

Investigasi Forensik Digital Artefak WhatsApp pada Skenario Penipuan Mengatasnamakan Bank BRI Menggunakan Metode NIJ

Silva Ayu Andesti¹, Fahmi Fachri²

^{1,2} Program Studi Teknik Informatika, Universitas Ma'arif Nahdlatul Ulama Kebumen
e-mail: silvaayuandesti4@gmail.com

Abstrak

WhatsApp merupakan aplikasi pesan instan yang berpotensi menyimpan artefak penting dalam investigasi forensik digital. Penelitian ini bertujuan menerapkan metode *National Institute of Justice* (NIJ) untuk menginvestigasi artefak WhatsApp pada skenario simulasi penipuan yang mengatasnamakan Bank BRI. Penelitian menggunakan pendekatan studi kasus forensik digital berbasis simulasi pada perangkat Samsung J2 Android 5.1.1 dalam kondisi *root* dengan WhatsApp versi 2.26.23.73. Artefak target terdiri atas 20 pesan teks, 10 pesan suara, 4 foto, 4 video, dan 2 tautan palsu yang dihapus dari antarmuka aplikasi. Proses investigasi dilakukan melalui tahapan identification, collection, examination, analysis, dan reporting menggunakan *MOBILedit Forensic Express* v10.1, *Autopsy* v4.19.3, dan *FTK Imager* v4.5. Hasil penelitian menunjukkan bahwa 26 dari 40 artefak berhasil ditemukan kembali dengan tingkat recovery 65%. Perbandingan tools menunjukkan MOBILedit Forensic menemukan 21 artefak atau 52,5%, *Autopsy* 20 artefak atau 50%, dan *FTK Imager* 12 artefak atau 30%. Temuan per tools tidak dijumlahkan sebagai artefak unik karena berpotensi tumpang tindih. Hasil penelitian menunjukkan bahwa metode NIJ dapat digunakan secara sistematis dalam investigasi artefak WhatsApp terhapus.

Kata Kunci: Forensik Digital, Whatsapp, NIJ, Artefak Digital, Recovery Artefak

Abstract

WhatsApp is an instant messaging application that may contain artefacts of significance in digital forensic investigations. This study aims to apply the National Institute of Justice (NIJ) methodology to investigate WhatsApp artefacts in a simulated fraud scenario impersonating Bank BRI. The research utilised a simulation-based digital forensic case study approach on a rooted Samsung J2 device running Android 5.1.1 with WhatsApp version 2.26.23.73. The target artefacts comprised 20 text messages, 10 voice messages, 4 photos, 4 videos, and 2 fake links that had been deleted from the app interface. The investigation process was carried out through the stages of identification, collection, examination, analysis, and reporting using *MOBILedit Forensic Express* v10.1, *Autopsy* v4.19.3, and *FTK Imager* v4.5. The results of the study showed that 26 out of 40 artefacts were successfully recovered, with a recovery rate of 65 per cent. A comparison of the tools showed that MOBILedit Forensic

recovered 21 artefacts (52.5 per cent), Autopsy 20 artefacts (50 per cent), and FTK Imager 12 artefacts (30 per cent). The findings per tool were not aggregated as unique artefacts due to the potential for overlap. The research results indicate that the NIJ method can be used systematically in the investigation of deleted WhatsApp artefacts.

Keywords : Digital Forensics, Whatsapp, NIJ, Digital Artifacts, Artifact Recovery

LATAR BELAKANG

Perkembangan teknologi informasi dan komunikasi telah mendorong perubahan besar dalam pola interaksi masyarakat. Aktivitas komunikasi, transaksi, dan pertukaran informasi kini banyak dilakukan melalui perangkat mobile dan aplikasi pesan instan (Qibriya et al., 2021). Kondisi tersebut memberikan kemudahan bagi pengguna, tetapi pada saat yang sama membuka peluang terjadinya penyalahgunaan teknologi dalam bentuk kejahatan digital. Salah satu bentuk kejahatan digital yang sering ditemukan adalah penipuan berbasis pesan instan dengan memanfaatkan teknik manipulasi sosial atau social engineering (Sahara & Kuswandi, 2025).

WhatsApp menjadi salah satu aplikasi pesan instan yang banyak digunakan karena mendukung pengiriman pesan teks, suara, gambar, video, dokumen, dan tautan secara cepat. Karakter komunikasi WhatsApp yang bersifat personal membuat aplikasi ini sering dimanfaatkan dalam berbagai skenario penipuan digital. Pada modus penipuan yang mengatasnamakan institusi perbankan, akun pengirim dapat menggunakan identitas palsu untuk membangun kepercayaan akun penerima. Pesan yang dikirim biasanya berisi instruksi tertentu, tautan palsu, file media, atau informasi yang diarahkan untuk memengaruhi tindakan akun penerima (Muallafah et al., 2023; Raharja et al., 2024).

Permasalahan utama dalam penanganan penipuan berbasis WhatsApp terletak pada proses pembuktian digital. Bukti digital seperti pesan teks, pesan suara, foto, video, tautan, metadata, dan database aplikasi bersifat mudah berubah, mudah dihapus, serta rentan kehilangan konteks apabila tidak ditangani dengan prosedur yang tepat. Penghapusan artefak dari antarmuka aplikasi tidak selalu berarti data tersebut hilang sepenuhnya dari perangkat. Oleh karena itu, pendekatan forensik digital diperlukan untuk mengidentifikasi, mengumpulkan, memeriksa, menganalisis, dan melaporkan artefak digital secara sistematis agar tetap dapat dipertanggungjawabkan (Rully, 2004; Setiawan & Hartiwiningsih, 2025).

Dalam konteks investigasi forensik digital, metode *National Institute of Justice* (NIJ) dapat digunakan sebagai kerangka kerja yang terstruktur. Metode NIJ mencakup tahapan identification, collection, examination, analysis, dan reporting yang berfungsi untuk menjaga alur pemeriksaan bukti digital. Tahap identification digunakan untuk menentukan perangkat, aplikasi, dan artefak target yang relevan dengan skenario penelitian. Tahap collection, examination, analysis, dan reporting kemudian digunakan untuk memperoleh data, memeriksa artefak, menafsirkan temuan, serta menyajikan hasil investigasi dalam bentuk laporan forensik (Mursyid et al., 2025; Shabira & Fachri, 2025).

Beberapa penelitian sebelumnya telah membahas forensik digital pada aplikasi pesan instan dan perangkat mobile. Namun, kajian yang secara khusus menguji pemulihan

artefak WhatsApp terhapus pada skenario penipuan yang mengatasnamakan institusi perbankan masih perlu diperkuat. Sebagian penelitian lebih banyak membahas aspek umum kejahatan siber, literasi digital, atau perlindungan hukum, sedangkan pembahasan teknis mengenai artefak WhatsApp, struktur database, file media, tautan palsu, dan recovery artefak masih terbatas. Kondisi ini menunjukkan adanya kebutuhan untuk melakukan penelitian yang lebih terarah pada aspek teknis forensik digital berbasis skenario simulasi (Daraghmi et al., 2023; Rosita, 2023; Utami et al., 2021).

Penelitian ini dilakukan untuk menganalisis investigasi forensik digital artefak WhatsApp pada skenario simulasi penipuan mengatasnamakan Bank BRI menggunakan metode NIJ. Skenario penelitian menggunakan akun uji WhatsApp pada perangkat Samsung J2 Android 5.1.1 dalam kondisi *root*, dengan artefak target berupa 20 pesan teks, 10 pesan suara, 4 foto, 4 video, dan 2 tautan palsu. Setelah skenario komunikasi dilakukan, seluruh artefak dihapus dari aplikasi untuk menguji kemungkinan pemulihan bukti digital. Penelitian ini menggunakan *MOBILedit Forensic Express v10.1*, *Autopsy v4.19.3*, dan *FTK Imager v4.5* sebagai perangkat lunak forensik untuk membantu proses ekstraksi, pemeriksaan, analisis, dan validasi artefak digital.

Berdasarkan uraian tersebut, penelitian ini berfokus pada dua tujuan utama. Pertama, menerapkan metode NIJ dalam investigasi forensik digital pada skenario penipuan berbasis WhatsApp yang mengatasnamakan Bank BRI. Kedua, mengidentifikasi artefak digital WhatsApp yang masih dapat ditemukan setelah proses penghapusan, meliputi pesan teks, pesan suara, foto, video, tautan palsu, database, metadata, dan informasi pendukung lainnya. Hasil penelitian ini diharapkan dapat memberikan gambaran teknis mengenai proses pemulihan artefak WhatsApp serta memperkuat pemahaman tentang pentingnya prosedur forensik digital dalam penanganan bukti elektronik.

METODE

Penelitian ini menggunakan pendekatan studi kasus forensik digital berbasis simulasi. Pendekatan ini dipilih karena penelitian tidak dilakukan pada perkara hukum nyata, melainkan pada skenario terkontrol yang dirancang untuk menggambarkan proses investigasi artefak digital WhatsApp. Skenario simulasi digunakan agar proses penelitian dapat dilakukan secara sistematis, etis, dan dapat direplikasi. Kerangka kerja yang digunakan dalam penelitian ini adalah metode *National Institute of Justice* (NIJ) yang terdiri atas tahapan *identification*, *collection*, *examination*, *analysis*, dan *reporting*.

Penelitian ini bersifat deskriptif. Data hasil pemeriksaan forensik dijelaskan berdasarkan jenis artefak, sumber artefak, status temuan, *tools* yang digunakan, serta relevansinya terhadap proses investigasi digital. Pendekatan deskriptif digunakan karena penelitian ini tidak bertujuan menguji hubungan statistik antarvariabel, tetapi menjelaskan proses pemeriksaan dan pemulihan artefak digital WhatsApp setelah data dihapus dari antarmuka aplikasi (Sugiyono, 2023).

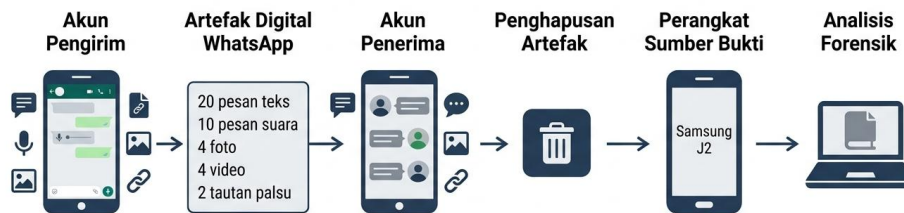
A. Skenario

Skenario penelitian dibuat untuk menggambarkan alur kejadian digital pada aplikasi WhatsApp di perangkat Android. Skenario ini berfokus pada aktivitas pengiriman pesan simulasi, penerimaan artefak digital, penghapusan artefak dari aplikasi, serta proses

pemeriksaan forensik terhadap data yang masih dapat ditemukan pada perangkat. Akun yang digunakan merupakan akun uji, bukan akun pribadi atau akun yang berasal dari perkara hukum nyata.

Skenario dimulai dari penggunaan aplikasi WhatsApp biasa versi 2.26.23.73 pada perangkat Samsung J2 dengan sistem operasi Android 5.1.1 dalam kondisi *root*. Akun pengirim mengirimkan artefak digital kepada akun penerima berupa pesan teks, pesan suara, foto, video, dan tautan palsu yang merepresentasikan pola penipuan mengatasnamakan Bank BRI. Setelah seluruh artefak dikirim, artefak tersebut dihapus dari antarmuka aplikasi WhatsApp. Penghapusan ini dilakukan untuk mensimulasikan kondisi ketika artefak digital tidak lagi terlihat secara langsung pada aplikasi.

Setelah proses penghapusan dilakukan, perangkat sumber bukti dianalisis menggunakan *tools* forensik digital. Proses ini bertujuan untuk mengetahui artefak apa saja yang masih dapat diidentifikasi setelah penghapusan dilakukan. Alur skenario penelitian ditampilkan pada Gambar 1.



Gambar 1. Skenario Simulasi Forensik Digital WhatsApp

B. Alat dan Bahan Penelitian

Alat dan bahan penelitian terdiri atas perangkat keras, perangkat lunak, dan data uji. Perangkat keras digunakan sebagai sumber bukti digital dan media analisis. Perangkat lunak digunakan untuk proses ekstraksi, pemeriksaan, analisis, dan validasi artefak digital. Data uji dalam penelitian ini adalah artefak WhatsApp yang dibuat untuk keperluan simulasi, sehingga tidak berasal dari data pribadi, data nasabah, atau perkara hukum nyata.

MOBILedit Forensic Express digunakan untuk melakukan ekstraksi data dari perangkat Android, terutama data aplikasi dan komunikasi WhatsApp. *Autopsy* digunakan untuk memeriksa hasil ekstraksi, menelusuri struktur folder, mengindeks file, serta membantu analisis artefak digital. *FTK Imager* digunakan sebagai *tools* pendukung apabila diperlukan untuk dokumentasi integritas, pratinjau file, atau pemeriksaan data hasil akuisisi. Alat dan bahan yang digunakan dalam penelitian ditampilkan pada Tabel 1.

Table 1. Alat dan Bahan Penelitian

Perangkat / Bahan	Spesifikasi
Perangkat	Samsung J2 versi 5.1.1
Kondisi	<i>Root</i>
Aplikasi	WhatsApp versi 2.26.23.73

Jenis Akun	Akun Uji
Laptop/PC	ASUS, Windows 10
Kabel data / USB	-
<i>Tool Forensic</i>	<i>MOBILedit Forensic Express</i> versi 10.1
<i>Tool Forensic</i>	<i>Autopsy</i> Versi 4.19.3
<i>Tool Forensic</i>	<i>FTK Imager</i> versi 4.5

C. Parameter Artefak Digital

Parameter artefak digital ditentukan untuk membatasi jenis bukti yang dicari selama proses pemeriksaan. Parameter ini digunakan sebagai dasar untuk menentukan apakah suatu data memiliki relevansi dengan skenario penelitian. Artefak utama yang menjadi target pemeriksaan terdiri atas pesan teks, pesan suara, foto, video, dan tautan palsu. Selain itu, penelitian juga memperhatikan artefak pendukung berupa database WhatsApp, metadata, *timestamp*, struktur folder media, dan nilai *hash* apabila tersedia.

Penentuan parameter artefak penting dilakukan agar proses pemeriksaan tidak melebar ke data lain yang tidak berkaitan dengan skenario. Setiap artefak target memiliki fungsi investigatif yang berbeda. Pesan teks digunakan untuk melihat pola komunikasi, pesan suara digunakan untuk melihat instruksi berbasis audio, foto dan video digunakan sebagai media pendukung, sedangkan tautan palsu digunakan untuk melihat indikasi pengalihan akun penerima ke halaman tertentu dalam skenario. Parameter barang bukti digital WhatsApp ditampilkan pada Tabel 2.

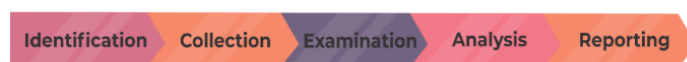
Table 2. Parameter Artefak Digital WhatsApp

Parameter	Keterangan
Informasi aplikasi	WhatsApp biasa versi 2.26.23.73
Informasi akun	Akun uji yang digunakan dalam skenario penelitian
Perangkat sumber bukti	Samsung J2 Android 5.1.1 dalam kondisi <i>root</i>
Pesan teks	20 pesan teks simulasi penipuan
Pesan suara	10 pesan suara berisi instruksi atau komunikasi pendukung
Foto	4 file foto sebagai media pendukung skenario
Video	4 file video sebagai media pendukung komunikasi
Tautan palsu	2 tautan palsu yang digunakan dalam skenario
Database WhatsApp	Database pesan dan kontak yang berkaitan dengan aplikasi WhatsApp
<i>Timestamp</i>	Catatan waktu aktivitas, seperti waktu pengiriman, perubahan, atau akses data

<i>Metadata</i>	Informasi teknis file, seperti ukuran, format, dan properti media
Struktur folder media	Direktori penyimpanan gambar, video, audio, dan file WhatsApp
Nilai <i>hash</i>	Validasi integritas file menggunakan algoritma <i>hash</i> apabila tersedia

D. Tahapan Metode NIJ

Penelitian ini mengikuti tahapan metode *National Institute of Justice* (NIJ), yaitu *identification*, *collection*, *examination*, *analysis*, dan *reporting*. Metode ini digunakan agar proses investigasi digital berjalan runtut, terdokumentasi, dan sesuai dengan prinsip *forensic soundness* (Fadillah et al., 2024; Raharja et al., 2024). Alur penelitian berdasarkan metode NIJ ditampilkan pada Gambar 2.



Gambar 2. Alur Penelitian Berdasarkan Metode NIJ

Tahap pertama adalah *identification*. Pada tahap ini dilakukan penentuan perangkat uji, aplikasi yang dianalisis, skenario penelitian, serta artefak digital yang menjadi target pemeriksaan. Objek yang diidentifikasi meliputi perangkat Samsung J2, sistem operasi Android 5.1.1, kondisi *root*, aplikasi WhatsApp versi 2.26.23.73, akun uji, serta artefak digital yang berkaitan dengan skenario simulasi.

Tahap kedua adalah *collection*. Pada tahap ini dilakukan proses pengumpulan data dari perangkat sumber bukti. Pengumpulan data dilakukan menggunakan *MOBILedit Forensic Express* untuk mengekstraksi data aplikasi WhatsApp dan artefak komunikasi yang tersimpan pada perangkat. Data yang dikumpulkan meliputi database WhatsApp, folder media, pesan, file audio, foto, video, tautan, metadata, dan file lain yang berkaitan dengan skenario. Proses ini dilakukan dengan memperhatikan prinsip kehati-hatian agar data asli tidak berubah selama proses pengambilan bukti.

Tahap ketiga adalah *examination*. Pada tahap ini data hasil ekstraksi diperiksa menggunakan *Autopsy*. Pemeriksaan dilakukan untuk memilah data yang relevan dengan skenario penelitian. Proses pemeriksaan meliputi penelusuran struktur folder WhatsApp, pemeriksaan database, identifikasi file media, pencarian *timestamp*, pemeriksaan metadata, dan penelusuran tautan yang tersimpan pada artefak komunikasi atau file pendukung.

Tahap keempat adalah *analysis*. Pada tahap ini artefak yang berhasil diidentifikasi dianalisis berdasarkan keterkaitannya dengan skenario simulasi. Analisis dilakukan dengan melihat hubungan antara artefak, waktu aktivitas, lokasi penyimpanan, informasi file, pesan, tautan, dan metadata. Hasil analisis digunakan untuk menjelaskan nilai forensik artefak serta mendukung rekonstruksi aktivitas komunikasi pada aplikasi WhatsApp.

Tahap kelima adalah *reporting*. Pada tahap ini hasil pemeriksaan disusun dalam bentuk uraian deskriptif, tabel, grafik, dan dokumentasi gambar. Penyajian hasil dilakukan agar proses investigasi dapat dipahami secara jelas dan dapat ditelusuri kembali. Tahap

pelaporan juga digunakan untuk menyusun hasil penelitian secara sistematis berdasarkan temuan artefak digital yang diperoleh.

E. Teknik Analisis Data

Teknik analisis data dilakukan secara deskriptif dan kuantitatif sederhana. Analisis deskriptif digunakan untuk menjelaskan jenis artefak, sumber artefak, status temuan, *tools* yang digunakan, serta fungsi forensiknya dalam skenario penelitian. Setiap artefak diklasifikasikan berdasarkan kategori yang telah ditentukan pada parameter artefak digital. Klasifikasi ini membantu peneliti membedakan artefak utama dan artefak pendukung dalam proses investigasi.

Analisis kuantitatif sederhana digunakan untuk menghitung persentase keberhasilan pemulihan artefak. Perhitungan dilakukan dengan membandingkan jumlah artefak yang ditemukan dengan jumlah artefak target pada setiap kategori (Fadillah et al., 2024; Muallaf et al., 2023; Raharja et al., 2024). Persentase keberhasilan pemulihan artefak dihitung menggunakan rumus berikut:

$$P_{on} = \frac{\sum P_n}{\sum P_o} \times 100\% \quad (1)$$

Dimana:

P_{on} = Presentase Kinerja Tools

$\sum P_o$ = Total data digital aplikasi WhatsApp

$\sum P_n$ = Total data Digital yang berhasil diperoleh

Perhitungan tersebut digunakan sebagai pendukung analisis deskriptif. Hasil perhitungan tidak digunakan untuk uji statistik inferensial, tetapi untuk memberikan gambaran tingkat keberhasilan proses pemulihan artefak digital WhatsApp. Angka hasil pemulihan dan interpretasinya disajikan pada bagian Hasil dan Pembahasan.

F. Validasi Integritas Bukti Digital

Validasi integritas bukti digital dilakukan untuk memastikan bahwa artefak yang dianalisis tidak mengalami perubahan selama proses penelitian. Validasi dapat dilakukan melalui pencatatan nilai *hash* pada file hasil ekstraksi atau artefak digital yang berhasil diperoleh. Nilai *hash* awal dibandingkan dengan nilai *hash* akhir untuk memastikan konsistensi file. Apabila nilai *hash* awal dan akhir sama, maka artefak dapat dinyatakan tidak mengalami perubahan selama proses pemeriksaan (Fadillah et al., 2024).

Selain pencatatan nilai *hash*, penelitian ini juga menerapkan dokumentasi tindakan forensik melalui prinsip *chain of custody*. Dokumentasi dilakukan dengan mencatat aktivitas pemeriksaan, waktu pemeriksaan, perangkat yang digunakan, *tools* yang digunakan, tindakan yang dilakukan, dan output yang diperoleh. Langkah ini dilakukan agar proses investigasi memiliki keterlacakan yang baik dan dapat dipertanggungjawabkan secara teknis.

Etika penelitian dijaga dengan menggunakan akun uji dan data simulasi. Penelitian ini tidak menggunakan data pribadi, data nasabah, atau data yang berasal dari perkara hukum nyata. Istilah akun pengirim dan akun penerima digunakan untuk menggantikan penyebutan

pihak yang berpotensi menimbulkan kesan tuduhan. Informasi sensitif seperti nomor telepon, identitas akun, dan tautan simulasi perlu disamarkan dalam penyajian hasil penelitian.

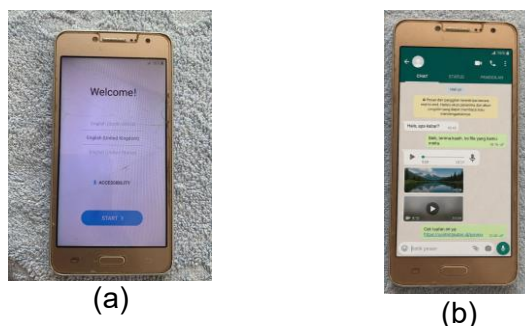
HASIL DAN PEMBAHASAN

Bagian ini menyajikan hasil penerapan metode *National Institute of Justice* (NIJ) dalam investigasi artefak digital WhatsApp pada skenario simulasi penipuan yang mengatasnamakan Bank BRI. Pembahasan disusun berdasarkan tahapan NIJ, yaitu *identification*, *collection*, *examination*, *analysis*, dan *reporting*. Setiap tahapan menjelaskan temuan yang diperoleh dari proses investigasi serta makna forensiknya. Penyajian hasil dilakukan dalam bentuk uraian deskriptif, tabel, dan grafik agar alur temuan dapat dipahami secara sistematis.

A. Identification

Tahap *identification* dilakukan untuk memastikan bahwa perangkat, aplikasi, akun uji, dan artefak target telah sesuai dengan skenario penelitian. Hasil identifikasi menunjukkan bahwa perangkat yang digunakan adalah Samsung J2 dengan sistem operasi Android 5.1.1 dalam kondisi *root*. Aplikasi yang dianalisis adalah WhatsApp biasa versi 2.26.23.73. Akun yang digunakan merupakan akun uji, sehingga data yang dianalisis tidak berasal dari akun pribadi atau perkara hukum nyata.

Perangkat tersebut digunakan sebagai sumber bukti digital karena menyimpan aktivitas komunikasi yang dibuat dalam skenario penelitian. Artefak target terdiri atas pesan teks, pesan suara, foto, video, dan tautan palsu. Seluruh artefak tersebut dikirim melalui WhatsApp, kemudian dihapus dari antarmuka aplikasi sebelum proses akuisisi dilakukan. Dokumentasi identifikasi perangkat dan aplikasi ditampilkan pada Gambar 3.

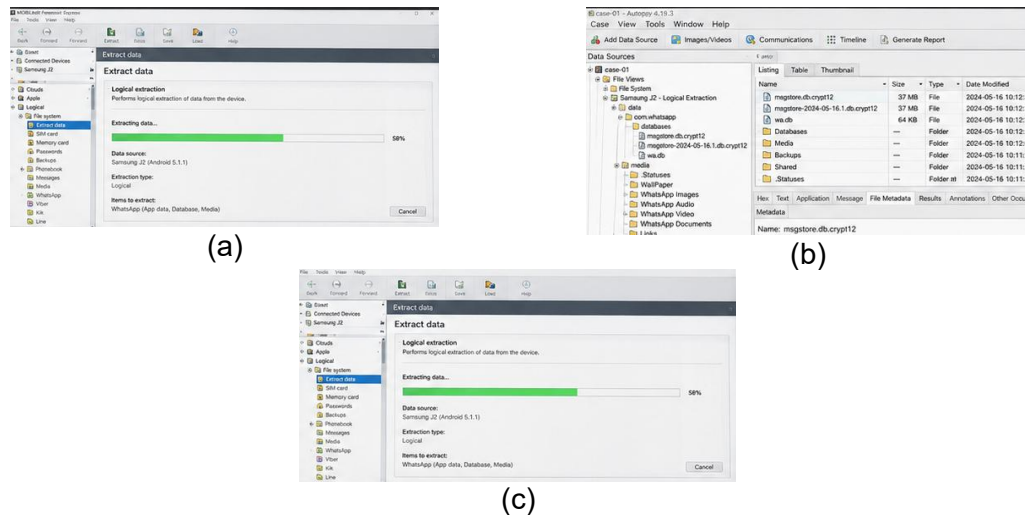


Gambar 3. Identifikasi Perangkat dan Aplikasi TikTok

(a) Perangkat Samsung J2 (b) Salah satu bahan uji pada aplikasi WhatsApp

B. Collection

Tahap *collection* dilakukan untuk mengumpulkan data dari perangkat sumber bukti. Proses pengumpulan data dilakukan menggunakan *MOBILedit Forensic Express* v10.1 dan didukung oleh *FTK Imager* v4.5 untuk kebutuhan pratinjau, dokumentasi integritas, atau pemeriksaan file tertentu apabila diperlukan. Data hasil pengumpulan kemudian diperiksa lebih lanjut menggunakan *Autopsy* v4.19.3. Dokumentasi penggunaan tools forensik ditampilkan pada Gambar 4.



Gambar 4. Penggunaan Tools Forensik dalam Pemeriksaan Artefak WhatsApp
 (a) Menggunakan MOBILedit forensik (b) Menggunakan Autopsy (c) Menggunakan FTK Imager

Pada tahap ini, data yang dikumpulkan meliputi database WhatsApp, struktur folder media, file pesan suara, foto, video, tautan palsu, serta artefak pendukung lain yang berkaitan dengan aktivitas komunikasi. Hasil *collection* menunjukkan bahwa database utama WhatsApp berhasil diekstrak. Database yang diperoleh meliputi msgstore.db sebagai sumber utama riwayat pesan dan wa.db sebagai database kontak WhatsApp. Selain database, struktur folder media WhatsApp juga berhasil dipetakan, termasuk folder WhatsApp Images, WhatsApp Video, dan WhatsApp Voice Notes. Hasil pengumpulan data pada tahap *collection* ditampilkan pada Tabel 3.

Table 3. Hasil Pengumpulan Data pada Tahap Collection

Jenis Data	Sumber/Tools	Status Pengumpulan	Keterangan
Database pesan	MOBILedit Forensic	Terkumpul	msgstore.db berhasil diekstrak
Database kontak	MOBILedit Forensic	Terkumpul	wa.db berhasil diekstrak
Folder media WhatsApp	FTK Imager	Terkumpul	Struktur folder media berhasil dipetakan
File pesan suara	FTK Imager	Terkumpul sebagian	Beberapa file audio berhasil ditemukan
File foto	FTK Imager	Terkumpul sebagian	Beberapa file gambar berhasil ditemukan

File video	FTK <i>Imager</i>	Terkumpul sebagian	Beberapa file video berhasil ditemukan
Tautan palsu	<i>Autopsy</i>	Terkumpul	Tautan ditemukan pada isi percakapan dan jejak pendukung
File validasi	MOBILedit Forensic	Terkumpul	Digunakan untuk pemeriksaan integritas data

Hasil pada Tabel 3 menunjukkan bahwa tahap *collection* tidak hanya menghasilkan data percakapan, tetapi juga artefak pendukung berupa database, file media, dan struktur folder WhatsApp. Hal ini menunjukkan bahwa penghapusan artefak dari antarmuka aplikasi tidak selalu menghapus seluruh jejak digital dari perangkat. Data hasil pengumpulan kemudian menjadi dasar untuk tahap *examination*.

C. Examination

Tahap *examination* dilakukan untuk memeriksa data hasil akuisisi dan ekstraksi. Pemeriksaan dilakukan dengan menelusuri database WhatsApp, struktur folder media, file audio, foto, video, tautan, dan metadata yang berkaitan dengan skenario penelitian. *Autopsy* v4.19.3 digunakan untuk membantu proses pemeriksaan terhadap struktur file dan artefak hasil ekstraksi. Artefak yang tidak berkaitan dengan skenario dipisahkan agar proses analisis lebih terarah.

Hasil pemeriksaan menunjukkan bahwa beberapa artefak digital masih dapat ditemukan setelah proses penghapusan dilakukan. Pesan teks ditemukan dalam bentuk teks utuh pada database WhatsApp, sedangkan sebagian pesan suara, foto, dan video ditemukan melalui folder media atau hasil pemeriksaan file. Tautan palsu ditemukan secara utuh pada isi percakapan dan jejak pendukung. Hasil pemeriksaan artefak digital WhatsApp ditampilkan pada Tabel 4.

Table 4. Hasil Pemeriksaan Artefak Digital WhatsApp

Artefak Digital	Target	Keterangan Kondisi Artefak
Database WhatsApp	-	msgstore.db dan wa.db berhasil diekstrak
Pesan teks	20	Sebagian pesan berhasil dipulihkan dalam bentuk teks utuh
Pesan suara	10	Sebagian file audio berhasil ditemukan, sebagian lain tidak terbaca
Foto	4	Sebagian file gambar berhasil diidentifikasi
Video	4	Sebagian file video berhasil ditemukan
Tautan Palsu	2	Tautan ditemukan secara utuh
Struktur folder media	-	Folder WhatsApp Images, WhatsApp Video, dan WhatsApp Voice Notes berhasil dipetakan
Meta data dan <i>timestamp</i>	-	Digunakan untuk mendukung rekonstruksi aktivitas

Berdasarkan Tabel 4, artefak yang telah dihapus masih meninggalkan jejak pada perangkat. Database WhatsApp menjadi artefak penting karena menyimpan informasi pesan dan kontak yang berkaitan dengan komunikasi dalam skenario penelitian. File media juga memiliki nilai forensik karena dapat mendukung pembuktian bahwa komunikasi tidak hanya dilakukan melalui teks, tetapi juga melalui pesan suara, foto, video, dan tautan. Temuan ini menunjukkan bahwa pemeriksaan forensik pada WhatsApp perlu dilakukan secara menyeluruh, tidak hanya pada tampilan aplikasi.

D. Analysis

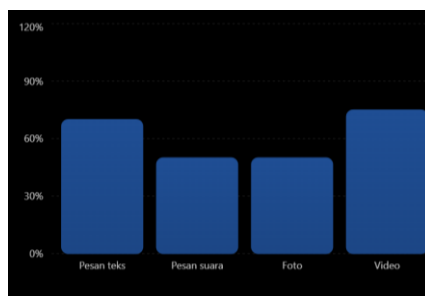
Tahap *analysis* dilakukan untuk menafsirkan artefak yang telah ditemukan pada tahap pemeriksaan. Analisis diarahkan untuk mengetahui tingkat keberhasilan pemulihan artefak dan nilai forensik dari setiap jenis artefak. Dari 40 artefak target yang digunakan dalam skenario, sebanyak 26 artefak berhasil ditemukan kembali. Dengan demikian, tingkat keberhasilan *recovery* keseluruhan adalah 65%.

Hasil pemulihan menunjukkan bahwa artefak yang paling tinggi tingkat keberhasilannya adalah tautan palsu, yaitu 2 dari 2 tautan berhasil ditemukan. Artefak video memiliki tingkat keberhasilan 75%, yaitu 3 dari 4 video berhasil ditemukan. Pesan teks memiliki tingkat keberhasilan 70%, yaitu 14 dari 20 pesan berhasil dipulihkan. Pesan suara dan foto masing-masing memiliki tingkat keberhasilan 50%. Rekapitulasi hasil *recovery* artefak WhatsApp ditampilkan pada Tabel 5.

Table 5. Persentase Keberhasilan Recovery Artefak WhatsApp

Artefak	Target	Ditemukan	Tidak ditemukan	Persentase Recovery
Pesan teks	20	14	6	70%
Pesan suara	10	5	5	50%
Foto	4	2	2	50%
Video	4	3	1	75%
Tautan palsu	2	2	0	100%

Untuk memperjelas distribusi tingkat keberhasilan pemulihan artefak, hasil tersebut divisualisasikan pada Gambar 5.



Gambar 5. Grafik Persentase Recovery Artefak WhatsApp

Berdasarkan Tabel 5 dan Gambar 5, tingkat keberhasilan *recovery* berbeda pada setiap kategori artefak. Tautan palsu berhasil ditemukan seluruhnya karena tautan tersebut masih tersimpan dalam isi percakapan atau jejak pendukung yang berkaitan dengan aktivitas komunikasi. Pesan teks memiliki tingkat pemulihan yang cukup tinggi karena sebagian pesan masih dapat ditemukan pada database WhatsApp. Sementara itu, pesan suara dan foto memiliki tingkat pemulihan lebih rendah karena sebagian file tidak terbaca atau struktur datanya tidak lengkap.

Video memiliki tingkat pemulihan sebesar 75%, yaitu 3 dari 4 video berhasil ditemukan. Temuan ini menunjukkan bahwa file media berukuran besar masih memiliki peluang untuk dipulihkan apabila struktur file atau kluster penyimpanannya belum sepenuhnya tertimpa data baru. Namun, satu video tidak berhasil dipulihkan karena kemungkinan mengalami kerusakan struktur atau tertimpa data lain. Kondisi ini memperlihatkan bahwa keberhasilan pemulihan artefak media sangat dipengaruhi oleh kondisi penyimpanan perangkat setelah proses penghapusan dilakukan.

E. Perbandingan Tools Forensik

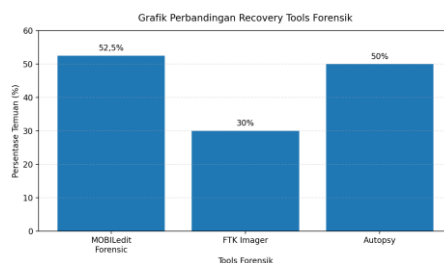
Perbandingan tools forensik dilakukan untuk melihat kontribusi masing-masing perangkat lunak dalam proses investigasi artefak WhatsApp. Setiap tools memiliki fokus kerja yang berbeda sehingga hasil temuannya tidak dapat dipahami sebagai data yang sepenuhnya berdiri sendiri. MOBILedit Forensic berperan pada proses ekstraksi logis database dan struktur chat WhatsApp. FTK *Imager* berperan dalam pemeriksaan file media, file carving, pratinjau file, serta validasi file tertentu. Sementara itu, *Autopsy* berperan dalam pemeriksaan struktur file, pengindeksan artefak, metadata, dan timeline hasil ekstraksi.

Berdasarkan hasil simulasi, MOBILedit Forensic menemukan 21 artefak dari 40 target artefak, sehingga persentase temuannya sebesar 52,5%. FTK *Imager* menemukan 12 artefak dari 40 target artefak, sehingga persentase temuannya sebesar 30%. *Autopsy* menemukan 20 artefak dari 40 target artefak, sehingga persentase temuannya sebesar 50%. Perbedaan persentase tersebut menunjukkan bahwa setiap tools memiliki ruang kerja dan kemampuan pemeriksaan yang berbeda. Namun, data temuan per tools perlu ditafsirkan secara hati-hati karena artefak yang ditemukan oleh satu tools dapat tumpang tindih dengan artefak yang ditemukan oleh tools lain. Oleh karena itu, jumlah temuan per tools tidak dapat dijumlahkan langsung sebagai artefak unik.

Table 6. Perbandingan Tools Forensik

Tools	Target Artefak	Artefak Ditemukan	Persentase	Fokus Pemeriksaan
MOBILedit forensik	40	21	52,5%	Ekstraksi logis database dan struktur chat
FTK Imager	40	12	30%	Pemeriksaan file media, <i>file carving</i> , dan validasi file
<i>Autopsy</i>	40	20	50%	Pemeriksaan struktur file, indeks artefak, metadata, dan <i>timeline</i>

Untuk memperjelas perbandingan kontribusi temuan antar-tools, hasil tersebut divisualisasikan pada Gambar 6.

**Gambar 6. Grafik Perbandingan Recovery Tools Forensik**

Tabel 6 dan Gambar 6 menunjukkan bahwa MOBILedit Forensic memiliki kontribusi temuan paling tinggi, yaitu 52,5%. Hasil ini menunjukkan bahwa MOBILedit Forensic cukup efektif dalam proses ekstraksi logis artefak WhatsApp, khususnya pada database dan struktur chat. *Autopsy* memiliki kontribusi yang hampir sebanding, yaitu 50%, karena mampu membantu pemeriksaan struktur file, indeks artefak, metadata, dan timeline. FTK *Imager* memiliki persentase temuan sebesar 30% karena perannya lebih dominan sebagai tools pendukung dalam pemeriksaan file media, file carving, pratinjau file, dan validasi file.

Berdasarkan hasil tersebut, penggunaan beberapa tools dalam investigasi forensik digital WhatsApp dapat memberikan hasil yang lebih lengkap dibandingkan penggunaan satu tools saja. MOBILedit Forensic dapat digunakan sebagai tools utama untuk ekstraksi data mobile, *Autopsy* dapat digunakan untuk pemeriksaan dan analisis lanjutan terhadap hasil ekstraksi, sedangkan FTK *Imager* dapat digunakan sebagai tools pendukung untuk pemeriksaan file dan validasi integritas. Dengan demikian, ketiga tools tersebut memiliki fungsi yang saling melengkapi dalam proses investigasi artefak WhatsApp.

F. Validasi Integritas Bukti Digital

Validasi integritas dilakukan untuk memastikan bahwa artefak digital yang diperoleh tidak mengalami perubahan selama proses pemeriksaan. Validasi dilakukan dengan membandingkan nilai *hash* awal dan nilai *hash* akhir pada artefak tertentu. Jika nilai *hash*

awal dan akhir sama, maka artefak dinyatakan memiliki status *match* atau valid. Validasi ini penting karena bukti digital bersifat mudah berubah dan rentan dimodifikasi.

Hasil validasi menunjukkan bahwa beberapa artefak memiliki nilai *hash* awal dan akhir yang sama. Artefak tersebut meliputi database chat, database kontak, *image* perangkat, dan folder media hasil pemeriksaan. Namun, nilai *hash* yang dicantumkan dalam naskah final harus dipastikan berasal dari keluaran asli tools forensik dan memenuhi format yang benar. Untuk MD5, nilai *hash* harus terdiri atas 32 karakter heksadesimal, yaitu angka 0–9 dan huruf a–f.

Table 7. Hasil Validasi Integritas Bukti Digital

Artefak	Tools	Hash Awal	Hash Akhir
msgstore.db	MOBILeditforensik	a1b2c3d4e5f67890abcd ef1237890	a1b2c3d4e5f67890abcdef1 234567890
wa.db	MOBILeditforensik	f9e8d7c6b5a43210fedcb a0987654321	f9e8d7c6b5a43210fedcba0 987654321
Evidence_Smartphone.E01	MOBILeditforensik	7b52009b64fd0a2a49e6 d8a939753073	7b5204fd0a2a49e6d8a939 753073
Folder media hasil pemeriksaan	MOBILeditforensik	5d41402ab2a76b9719d9 11017c592	5d41402abc4b2a76b9719 d911017c592

Berdasarkan Tabel 7, artefak yang memiliki nilai *hash* awal dan akhir yang sama dapat dinyatakan tidak mengalami perubahan selama proses pemeriksaan. Validasi ini memperkuat integritas hasil analisis karena artefak yang diperiksa dapat ditelusuri ke kondisi awal saat diperoleh. Namun, tabel *hash* harus diverifikasi kembali dengan keluaran asli tools sebelum naskah final dikirimkan.

G. Rekonstruksi Kronologi Simulasi

Rekonstruksi kronologi dilakukan untuk menghubungkan artefak digital yang ditemukan dengan urutan aktivitas dalam skenario penelitian. Artefak seperti pesan teks, tautan palsu, pesan suara, foto, video, *timestamp*, dan *cache* digunakan untuk menyusun alur komunikasi. Rekonstruksi ini penting karena nilai forensik artefak tidak hanya terletak pada keberadaannya, tetapi juga pada kemampuannya menjelaskan urutan aktivitas digital. Hasil rekonstruksi kronologi simulasi ditampilkan pada Tabel 8.

Table 8. Rekonstruksi Kronologi Simulasi Berdasarkan Artefak Digital

Urutan Kejadian	Bukti Pendukung	Makna Investigasi
Akun pengirim menghubungi akun penerima menggunakan identitas institusi perbankan	Log pesan teks pertama pada msgstore.db	Menunjukkan awal komunikasi manipulatif dalam skenario
Akun pengirim	Tautan_Phishing_BRI.url dan	Menunjukkan

mengirimkan tautan palsu dan pesan suara	file audio WhatsApp	penggunaan tautan dan komunikasi audio sebagai bagian dari skenario
Akun penerima membuka tautan palsu	Jejak <i>cache</i> dan riwayat akses tautan	Menunjukkan adanya respons terhadap tautan yang dikirim
Akun pengirim mengirim foto atau media pendukung	File gambar hasil pemeriksaan	Menunjukkan penggunaan media untuk memperkuat komunikasi
Artefak komunikasi dihapus dari aplikasi	Fragmen teks, database, dan sisa file media	Menunjukkan adanya proses penghapusan artefak dari antarmuka aplikasi

Berdasarkan Tabel 8, artefak digital yang ditemukan dapat digunakan untuk menyusun kembali urutan aktivitas dalam skenario penelitian. Pesan teks dan tautan palsu menjadi artefak utama karena menunjukkan pola komunikasi yang diarahkan pada akun penerima. Pesan suara, foto, dan video berperan sebagai artefak pendukung yang memperkuat konteks komunikasi. Dengan adanya *timestamp* dan struktur file, urutan aktivitas dapat dijelaskan secara lebih sistematis.

H. Reporting

Secara keseluruhan, hasil penelitian menunjukkan bahwa metode NIJ dapat digunakan untuk menyusun alur investigasi artefak WhatsApp secara sistematis. Dari 40 artefak target yang digunakan dalam skenario, 26 artefak berhasil ditemukan kembali dengan tingkat recovery keseluruhan sebesar 65%. Artefak yang ditemukan meliputi pesan teks, pesan suara, foto, video, tautan palsu, database WhatsApp, struktur folder media, metadata, dan timestamp. Temuan ini menunjukkan bahwa penghapusan artefak dari antarmuka WhatsApp tidak selalu menghilangkan seluruh jejak digital dari perangkat.

Hasil penelitian juga menunjukkan bahwa setiap tools memiliki fungsi yang berbeda dalam proses investigasi. MOBILedit Forensic lebih kuat pada proses ekstraksi data mobile, terutama database dan struktur chat WhatsApp. *Autopsy* membantu pemeriksaan struktur file, indeks artefak, metadata, dan timeline. FTK *Imager* berperan sebagai tools pendukung pada aspek pemeriksaan file media, file carving, pratinjau data, dan validasi integritas. Berdasarkan perbandingan hasil temuan, MOBILedit Forensic menemukan 21 artefak dari 40 target artefak atau 52,5%, *Autopsy* menemukan 20 artefak atau 50%, sedangkan FTK *Imager* menemukan 12 artefak atau 30%. Namun, hasil tersebut tidak dijumlahkan sebagai artefak unik karena terdapat kemungkinan tumpang tindih temuan antar-tools.

Temuan ini perlu ditafsirkan secara hati-hati karena penelitian menggunakan skenario simulasi dan perangkat uji tertentu. Hasil pemulihan dapat berbeda apabila penelitian dilakukan pada perangkat lain, versi Android lain, versi WhatsApp lain, atau kondisi perangkat non-root. Selain itu, aktivitas perangkat setelah penghapusan juga dapat memengaruhi peluang pemulihan data karena artefak digital dapat tertimpa oleh data baru. Dengan demikian, hasil penelitian ini memberikan gambaran teknis awal mengenai

pemulihan artefak WhatsApp, tetapi masih dapat dikembangkan pada penelitian lanjutan dengan variasi perangkat dan skenario yang lebih luas.

SIMPULAN

Berdasarkan hasil penelitian yang telah dilakukan, metode *National Institute of Justice* (NIJ) dapat digunakan sebagai alur kerja sistematis dalam investigasi forensik digital pada artefak WhatsApp. Tahapan identification, collection, examination, analysis, dan reporting membantu proses pemeriksaan berjalan lebih terarah, mulai dari penentuan perangkat dan artefak target, pengumpulan data, pemeriksaan artefak, analisis temuan, hingga penyusunan laporan forensik. Penerapan metode ini juga membantu menjaga keterlacakan proses investigasi, terutama karena bukti digital bersifat mudah berubah, mudah dihapus, dan dapat tertimpa oleh data baru.

Hasil penelitian menunjukkan bahwa penghapusan artefak dari antarmuka WhatsApp tidak selalu menghilangkan seluruh jejak digital dari perangkat. Dari 40 artefak target yang digunakan dalam skenario simulasi, 26 artefak berhasil ditemukan kembali dengan tingkat recovery keseluruhan sebesar 65%. Artefak yang berhasil ditemukan meliputi 14 pesan teks, 5 pesan suara, 2 foto, 3 video, dan 2 tautan palsu. Temuan ini menunjukkan bahwa artefak WhatsApp yang telah dihapus masih berpotensi ditemukan melalui proses forensik digital, meskipun tingkat keberhasilannya berbeda pada setiap jenis artefak.

Penggunaan *MOBILedit Forensic Express*, *Autopsy*, dan *FTK Imager* menunjukkan fungsi yang saling melengkapi dalam proses investigasi. *MOBILedit Forensic Express* berperan dalam proses ekstraksi data perangkat mobile, terutama database dan struktur komunikasi WhatsApp. *Autopsy* membantu proses pemeriksaan dan analisis struktur file, indeks artefak, metadata, serta timeline. *FTK Imager* berperan sebagai tools pendukung dalam pemeriksaan file media, file carving, pratinjau file, dan validasi integritas. Berdasarkan hasil perbandingan tools, *MOBILedit Forensic* menemukan 21 artefak dari 40 target artefak atau 52,5%, *Autopsy* menemukan 20 artefak atau 50%, sedangkan *FTK Imager* menemukan 12 artefak atau 30%. Namun, hasil perbandingan tools perlu ditafsirkan secara hati-hati karena setiap tools memiliki fungsi, target artefak, dan ruang kerja yang berbeda, serta memungkinkan adanya tumpang tindih temuan.

Secara umum, penelitian ini menunjukkan bahwa artefak digital WhatsApp memiliki nilai penting dalam rekonstruksi skenario penipuan berbasis pesan instan. Pesan teks dan tautan palsu menjadi artefak utama karena dapat menunjukkan pola komunikasi dan arah tindakan yang disimulasikan. Pesan suara, foto, video, metadata, timestamp, database, dan struktur folder media berperan sebagai artefak pendukung untuk memperkuat kronologi digital. Dengan demikian, pemeriksaan forensik WhatsApp tidak dapat hanya bergantung pada satu jenis artefak atau satu tools, tetapi perlu melihat hubungan antarartefak secara menyeluruh.

Penelitian ini memiliki keterbatasan karena dilakukan pada satu perangkat uji, satu versi Android, satu versi WhatsApp, dan skenario simulasi tertentu. Hasil pemulihan artefak dapat berbeda apabila dilakukan pada perangkat lain, versi aplikasi berbeda, kondisi perangkat non-root, atau aktivitas perangkat yang lebih kompleks setelah penghapusan data. Oleh karena itu, penelitian selanjutnya disarankan untuk menggunakan variasi

perangkat, versi Android, versi WhatsApp, serta membandingkan kondisi perangkat *root* dan *non-root*. Penelitian lanjutan juga dapat menambahkan analisis lebih mendalam terhadap struktur database WhatsApp agar proses identifikasi pesan, media, tautan, timestamp, dan metadata dapat dilakukan secara lebih akurat.

DAFTAR PUSTAKA

- Daraghmi, E., Qaroush, Z., Hamdi, M., & Cheikhrouhou, O. (2023). Forensic Operations For Recognizing Sqlite Content (FORC): An Automated Forensic Tool For Efficient Sqlite Evidence Extraction On Android Devices. *Applied Sciences* 2023, Vol. 13, Page 10736, 13(19), 10736. <https://doi.org/10.3390/app131910736>
- Fadillah, M. F., Fadillah, M. F., & Yuniati, T. (2024). Perbandingan Hasil Recovery Tools Mobile Forensic Di Smartphone Android Menggunakan Metode National Institute Of Justice (NIJ). *Cyber Security Dan Forensik Digital*, 6(2), 54–61. <https://doi.org/10.14421/csecurity.2023.6.2.4172>
- Mualfah, D., Syam, M. I., & Baidarus. (2023). Analisis Perbandingan Tools Mobile Forensic Menggunakan Metode National Institute Of Justice (NIJ). *Jurnal Coscitech (Computer Science And Information Technology)*, 4(1), 283–292. <https://doi.org/10.37859/Coscitech.V4i1.4767>
- Mursyid, Airlangga Putera, & Miftahul Jannah. (2025). Rekonstruksi Peran Digital Forensik Dalam Penyidikan Tindak Pidana Siber: Analisis Kritis Terhadap Konstruksi Hukum Pidana Di Indonesia | Jurnal Tana Mana. *Jurnal Tana Mana*, 6(2). <https://doi.org/10.33648/jtm.v6i2.1194>
- Qibriya, M. R. D., Ambarwati, A., & Susilo, K. E. (2021). Analisis Forensik Digital Pada Aplikasi Instant Messaging Di Smartphone Berbasis Android Untuk Bukti Digital. *Jurnal Teknologi Informasi*, 5(2), 114–121. <https://doi.org/10.36294/jurti.v5i2.2200>
- Raharja, R. P., Alwi, E. I., Widya, A., Gaffar, M., & Kunci, K. (2024). Analisis Digital Forensic Pada Aplikasi Whatsapp Menggunakan Metode National Institute Of Justice (NIJ) Pada Smartphone Android. *Buletin Sistem Informasi Dan Teknologi Islam (BUSITI)*, 5(2), 160–168. <https://doi.org/10.33096/busiti.v5i2.2180>
- Rosita, M. (2023). Analisis Komparatif Performa FTK IMAGER Dan AUTOPSY Dalam Forensik Digital Pada Flashdisk. *Info Kripto*, 17(3). <https://doi.org/10.56706/ik.v17i3.83>
- Rully. (2004). *Forensic Examination Of Digital Evidence: A Guide For Law Enforcement* (Pp. 94–101). <https://nij.ojp.gov/library/publications/forensic-examination-digital-evidence-guide-law-enforcement>
- Sahara, A., & Kuswandi, K. (2025). Penipuan Online Sebagai Bentuk Kejahatan Siber Dalam Perspektif Kriminologi. *Parlementer: Jurnal Studi Hukum Dan Administrasi Publik*, 2(4), 92–105. <https://doi.org/10.62383/Parlementer.V2i4.1425>
- Setiawan, E., & Hartwiningsih, H. (2025). Optimizing The Use Of Digital Forensics And Information Technology In Proving Criminal Acts Of Electronic Document Forgery In Indonesia. *International Journal Of Law, Crime And Justice*, 2(2), 72–86. <https://doi.org/10.62951/ijlcj.v2i2.587>
- Shabira, A. F., & Fachri, F. (2025). Analisis Forensik Digital Pada File Steganografi

- Menggunakan FTK Imager Dan Winhex Dalam Kasus Peredaran Narkoba Dengan Live Forensics. *Rabit: Jurnal Teknologi Dan Sistem Informasi Univrab*, 10(2), 228–240. <https://doi.org/10.36341/Rabit.V10i2.6020>
- Sugiyono; (2023). *Metode Penelitian Pendidikan Pendekatan Kuantitatif, Kualitatif Dan R&D*. Alfabeta.
- Utami, S. D., Utami, S. D., Carudin, C., & Ridha, A. A. (2021). Analisis Live Forensic Pada Whatsapp Web Untuk Pembuktian Kasus Penipuan Transaksi Elektronik. *Cyber Security Dan Forensik Digital*, 4(1), 24–32. <https://doi.org/10.14421/Csecurity.2021.4.1.2416>