliputi *file* dan direktori yang terletak pada penyimpanan tersebut, diperoleh informasi bukti digital yang terhapus pada *smartphone* pelaku. Hasil dari proses ekstraksi akan berupa *file* yang ada dimemori perangkat *seluler*, Cara ini memberikan akses ke seluruh *file* yang diperoleh selama ekstarksi yang tersedia di aplikasi penyimpanan *cloud* *Google Drive*. Hasil yang didapat saat diekstrak menggunakan *Magnet AXIOM* mendapatkan 2 *folder* saja.



Gambar 4. Hasil dari proses Ekstrak aplikasi *Magnet AXIOM*

Langkah selanjutnya adalah mencari bukti foto dan video yang telah dihapus oleh pelaku. Berdasarkan hasil ekstrak didapatkan foto dan video pada aplikasi *Google Drive* seperti pada Gambar 5

dan Gambar 6. Ditemukan folder foto dan video hasil dari ekstrak menggunakan aplikasi *MobileEdit Forensics* dan *Magnet AXIOM* pada gambar dibawah ini.



Gambar 5. Barang Bukti foto *Magnet AXIOM & MobileEdit Forensics*



Gambar 6. Barang Bukti Video *Magnet AXIOM & MobileEdit Forensics*

Bukti diatas didapatkan melalui proses investigasi mendapatkan 2 buah barang bukti digital berupa 1 buah foto seorang wanita yang sedang berpakaian dan berpose seksi, juga ditemukan 1 buah video perempuan melakukan kegiatan yang memiliki unsur pornografi.

### 3.5 Reporting

Setelah melakukan akuisisi pada barang bukti yang ditemukan, dapat disimpulkan bahwa melakukan proses forensik pada *Android* maka bukti yang berkaitan berhasil dikumpulkan. Berdasarkan hasil simulasi yang dilakukan, berhasil menemukan bukti digital penyebaran dan unggahan foto dan video yang dilakukan oleh pelaku. Setelah dilakukan akuisisi terhadap aplikasi *Google Drive* Menggunakan *MobileEdit Forensic* dan *Magnet AXIOM* diketahui memiliki efisiensi yang tinggi pada hasil ekstraksi, dan sama – sama mendapatkan barang bukti digital pada *smartphone* pelaku.

Tabel 1. Hasil Ekstraksi

Informasi	MobileEdit Forensic	Magnet AXIOM
Versi Aplikasi	7.4.1.21502	5.4.0.26185
Email	masfuad69@gmail.com	masfuad69@gmail.com
Waktu Kejadian	Didapatkan	Didapatkan
Foto	Didapatkan 1 foto	Didapatkan 1 foto
Video	Didapatkan 1video	Didapatkan 1video

#### 4. Kesimpulan

Berdasarkan hasil pembahasan diatas, *framework NIJ* menggunakan *tools MobilEdit Forensics* dan *Magnet AXIOM* mampu melakukan pengumpulan data forensik pada salah satu aplikasi *cloud storage android* khususnya *Google Drive*. Hasil yang diperoleh dari penelitian tersebut dapat digunakan oleh Penyidik sebagai alat bukti pendukung dalam penanganan perkara pidana dan menjadi rujukan dalam pencarian alat bukti dalam perkara pidana pornografi pada aplikasi *Google Drive*. *MobileEdit Forensic* dan *Magnet AXIOM* memperoleh semua bukti yang telah dihapus oleh pelaku.

#### Daftar Pustaka

- [1] K. E. Tria Sutrisna, "Polisi Sita Akun 'Google Drive' Milik Dea yang Diduga Berisi Video Pornografi," *Kompas*, 2022. <https://megapolitan.kompas.com/read/2022/04/02/11181271/polisi-sita-akun-google-drive-milik-dea-yang-diduga-berisi-video#> (accessed Jan. 23, 2024).
- [2] 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.
- [3] A.- Ahmadi, "Akuisisi Data Forensik Google Drive Pada Android Dengan Metode National Institute of Justice ( NIJ )," *J. CoreIT J. Has. Penelit. Ilmu Komput. dan Teknol. Inf.*, vol. 4, no. 1, p. 8, 2018, doi: 10.24014/coreit.v4i1.5803.
- [4] I. P. D. I. Putra and I. K. G. Suhartana, "Cyberbullying Analysis on WhatsApp Messenger Using the National Institute of Justice (NIJ) Method," *JELIKU (Jurnal Elektron. Ilmu Komput. Udayana)*, vol. 9, no. 4, p. 501, 2021, doi: 10.24843/jlk.2021.v09.i04.p07.
- [5] D. Mualfah, A. Viransa, and H. F. Amran, "Akuisisi Bukti Digital Pada Aplikasi Tamtam Messenger Menggunakan Metode National Institute of Justice," *J. Softw. Eng. Inf. Syst.*, vol. 3, no. 1, 2021, doi: 10.37859/seis.v3i1.4548.
- [6] I. G. N. Guna Wicaksana and I. K. Gede Suhartana, "Forensic Analysis of Telegram Desktop-based Applications using the National Institute of Justice (NIJ) Method," *JELIKU (Jurnal Elektron. Ilmu Komput. Udayana)*, vol. 8, no. 4, p. 381, 2020, doi: 10.24843/jlk.2020.v08.i04.p03.
- [7] S. R. A. Ardiningtias, S. Sunardi, and H. Herman, "Investigasi Digital Pada Facebook Messenger Menggunakan National Institute of Justice," *J. Inform. Polinema*, vol. 7, no. 4, pp. 19–26, 2021, doi: 10.33795/jip.v7i4.709.
- [8] H. Nurhairani and I. Riadi, "Analysis Mobile Forensics on Twitter Application using the National Institute of Justice (NIJ) Method," *Int. J. Comput. Appl.*, vol. 177, no. 27, pp. 35–42, 2019, doi: 10.5120/ijca2019919749.
- [9] C. Putra, I. W., Suharso, A., Rozikin, "Akuisisi bukti digital dan deteksi keaslian citra pada whatsapp menggunakan metode NIST dan ELA," *J. Sains Komput. Inform.*, vol. 5, no. 2, pp. 1–15, 2021.
- [10] F. A. S. Yuyun Dwi Lestari, Yessi Fitri Annisah Lubis, "Analisis Perbandingan Kinerja Root Explorer Dan Oxygen Forensic Detective Pada Forensic Digital," *J. Syntax Fusion*, vol. 3, no. 08, pp. 1–14, 2023, doi: <https://doi.org/10.54543/fusion.v3i05.350>.
- [11] A. M. Afdal, Y. Salim, and A. R. Manga, "Analisis Bukti Digital Forensik Pada Discord Menggunakan Metode National Institute of Standards Technology," *Bul. Sist. Inf. dan Teknol. Islam*, vol. 3, no. 4, pp. 293–300, 2022, doi: 10.33096/busiti.v3i4.1425.
- [12] I. R. Roni Anggara Putra, Abdul Fadlil, "Forensik Mobile Pada Smartwatch Berbasis Android," *JURTI*, vol. 1, no. 1, pp. 43–47, 2017.
- [13] M. N. Faiz, R. Umar, and A. Yudhana, "Implementasi Live Forensics untuk Perbandingan Browser pada Keamanan Email," *JISKA (Jurnal Inform. Sunan Kalijaga)*, vol. 1, no. 3, pp. 108–114, 2017, doi: 10.14421/jiska.2017.13-02.
- [14] S. Marcellino, H. B. Seta, and I. W. Widi, "Analisis Forensik Digital Recovery Data Smartphone pada Kasus Penghapusan Berkas Menggunakan Metode National Institute of Justice (NIJ)," *Inform. J. Ilmu Komput.*, vol. 19, no. 2, pp. 141–156, 2023, doi: 10.52958/iftk.v19i2.4676.
- [15] R. A. Bintang, R. Umar, and A. Yudhana, "Analisis Media Sosial Facebook Lite dengan tools Forensik menggunakan Metode NIST," *Techno (Jurnal Fak. Tek. Univ. Muhammadiyah Purwokerto)*, vol. 21, no. 2, p. 125, 2020, doi: 10.30595/techno.v21i2.8494.
- [16] N. Nasirudin, S. Sunardi, and I. Riadi, "Analisis Forensik Smartphone Android Menggunakan Metode NIST dan Tool MOBILedit Forensic Express," *J. Inform. Univ. Pamulang*, vol. 5, no. 1, p. 89, 2020, doi: 10.32493/informatika.v5i1.4578.