



Analisis Forensik Digital Dan Ekstraksi Artefak Aplikasi Gbwhatsapp Pada Perangkat Android Menggunakan Framework NIST SP 800-86

Riyad Saifani^{1*}, Mahardika Abdi Prawira Tanjung²

^{1*,2}Program Studi Sistem Informasi, Fakultas Ilmu Komputer dan Teknologi Informasi, Universitas Muhammadiyah Sumatera Utara, Medan, Indonesia

Email: ^{1*}r.fan1180@gmail.com, ²mahardikaabdiprawira@umsu.ac.id

Abstrak

Perkembangan aplikasi pesan instan hasil modifikasi seperti GBWhatsApp menimbulkan tantangan baru dalam pemeriksaan forensik digital, terutama terkait keberadaan pesan yang telah ditarik (revoked) oleh pengirim serta kesesuaian struktur basis datanya dengan WhatsApp resmi. Penelitian ini bertujuan menganalisis kemungkinan identifikasi dan pemulihan pesan yang telah ditarik pada GBWhatsApp, memetakan sumber dan struktur data GBWhatsApp pada perangkat Android, serta menilai kesesuaian metode pemeriksaan WhatsApp resmi apabila diterapkan pada GBWhatsApp. Penelitian menerapkan kerangka kerja NIST SP 800-86 melalui tahapan collection, examination, analysis, dan reporting terhadap salinan forensik WhatsApp resmi dan GBWhatsApp yang diperoleh dari perangkat Android berhak akses root. Sebagai alat bantu pemeriksaan, dikembangkan Web Viewer berbasis Laravel dan mesin pengolahan Python yang mengintegrasikan pengelolaan barang bukti, examination, analisis percakapan, perbandingan database, dan pelaporan. Hasil pengujian Black Box menunjukkan seluruh fungsi utama sistem berjalan sesuai rancangan. Hasil pemeriksaan artefak menunjukkan bahwa pesan yang telah ditarik dapat diidentifikasi melalui basis data SQLite dan berkas Write-Ahead Log, serta pada kondisi tertentu kontennya dapat dipulihkan berdasarkan artefak historis yang masih tersimpan. Perbandingan struktur database menunjukkan adanya kesamaan dan perbedaan antara WhatsApp resmi dan GBWhatsApp, yang selanjutnya digunakan sebagai dasar penilaian bahwa metode pemeriksaan WhatsApp resmi dapat diterapkan pada GBWhatsApp dengan penyesuaian tertentu.

Kata Kunci: Forensik Digital, GBWhatsApp, Pesan Ditarik, NIST SP 800-86, Struktur Database.

PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi menjadikan aplikasi pesan instan sebagai salah satu media utama pertukaran informasi digital, mulai dari teks, suara, gambar, video, hingga dokumen. Aktivitas komunikasi pada perangkat bergerak meninggalkan berbagai data yang memiliki nilai penting dalam pemeriksaan forensik digital. Anglano (2014) menunjukkan bahwa pemeriksaan aplikasi WhatsApp pada perangkat Android dapat menghasilkan sejumlah artefak komunikasi, seperti basis data percakapan, daftar kontak, dan metadata waktu, yang dapat digunakan untuk merekonstruksi aktivitas pengguna. Dengan demikian, data komunikasi yang tersimpan pada perangkat dapat menjadi sumber informasi penting ketika perangkat tersebut berkaitan dengan suatu proses penyelidikan.

Kebutuhan memperoleh informasi komunikasi menjadi semakin penting ketika komunikasi tersebut berkaitan dengan dugaan tindak pidana. Sebagai ilustrasi, dalam penyelidikan dugaan transaksi narkoba, perangkat milik salah satu pihak dapat memuat riwayat percakapan dengan pihak lain yang diduga terlibat. Apabila pesan yang memuat informasi transaksi tersebut telah ditarik atau dihapus oleh pengirim sebelum perangkat diperiksa, isi pesan tidak lagi dapat diketahui hanya melalui tampilan percakapan pada aplikasi, sehingga dapat menyulitkan penyidik dalam memahami keterkaitan antarpihak yang diperiksa. Upaya memperoleh kembali isi komunikasi tersebut tidak dapat semata-mata bergantung pada permintaan kepada penyedia layanan, karena penerapan end-to-end encryption membatasi kemampuan pihak eksternal untuk memperoleh isi percakapan WhatsApp dalam bentuk terbaca melalui intersepsi konvensional (Wijnberg & Le-Khac, 2021). WhatsApp tidak menyimpan pesan dalam bentuk terdekripsi maupun kunci privat yang diperlukan untuk mendekripsinya, sehingga pemeriksaan forensik terhadap perangkat menjadi pendekatan penting untuk mengetahui apakah pesan yang telah ditarik masih dapat ditemukan atau dipulihkan dari data yang tersimpan pada perangkat.

Permasalahan menjadi lebih kompleks ketika aplikasi yang diperiksa bukan WhatsApp resmi, melainkan GBWhatsApp, yaitu aplikasi WhatsApp hasil modifikasi pihak ketiga yang tidak dikembangkan maupun didistribusikan oleh pengembang resmi WhatsApp. Modifikasi tersebut menghadirkan sejumlah fungsi tambahan yang tidak tersedia atau berperilaku berbeda dibandingkan aplikasi resmi, antara lain Anti-Revoke (mempertahankan pesan yang ditarik oleh pengirim), Hide Blue Ticks (menyembunyikan tanda pesan telah dibaca), dan Anti-View Once (memungkinkan media sekali lihat tetap dapat diakses). Keberadaan fungsi-fungsi tersebut mengindikasikan bahwa struktur penyimpanan, basis data, berkas, metadata, maupun komponen data lain pada GBWhatsApp berpotensi memiliki karakteristik berbeda dari WhatsApp resmi, meskipun perbedaan tersebut belum dapat ditetapkan hanya berdasarkan keberadaan fitur tambahan dan perlu dibuktikan melalui pemeriksaan langsung.

Sejumlah penelitian terdahulu telah membahas pemeriksaan forensik terhadap aplikasi pesan instan dengan berbagai objek dan metode, sebagaimana diringkas pada Tabel 1.

Tabel 1. Perbandingan Penelitian Terdahulu

No	Peneliti & Tahun	Objek dan Pendekatan	Fokus/Hasil Penelitian	Perbedaan dengan Penelitian Ini
1	Widodo & Sugiantoro (2018)	GBWhatsApp pada smartphone Tizen menggunakan framework HDFIP	Pemulihan percakapan terhapus melalui dekripsi basis data	Dilakukan pada sistem operasi Tizen; tidak memetakan struktur database GBWhatsApp pada Android
2	Ramadhan & Riadi (2019)	WhatsApp resmi pada Android menggunakan kerangka NIST	Pemeriksaan data WhatsApp dalam konteks investigasi tindak penipuan	Objek berupa WhatsApp resmi; tidak membahas GBWhatsApp maupun pesan ditarik
3	Anglano (2014)	WhatsApp Messenger pada perangkat Android	Identifikasi artefak kontak dan riwayat komunikasi dari basis data WhatsApp	Tidak membahas GBWhatsApp maupun pemulihan pesan yang telah ditarik
4	Prabowo dkk. (2025)	WhatsApp msgstore.db.crypt14 pada perangkat rooted dan non-rooted	Ekstraksi, dekripsi, dan analisis basis data WhatsApp terenkripsi	Berfokus pada WhatsApp resmi; tidak memeriksa karakteristik data GBWhatsApp

Widodo dan Sugiantoro (2018) melakukan pemeriksaan terhadap GBWhatsApp pada smartphone berbasis Tizen menggunakan framework Harmonised Digital Forensic Investigation Process (HDFIP) dan berhasil memulihkan percakapan yang telah dihapus melalui proses dekripsi basis data. Penelitian tersebut memiliki kesamaan objek dengan penelitian ini, namun dilakukan pada lingkungan sistem operasi Tizen sehingga hasilnya belum dapat secara langsung menggambarkan karakteristik penyimpanan dan pemulihan data GBWhatsApp pada perangkat Android. Ramadhan dan Riadi (2019) serta Prabowo dkk. (2025) memeriksa WhatsApp resmi pada perangkat Android menggunakan kerangka NIST dan teknik dekripsi berkas msgstore.db.crypt14, tetapi kedua penelitian tersebut berfokus pada WhatsApp resmi dan tidak memeriksa karakteristik aplikasi hasil modifikasi seperti GBWhatsApp. Dengan demikian, pemetaan struktur penyimpanan dan basis data GBWhatsApp pada Android serta perbandingannya dengan karakteristik WhatsApp resmi belum menjadi fokus penelitian-penelitian tersebut. Kesenjangan ini penting dikaji karena tanpa pemahaman terhadap karakteristik GBWhatsApp pada Android, proses pemeriksaan berpotensi menggunakan asumsi yang tidak sesuai sehingga data yang relevan dapat terlewat.

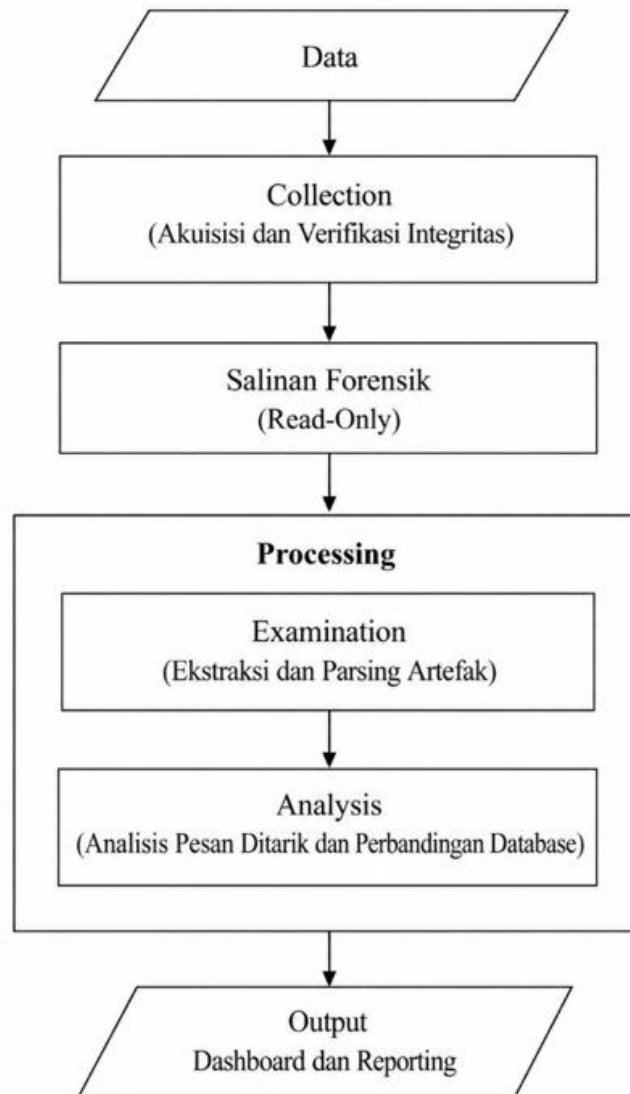
Untuk menjawab kesenjangan tersebut, penelitian ini melakukan pemeriksaan forensik digital terhadap GBWhatsApp pada perangkat Android menggunakan kerangka kerja NIST SP 800-86 yang meliputi tahapan collection, examination, analysis, dan reporting untuk mengarahkan proses pemeriksaan secara sistematis, mulai dari pengumpulan data hingga penyajian hasil (Kent dkk., 2006). Pemeriksaan dilakukan dengan mengidentifikasi dan memetakan sumber serta struktur data GBWhatsApp, kemudian membandingkan karakteristik yang relevan dengan WhatsApp resmi berdasarkan penelitian terdahulu. Data yang diperoleh selanjutnya diekstraksi dan dianalisis untuk menguji kemungkinan menemukan atau memulihkan pesan yang telah ditarik atau dihapus. Selain hasil pemeriksaan forensik digital, penelitian ini mengembangkan Web Viewer lokal berbasis web sebagai alat bantu untuk mengolah dan menyajikan hasil pemeriksaan secara terstruktur, mencakup data komunikasi, metadata waktu, media, sumber data, serta informasi lain yang berhasil diperoleh selama pemeriksaan. Setiap berkas hasil akuisisi diverifikasi integritasnya menggunakan nilai hash, sejalan dengan prinsip bahwa penggunaan fungsi hash seperti SHA-256 dapat digunakan untuk memverifikasi konsistensi data digital pada berbagai jenis sistem, termasuk pada sistem pertukaran pesan berbasis web (Al Afgani & Riza, 2026).

Berdasarkan uraian tersebut, penelitian ini bertujuan untuk: (1) menganalisis kemungkinan pesan yang telah ditarik atau dihapus pada GBWhatsApp untuk dapat ditemukan atau dipulihkan melalui

pemeriksaan forensik digital; (2) mengidentifikasi dan memetakan sumber serta struktur data GBWhatsApp pada perangkat Android, kemudian mengidentifikasi persamaan dan perbedaannya dengan karakteristik WhatsApp resmi; (3) menerapkan tahapan NIST SP 800-86 dalam proses pemeriksaan forensik digital terhadap data GBWhatsApp pada perangkat Android; dan (4) merancang serta membangun Web Viewer lokal untuk mengolah dan menyajikan hasil pemeriksaan forensik digital GBWhatsApp secara terstruktur sehingga mendukung proses penelusuran, analisis, dan pelaporan hasil pemeriksaan.

METODE

Penelitian ini menggunakan pendekatan eksperimental dengan kerangka kerja NIST SP 800-86 yang terdiri atas empat tahapan, yaitu collection, examination, analysis, dan reporting (Kent dkk., 2006). Keempat tahapan tersebut diselaraskan dengan arsitektur penelitian berpola Data-Processing-Output, sebagaimana ditunjukkan pada Gambar 1, yang menggambarkan alur penelitian mulai dari penyiapan data, proses pemeriksaan, hingga penyajian hasil melalui sistem Web Viewer yang dikembangkan.



Gambar 1. Arsitektur Penelitian (Data-Processing-Output)

Tahap Data (Collection)

Sumber data penelitian adalah artefak digital yang diperoleh dari perangkat Android yang menjalankan WhatsApp resmi dan GBWhatsApp Pro versi 26.90. GBWhatsApp menjadi objek utama pemeriksaan, sedangkan WhatsApp resmi digunakan sebagai pembandingan struktur database. Perangkat Android yang digunakan harus memiliki hak akses root karena sebagian artefak aplikasi tersimpan pada direktori privat yang tidak dapat dijangkau menggunakan hak pengguna biasa. Lingkungan Android disediakan melalui layanan cloud phone Redfinger sebagai lingkungan utama dan emulator Genymotion sebagai lingkungan cadangan, keduanya terhubung dengan komputer pemeriksa melalui Android Debug Bridge (ADB).

Sebelum akuisisi dilakukan, peneliti membuat kondisi pengujian melalui skenario simulasi percakapan pada GBWhatsApp, meliputi aktivitas komunikasi yang kemudian diikuti dengan penarikan atau penghapusan sebagian pesan, sehingga tersedia data yang dapat digunakan untuk menguji kemampuan sistem dalam mendeteksi dan menelusuri kembali artefak pesan yang telah ditarik. Data penelitian diperoleh melalui skenario terkontrol ini, bukan dari komunikasi pribadi pengguna sebenarnya maupun barang bukti dari kasus hukum nyata. Proses akuisisi dilakukan melalui Termux sebagai terminal pada lingkungan Android, dengan akses superuser (perintah su) untuk menjangkau direktori privat aplikasi. Artefak yang diakuisisi meliputi basis data utama, berkas Write-Ahead Log (WAL), Shared Memory (SHM), shared preferences, media, konfigurasi, serta komponen kunci atau data pendukung kriptografi, dengan struktur direktori asli tetap dipertahankan agar keterkaitan antarartefak dapat ditelusuri.

Seluruh berkas hasil akuisisi dihitung nilai hash SHA-256-nya secara langsung melalui Termux dan dicatat ke dalam berkas teks pada direktori akuisisi yang sama sebagai catatan integritas. Direktori hasil akuisisi beserta catatan hash kemudian dikompresi menjadi satu berkas ZIP dan dipindahkan ke lingkungan pemeriksaan melalui Google Drive. Salinan forensik yang diperoleh selanjutnya diperlakukan dalam kondisi read-only agar pemeriksaan tidak mengubah data sumber.

Tahap Processing (Examination dan Analysis)

Pada tahap examination, salinan forensik WhatsApp resmi dan GBWhatsApp diperiksa untuk mengidentifikasi struktur basis data, tabel, kolom, serta data yang berkaitan dengan aktivitas komunikasi, termasuk berkas WAL dan SHM, kemudian diekstraksi dan diparsing ke dalam bentuk yang dapat diproses pada tahap analysis. Tahap analysis berfokus pada dua hal: (1) mengidentifikasi keberadaan pesan yang telah ditarik serta menilai kemungkinan pemulihan kontennya berdasarkan artefak historis yang tersisa pada basis data dan WAL; dan (2) membandingkan struktur database GBWhatsApp dengan WhatsApp resmi pada tingkat basis data, tabel, dan kolom untuk mengetahui tingkat kesamaan maupun perbedaannya, sebagai dasar penilaian kesesuaian metode pemeriksaan WhatsApp resmi terhadap GBWhatsApp. Proses examination dan analysis dijalankan oleh mesin pengolahan berbasis Python yang terintegrasi dengan aplikasi web melalui ExaminationController.

Tahap Output (Dashboard dan Reporting)

Hasil examination dan analysis disajikan melalui Web Viewer berbasis Laravel 10.50.3 dengan basis data MySQL, yang dikembangkan mengikuti pola arsitektur Model-View-Controller sejalan dengan praktik umum pengembangan aplikasi berbasis Laravel (Ariyanto dkk., 2024; Santoso dkk., 2021). Sistem menyediakan fungsi pengelolaan kasus dan barang bukti, pelaksanaan examination, analisis percakapan dengan penanda pesan ditarik dan pesan terpulihkan, perbandingan struktur database, serta pelaporan yang dapat dicetak maupun diekspor ke format PDF. Rancangan fungsional sistem dimodelkan menggunakan Unified Modeling Language (UML), mencakup use case diagram, activity diagram, sequence diagram, dan class diagram, sejalan dengan praktik pemodelan sistem informasi berbasis UML pada penelitian-penelitian terdahulu (Wayahdi & Ruziq, 2023).

Lingkungan Implementasi dan Pengujian

Implementasi dan pengujian sistem dilakukan menggunakan satu unit laptop dengan prosesor AMD Ryzen 7 6800H (3,20 GHz), RAM 16 GB, GPU NVIDIA GeForce RTX 3050 4 GB, dan penyimpanan 512 GB, berjalan pada sistem operasi Windows 11 64-bit. Perangkat lunak pendukung terdiri atas Laravel 10.50.3 untuk aplikasi Web Viewer, Python 3.10.6 untuk mesin pengolahan artefak forensik, Laragon 6.10 sebagai lingkungan server lokal, Android Debug Bridge untuk komunikasi dengan perangkat Android, Redfinger dan Genymotion sebagai penyedia lingkungan Android, Termux sebagai terminal akses root, Google Drive untuk pemindahan data akuisisi, serta Visual Studio Code sebagai editor kode sumber.

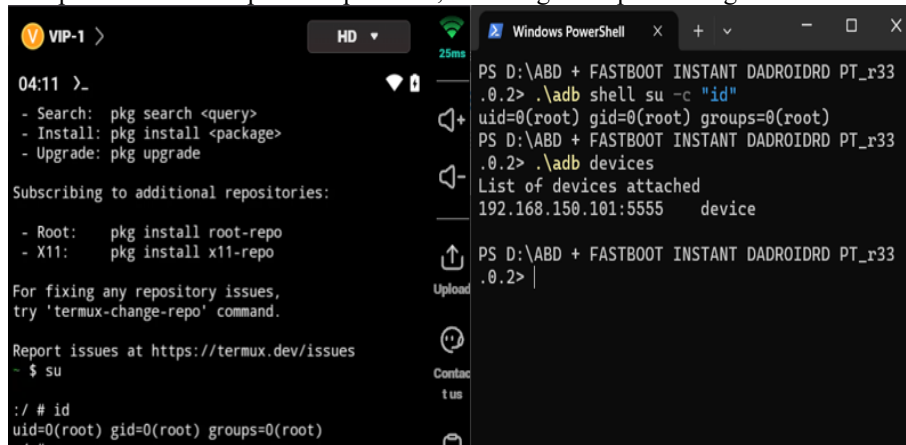
Pengujian sistem dilakukan dalam dua bentuk. Pertama, pengujian fungsional menggunakan metode Black Box Testing untuk memastikan setiap fungsi Web Viewer, mulai dari login, unggah barang bukti, pelaksanaan examination, analisis percakapan, perbandingan database, pelaporan, cetak/ekspor PDF, hingga logout, berjalan sesuai kebutuhan yang dirancang, dengan dua belas skenario pengujian sebagaimana dirangkum pada Tabel 2. Kedua, pengujian pemeriksaan artefak dilakukan terhadap data hasil akuisisi untuk mengevaluasi kemampuan sistem dalam mengidentifikasi dan memulihkan pesan yang telah ditarik serta membandingkan struktur database WhatsApp resmi dan GBWhatsApp, yang hasilnya menjadi dasar pembahasan pada bagian Hasil dan Pembahasan.

HASIL DAN PEMBAHASAN

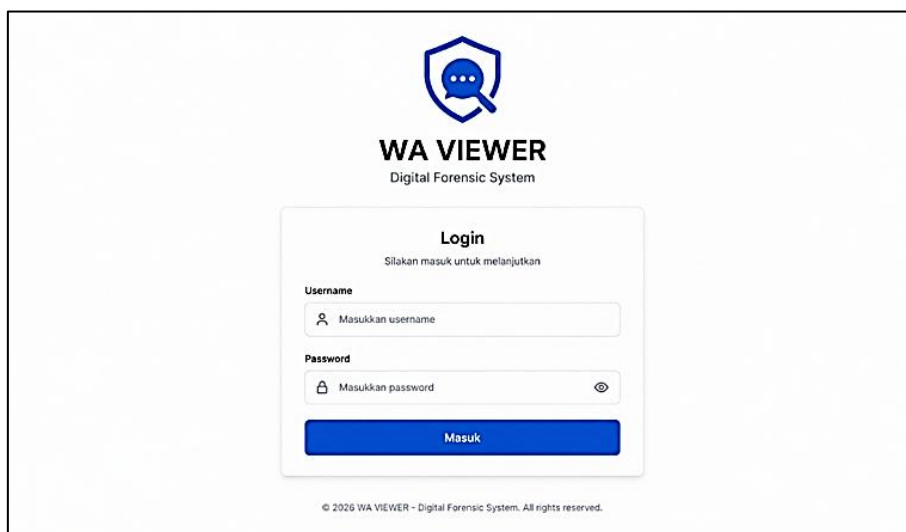
Implementasi Antarmuka Web Viewer

Web Viewer dibangun mengikuti alur pemeriksaan yang telah ditetapkan, mulai dari login, pengelolaan barang bukti, pelaksanaan examination, analisis percakapan, perbandingan database, hingga pelaporan. Halaman login (Gambar 2) menyediakan kolom username dan password yang diperiksa oleh controller autentikasi sebelum pengguna diarahkan ke halaman dashboard. Halaman dashboard (Gambar

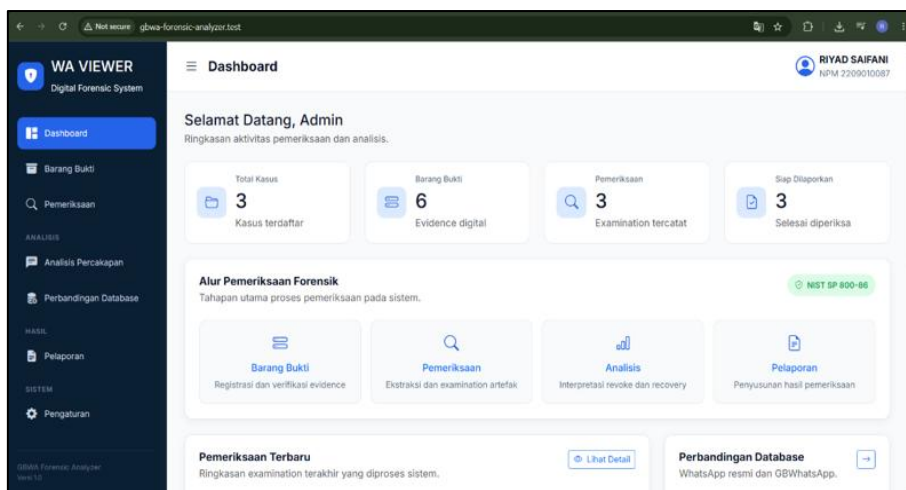
3) menyajikan ringkasan jumlah kasus, barang bukti, dan pemeriksaan, informasi pemeriksaan terbaru beserta jumlah pesan ditarik dan pesan terpulihkan, serta ringkasan perbandingan database.



Gambar 2. Akses Root dan Koneksi Perangkat Melalui Termux

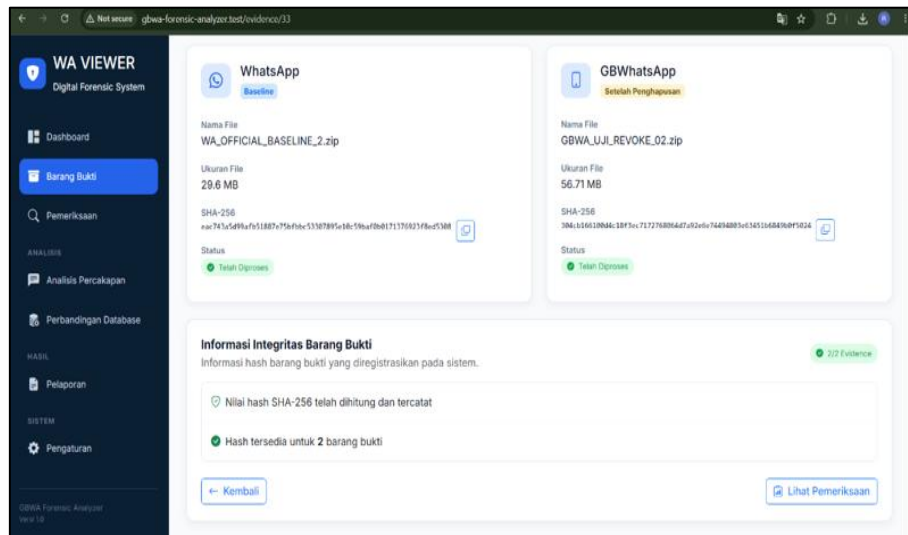


Gambar 3. Halaman Login Sistem

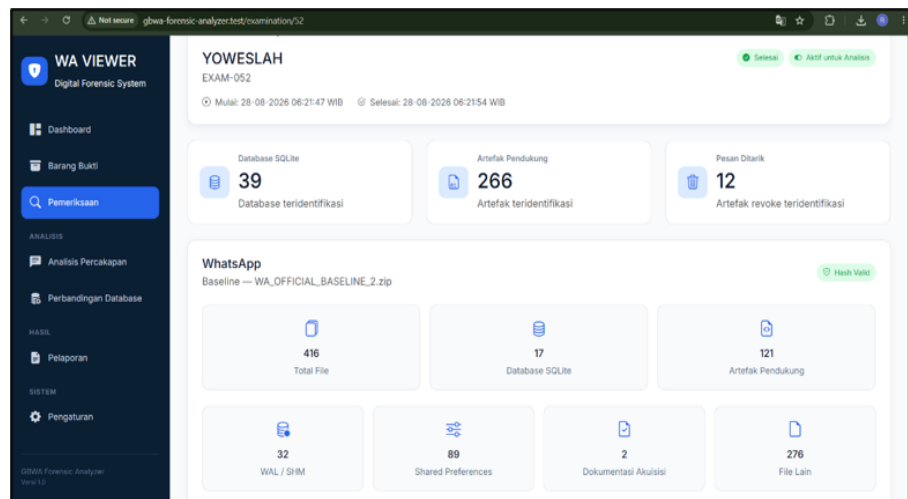


Gambar 4. Halaman Dashboard Sistem

Halaman Barang Bukti (Gambar 4) digunakan untuk mengunggah dan mengelola salinan forensik WhatsApp resmi dan GBWhatsApp sebagai pasangan data dalam satu pemeriksaan; setiap berkas yang diunggah dicatat metadatanya beserta nilai hash SHA-256 sebagai identitas integritas. Halaman Pemeriksaan (Gambar 5) digunakan untuk menjalankan proses examination, yang pada sisi backend dikendalikan oleh ExaminationController yang membentuk job pemeriksaan dalam format JSON dan menjalankan Python Forensic Engine untuk mengolah salinan forensik.

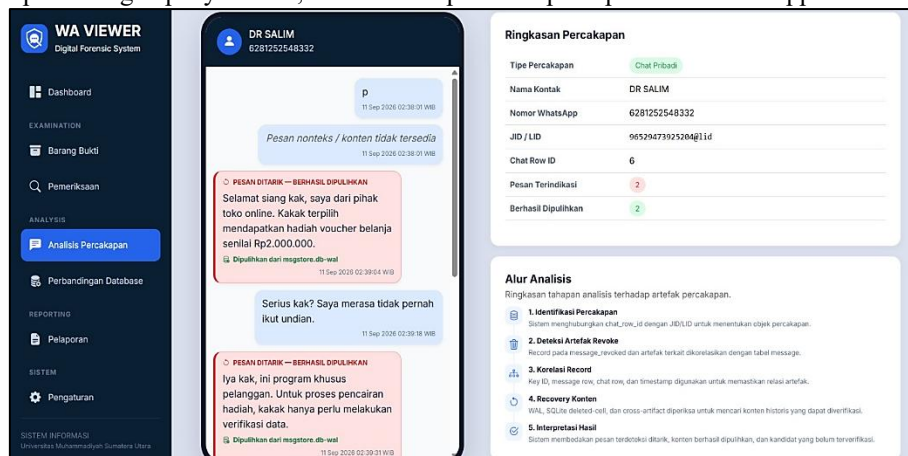


Gambar 5. Halaman Barang Bukti



Gambar 6. Halaman Pemeriksaan

Hasil examination selanjutnya ditampilkan melalui halaman Analisis Percakapan (Gambar 6) dan halaman Perbandingan Database (Gambar 7). Halaman Analisis Percakapan menyajikan percakapan yang memiliki artefak terkait pesan ditarik berdasarkan message row, key ID, chat row ID, dan timestamp, serta membedakan secara eksplisit antara pesan yang terdeteksi sebagai ditarik dan pesan yang kontennya berhasil dipulihkan. Halaman Perbandingan Database menampilkan jumlah tabel yang sama, tabel yang hanya terdapat pada salah satu aplikasi, serta perbedaan struktur kolom pada tabel yang memiliki nama sama, disertai interpretasi apakah metode pemeriksaan berbasis struktur WhatsApp resmi dapat diterapkan, dapat diterapkan dengan penyesuaian, atau tidak dapat diterapkan pada GBWhatsApp.



Gambar 7. Halaman Analisis Percakapan

Database	WA Result	GBWhatsApp	Tabel Sama	Hanya WA	Hanya GBWA	Struktur Berbeda	Kesamaan
_loginuser-whatappbmanager	2	2	2	0	0	0	100%
account_switcher.db	3	3	3	0	0	0	100%
androidx.work.workub	9	9	9	0	0	0	100%
automesage.db	0	2	0	0	2	2	0%
axoloti.db	14	14	14	0	0	0	100%
btor.db	0	2	0	0	2	2	0%
chatsettings.db	3	3	3	0	0	0	100%
com.pinterest.pinterest-account-creator	2	2	2	0	0	0	100%

Gambar 8. Halaman Perbandingan Database

Halaman Pelaporan (Gambar 8) menyajikan hasil pemeriksaan secara terstruktur, memisahkan bagian Temuan Pesan Ditarik dari bagian Recovery Terverifikasi agar hasil deteksi tidak disamakan dengan keberhasilan pemulihan, serta menyediakan fungsi cetak dan ekspor PDF yang menggunakan sumber data yang sama dengan tampilan laporan sehingga informasi tetap konsisten.

Identitas Pemeriksaan	
Nomor Kasus	CASE-018
Nama Kasus	YOWESLAH
Nomor Pemeriksaan	EXAM-052
Status Pemeriksaan	Completed
Waktu Mulai	28-08-2026 06:21:47 WIB
Waktu Selesai	28-08-2026 06:21:54 WIB
Engine Pemeriksaan	Python Forensic Analyzer v3.6
Metodologi	NIST SP 800-86 -- Examination, Analysis, dan Reporting

Gambar 9. Halaman Pelaporan

Hasil Pengujian Fungsional

Pengujian fungsional menggunakan metode Black Box Testing dilakukan terhadap dua belas skenario yang mencakup seluruh alur utama Web Viewer. Hasil pengujian dirangkum pada Tabel 2.

Tabel 2. Skenario dan Hasil Pengujian Fungsional Sistem (Black Box Testing)

No	Fungsi yang Diuji	Skenario Pengujian	Hasil yang Diharapkan	Status
1	Login	Memasukkan username/password yang benar	Autentikasi berhasil, Dashboard tampil	Berhasil
2	Login	Memasukkan username/password yang salah	Autentikasi ditolak, pesan kesalahan tampil	Berhasil
3	Unggah Barang Bukti	Mengunggah salinan forensik yang sesuai	Data barang bukti tersimpan dan tampil	Berhasil
4	Unggah Barang Bukti	Mengunggah berkas yang tidak sesuai	Sistem menolak dan menampilkan pesan kesalahan	Berhasil
5	Jalankan Pemeriksaan	Menjalankan examination dengan barang bukti lengkap	Pemeriksaan berjalan, riwayat pemeriksaan terbentuk	Berhasil
6	Detail Pemeriksaan	Membuka pemeriksaan berstatus Completed	Detail dan hasil pemeriksaan tampil	Berhasil
7	Analisis Percakapan	Membuka analisis dari pemeriksaan aktif	Hasil analisis percakapan dan artefak pesan ditarik tampil	Berhasil

No	Fungsi yang Diuji	Skenario Pengujian	Hasil yang Diharapkan	Status
8	Perbandingan Database	Membuka perbandingan dari pemeriksaan aktif	Hasil perbandingan struktur database tampil	Berhasil
9	Pelaporan	Membuka laporan pemeriksaan	Laporan hasil pemeriksaan tampil	Berhasil
10	Cetak Laporan	Memilih fungsi cetak	Laporan tampil dalam format siap cetak	Berhasil
11	Ekspor PDF	Memilih fungsi ekspor PDF	Dokumen PDF laporan dihasilkan	Berhasil
12	Logout	Memilih Logout	Sesi berakhir, pengguna diarahkan ke halaman Login	Berhasil

Seluruh skenario pengujian pada Tabel 2 menunjukkan hasil Berhasil, yang berarti fungsi autentikasi, pengelolaan barang bukti, pelaksanaan examination, penyajian hasil pemeriksaan, analisis percakapan, perbandingan database, pelaporan, pencetakan/ekspor PDF, dan logout telah berjalan sesuai dengan kebutuhan yang ditetapkan pada tahap perancangan. Hasil ini menunjukkan bahwa Web Viewer secara fungsional telah menyediakan alur yang diperlukan untuk mendukung pemeriksaan GBWhatsApp. Namun, keberhasilan fungsi antarmuka dan alur aplikasi belum secara langsung membuktikan keberhasilan metode pemeriksaan forensik dalam menemukan pesan yang telah ditarik maupun kesesuaian struktur database WhatsApp resmi dan GBWhatsApp, sehingga kemampuan tersebut dievaluasi lebih lanjut melalui pemeriksaan artefak pada subbagian berikut.

Identifikasi dan Pemulihan Pesan yang Telah Ditarik

Pemeriksaan artefak terhadap salinan forensik GBWhatsApp menunjukkan bahwa pesan yang telah ditarik oleh pengirim tetap meninggalkan jejak pada basis data SQLite maupun pada berkas Write-Ahead Log (WAL), meskipun pesan tersebut tidak lagi ditampilkan melalui antarmuka aplikasi. Jejak tersebut teridentifikasi melalui kombinasi penanda revoke pada tabel pesan, key ID, chat row ID, dan timestamp yang tetap tersimpan pada struktur basis data walaupun isi pesan pada baris aktif telah berubah menjadi status ditarik. Temuan ini sejalan dengan prinsip bahwa berkas WAL menyimpan salinan transaksi yang belum sepenuhnya digabungkan (checkpoint) ke dalam basis data utama, sehingga versi data sebelum perubahan termasuk isi pesan sebelum ditarik berpotensi masih dapat ditemukan pada berkas tersebut selama belum tertimpa oleh transaksi baru (Allen & Owens, 2010).

Pada kondisi artefak historis yang relevan masih tersedia dan belum tertimpa oleh aktivitas aplikasi berikutnya, Web Viewer dapat menampilkan serta memverifikasi konten pesan yang ditarik sebagai hasil pemulihan (recovery terverifikasi). Sebaliknya, pada kondisi artefak historis tersebut telah hilang atau tertimpa, sistem hanya dapat menampilkan keberadaan pesan yang terindikasi ditarik tanpa dapat memulihkan isinya secara penuh. Dengan demikian, pemulihan konten tidak terjadi secara seragam pada setiap artefak, melainkan bergantung pada ketersediaan dan keterverifikasian data historis yang masih ditemukan pada salinan forensik. Temuan ini memperkuat hasil penelitian Widodo dan Sugiantoro (2018) yang menunjukkan bahwa percakapan terhapus pada GBWhatsApp berbasis Tizen masih dapat ditemukan melalui dekripsi basis data, serta memperluasnya dengan menunjukkan bahwa pola serupa juga berlaku pada GBWhatsApp berbasis Android, khususnya melalui kombinasi basis data utama dan berkas WAL.

Keberadaan fitur Anti-Revoke pada GBWhatsApp secara fungsional mempertahankan tampilan pesan yang ditarik pada sisi antarmuka pengguna, tetapi hasil pemeriksaan menunjukkan bahwa mekanisme tersebut tidak menghilangkan jejak artefak pada tingkat basis data. Sebaliknya, keberadaan fitur tersebut justru menjadi indikator tambahan bagi pemeriksa untuk mengarahkan pemeriksaan pada baris data yang relevan. Temuan ini konsisten dengan hasil Prabowo dkk. (2025) yang menunjukkan bahwa struktur penyimpanan pesan WhatsApp pada berkas basis data terenkripsi tetap dapat diekstraksi dan dianalisis selama proses dekripsi dan parsing dilakukan dengan tepat, meskipun objek penelitian tersebut adalah WhatsApp resmi dan tidak membahas fitur modifikasi seperti Anti-Revoke.

Perbandingan Struktur Database WhatsApp Resmi dan GBWhatsApp

Perbandingan struktur database yang dilakukan oleh fitur Perbandingan Database pada Web Viewer menunjukkan bahwa GBWhatsApp secara umum mempertahankan sebagian besar struktur basis data WhatsApp resmi pada tabel-tabel inti yang berkaitan dengan penyimpanan pesan, informasi kontak, dan metadata percakapan, sejalan dengan karakteristik GBWhatsApp sebagai aplikasi yang dibangun di atas basis kode (codebase) WhatsApp resmi yang dimodifikasi. Pada tingkat ini, pendekatan pemeriksaan berbasis struktur yang digunakan pada WhatsApp resmi, sebagaimana diterapkan oleh Ramadhan dan Riadi (2019), tetap relevan untuk diterapkan pada GBWhatsApp.

Meskipun demikian, perbandingan juga menunjukkan adanya perbedaan pada sejumlah tabel dan kolom pendukung, khususnya yang berkaitan dengan fitur tambahan GBWhatsApp seperti penanda status

pesan ditarik, status pembacaan (terkait fitur Hide Blue Ticks), dan status akses media sekali lihat (terkait fitur Anti-View Once). Perbedaan tersebut tidak mengubah struktur inti penyimpanan pesan secara mendasar, tetapi menambahkan kolom atau tabel pendukung yang tidak terdapat pada WhatsApp resmi. Dengan demikian, hasil perbandingan database pada penelitian ini menunjukkan bahwa metode pemeriksaan WhatsApp resmi dapat diterapkan pada GBWhatsApp, tetapi dengan penyesuaian pada bagian struktur pendukung yang berkaitan dengan fitur modifikasi, bukan diterapkan secara identik tanpa verifikasi struktur terlebih dahulu. Temuan ini menjawab permasalahan penelitian mengenai kesesuaian metode pemeriksaan WhatsApp resmi terhadap GBWhatsApp berdasarkan struktur databasenya, serta melengkapi penelitian Widodo dan Sugiantoro (2018) yang belum secara khusus memetakan struktur database GBWhatsApp pada Android.

Pembahasan Umum

Secara keseluruhan, hasil penelitian ini menunjukkan tiga hal utama. Pertama, pesan yang telah ditarik pada GBWhatsApp dapat diidentifikasi melalui artefak forensik yang tersedia, dan pada kondisi tertentu kontennya dapat dipulihkan berdasarkan ketersediaan data historis, sehingga menjawab permasalahan penelitian mengenai kemungkinan penemuan dan pemulihan pesan ditarik. Kedua, struktur database GBWhatsApp dapat dipetakan dan dibandingkan dengan WhatsApp resmi, dengan hasil berupa kesamaan pada struktur inti dan perbedaan pada struktur pendukung terkait fitur modifikasi, yang digunakan sebagai dasar penilaian kesesuaian metode pemeriksaan. Ketiga, Web Viewer yang dikembangkan terbukti secara fungsional mampu mengintegrasikan seluruh tahapan examination, analysis, dan reporting ke dalam satu alur pemeriksaan berbasis web, sehingga mendukung proses penelusuran dan dokumentasi hasil pemeriksaan secara lebih terstruktur dibandingkan pemeriksaan manual terhadap artefak mentah.

Dibandingkan dengan penelitian Widodo dan Sugiantoro (2018) yang menggunakan framework HDFIP pada sistem operasi Tizen, penelitian ini memperluas kajian GBWhatsApp ke lingkungan Android menggunakan kerangka NIST SP 800-86 sekaligus menambahkan dimensi perbandingan struktur database yang belum menjadi fokus penelitian tersebut. Dibandingkan dengan Ramadhan dan Riadi (2019), Anglano (2014), dan Prabowo dkk. (2025) yang berfokus pada WhatsApp resmi, penelitian ini menunjukkan bahwa meskipun pendekatan pemeriksaan berbasis struktur basis data secara umum tetap relevan, penerapannya pada aplikasi hasil modifikasi seperti GBWhatsApp memerlukan verifikasi struktur terlebih dahulu agar artefak yang relevan, khususnya yang berkaitan dengan fitur tambahan, tidak terlewat selama proses pemeriksaan.

Penelitian ini memiliki keterbatasan karena pemeriksaan dilakukan pada satu versi GBWhatsApp (Pro 26.90) dan satu skenario simulasi komunikasi yang dirancang secara terkontrol, sehingga hasil pemulihan dan perbandingan struktur database belum sepenuhnya menggambarkan kondisi pada versi aplikasi lain atau pola penggunaan yang berbeda. Selain itu, data yang digunakan bukan merupakan barang bukti dari kasus hukum nyata, sehingga hasil penelitian ini perlu dipahami sebagai bukti konsep (proof of concept) mengenai kemampuan identifikasi dan pemulihan artefak, bukan sebagai pernyataan mengenai kekuatan pembuktian hukum atas suatu data.

KESIMPULAN

Penelitian ini menunjukkan bahwa pesan yang telah ditarik pada GBWhatsApp dapat diidentifikasi melalui artefak forensik yang tersedia pada basis data SQLite dan berkas Write-Ahead Log, serta dapat dipulihkan kontennya pada kondisi data historis yang relevan masih tersedia dan belum tertimpa oleh aktivitas aplikasi berikutnya; pemulihan tidak terjadi secara seragam pada setiap artefak, melainkan bergantung pada ketersediaan dan keterverifikasian data tersebut. Struktur database GBWhatsApp dan WhatsApp resmi menunjukkan kesamaan pada tabel-tabel inti penyimpanan pesan dan kontak, tetapi berbeda pada struktur pendukung yang berkaitan dengan fitur modifikasi seperti Anti-Revoke, Hide Blue Ticks, dan Anti-View Once, sehingga metode pemeriksaan WhatsApp resmi dapat diterapkan pada GBWhatsApp dengan penyesuaian pada bagian struktur pendukung tersebut, bukan diterapkan secara identik tanpa verifikasi. Penerapan kerangka kerja NIST SP 800-86 melalui tahapan collection, examination, analysis, dan reporting terbukti dapat mengarahkan proses pemeriksaan GBWhatsApp secara sistematis, mulai dari akuisisi artefak hingga penyajian hasil. Web Viewer berbasis Laravel dan mesin pengolahan Python yang dikembangkan dalam penelitian ini berhasil mengintegrasikan pengelolaan barang bukti, pelaksanaan examination, analisis percakapan, perbandingan struktur database, hingga pelaporan ke dalam satu alur pemeriksaan, dan seluruh fungsi utamanya terbukti berjalan sesuai rancangan berdasarkan hasil pengujian Black Box.

Penelitian selanjutnya disarankan untuk menguji lebih banyak versi WhatsApp resmi dan GBWhatsApp serta berbagai kondisi perangkat Android agar konsistensi hasil akuisisi, pemeriksaan artefak, dan pemulihan pesan dapat diketahui secara lebih luas. Kemampuan korelasi dan pemulihan artefak juga dapat dikembangkan lebih lanjut dengan menambahkan sumber artefak lain yang berpotensi

menyimpan data historis, sementara fitur perbandingan database dapat diperluas cakupan strukturnya agar perubahan akibat modifikasi aplikasi dapat dipetakan secara lebih mendalam, dan sisi pelaporan Web Viewer dapat dikembangkan agar mendukung dokumentasi pemeriksaan yang lebih lengkap.

UCAPAN TERIMA KASIH

Penulis menyampaikan terima kasih kepada Program Studi Sistem Informasi, Fakultas Ilmu Komputer dan Teknologi Informasi, Universitas Muhammadiyah Sumatera Utara, atas dukungan fasilitas dan bimbingan akademik selama penelitian ini berlangsung, serta kepada seluruh pihak yang telah membantu proses pengumpulan data dan pengembangan sistem dalam penelitian ini.

DAFTAR PUSTAKA

- Al Afgani, A., & Riza, F. (2026). Penerapan kriptografi ASCON, RSA, dan SHA-256 pada sistem chat berbasis web. *Indonesian Journal of Multidisciplinary Scientific Studies*, 4(6), 536–556. <https://doi.org/10.33151/ijomss.v4i6.1143>
- Allen, G., & Owens, M. (2010). *The definitive guide to SQLite* (1st ed.). Apress.
- Anglano, C. (2014). Forensic analysis of WhatsApp Messenger on Android smartphones. *Digital Investigation*, 11(3), 201–213. <https://doi.org/10.1016/j.diin.2014.04.003>
- Ariyanto, Y., Farhan, M., Rachmad, F., & Puspitasari, D. (2024). Laravel framework and native PHP: Comparison in the creation of rest API. *Matrix: Jurnal Manajemen Teknologi dan Informatika*, 14(2), 66–73.
- Ayers, R., Brothers, S., & Jansen, W. (2014). *Guidelines on mobile device forensics* (NIST Special Publication 800-101 Rev. 1). National Institute of Standards and Technology.
- Dasmen, R. N., Pratama, M. R., Yasir, H., & Budiman, A. (2024). Analisis forensik digital pada kasus cyberbullying dengan metode National Institute of Standard and Technology SP 800-86. *Jurnal Ilmiah Informatika*, 12(1), 68–73. <https://doi.org/10.33884/jif.v12i01.8344>
- Fayyad-Kazan, H., Kassem-Moussa, S., Hejase, H. J., & Hejase, A. J. (2022). Forensic analysis of WhatsApp SQLite databases on the unrooted Android phones. *HighTech and Innovation Journal*, 3(2), 175–195.
- Garfinkel, S. L. (2010). Digital forensics research: The next 10 years. *Digital Investigation*, 7, S64–S73. <https://doi.org/10.1016/j.diin.2010.05.009>
- Hoog, A. (2011). *Android forensics: Investigation, analysis, and mobile security for Google Android*. Syngress.
- Kent, K., Chevalier, S., Grance, T., & Dang, H. (2006). *Guide to integrating forensic techniques into incident response* (NIST Special Publication 800-86). National Institute of Standards and Technology.
- Prabowo, W. A., Mohsen, F., & Selamat, S. R. (2025). WhatsApp mobile applications in the lens of digital forensics: Deciphering the msgstore.db.crypt14 file. *Journal of Cyber Security and Mobility*, 14(4), 823–848. <https://doi.org/10.13052/jcsm2245-1439.1443>
- Ramadhan, M. I., & Riadi, I. (2019). Forensic WhatsApp based Android using National Institute of Standard Technology (NIST) method. *International Journal of Computer Applications*, 177(8), 1–7.
- Rifqi, M., Ismail, S. J. I., & Rizal, M. F. (2023). Analisis forensik untuk penanganan cyber crime pada aplikasi WhatsApp menggunakan metode National Institute of Standard and Technology (NIST SP 800-86). *e-Proceeding of Engineering*, 9(6), 3017–3022.
- Santoso, G. B., Sinaga, T. M., & Zuhdi, A. (2021). MVC implementation in Laravel framework for development web-based e-commerce applications. *Intelmatiks*, 1(1), 37–42. <https://doi.org/10.25105/itm.v1i1.7867>
- Stallings, W. (2005). *Cryptography and network security* (4th ed.). Prentice Hall.
- Sudiana, D., Nuruddin, C. H., Rizkinia, M., & Husna, D. (2024). Forensic analysis of WhatsApp disappearing message on unrooted Android using mobile device forensics methodology NIST SP 800-101r1. *Evergreen*, 11(1), 516–524. <https://doi.org/10.5109/7172316>

- Wayahdi, M. R., & Ruziq, F. (2023). Pemodelan sistem penerimaan anggota baru dengan Unified Modeling Language (UML) (Studi kasus: Programmer Association of Battuta). *Jurnal Minfo Polgan*, 12(1), 1514–1521. <https://doi.org/10.33395/jmp.v12i1.12870>
- Widodo, & Sugiantoro, B. (2018). Penerapan framework Harmonised Digital Forensic Investigation Process (HDFIP) untuk mendapatkan artifak digital evidence. *CyberSecurity dan Forensik Digital*, 1(2), 67–74.
- Wijnberg, D., & Le-Khac, N. A. (2021). Identifying interception possibilities for WhatsApp communication. *Forensic Science International: Digital Investigation*, 38, 301132. <https://doi.org/10.1016/j.fsidi.2021.301132>