Volume 21 Nomor 01 (2026) 83-91
E – Link P-ISSN 1858-2109 E-ISSN 2656-5676
Jurnal Teknik Elektro dan Informatika

INVESTIGASI PENIPUAN *WHATSAPP* BERBASIS *INTEGRATED DIGITAL FORENSIC INVESTIGATION FRAMEWORK v2*(IDFIF v2) PADA PESAN TERHAPUS

Siti Nur Ashfia[1)] , Fahmi Fachri[2)]
[1,2)] Program Studi Teknik Informatika, Fakultas Teknik, Universitas Ma'arif Nahdlatul Ulama Kebumen
Jln. Kutoarjo Km. 05, Jatisari, Kebumen, Jawa Tengah, Indonesia.
E-mail **:** [1)]nurashfia84@gmail.com**,** [2)]fahmifachriumnu@gmail.com

ABSTRAK

Kasus penipuan online melalui aplikasi *WhatsApp* semakin meningkat seiring tingginya penggunaan layanan pesan instan di Indonesia. Permasalahan utama dalam investigasi digital adalah data komunikasi yang mudah dihapus sehingga menyulitkan proses pembuktian. Penelitian bertujuan menerapkan metode Integrated Digital Forensic Investigation Framework v2 (IDFIF v2) untuk mengungkap artefak digital pada dugaan kasus penipuan melalui *WhatsApp* di perangkat Android. Metode penelitian menggunakan pendekatan kualitatif eksperimental dengan tahapan IDFIF v2 meliputi *preparation*, *incident response*, *laboratory process*, dan *presentation*. Proses akuisisi data dilakukan menggunakan Andriller, sedangkan analisis basisdata dilakukan menggunakan DB Browser for SQLite terhadap file msgstore.db. Hasil penelitian menunjukkan bahwa Andriller berhasil mengekstraksi artefak digital berupa file media *WhatsApp* yang telah terhapus, seperti gambar dan video. Analisis *database* menunjukkan adanya aktivitas komunikasi serta ditemukan 22 pesan yang telah dihapus. Isi pesan dalam *database* tersebut tidak dapat dipulihkan secara langsung, metadata yang diperoleh dapat mendukung proses investigasi. Hasil penelitian menunjukkan kombinasi Andriller dan SQLite dapat memberikan kontribusi dalam pembuktian digital, namun masih memiliki keterbatasan pada pemulihan isi pesan terhapus. Oleh karena itu, penelitian selanjutnya perlu mengombinasi tools dan metode lain untuk meningkatkan efektivitas proses investigasi.

Kata kunci : Forensik Digital, *WhatsApp*, IDFIF v2, Andriller, SQLite

ABSTRACT

Online fraud cases through the WhatsApp applicatipn continue to increase alongside the high usage of instant messaging servise in Indonesia. The main challenge in digital investigations is that communication data can be easily deleted, making evidence collection difficult. This study aims to implement the Integrated Digital Forensic Investigastion Framework v2 (IDFIF v2) to uncover digital artifact in a suspected WhatsApp fraud case on an Android device. The research uses a qualitative experimental approach using IDFIF v2 stages including preparation, incident response, laboratory process, and presentation. Data acquisition is conducted using Andriller, while database analysis is performed using DB Browser for SQLite on the msgstore.db file. The results show that Andriller successfully extracted deleted WhatsApp media artifacts such as images and videos. Database analysis reveals communication activities and identifies 22 deleted messages. Although the message contents could not be directly recovered, metadata provides valuable evidence for

investigation. This study demonstrates that combining Andriller and SQLite contributes to digital vidence analysis, although limitations remain in recovering deleted message content, therefore, future research should integrate additional tools and methods to enhance investigation effectiveness.

Keywords: *Digital Forensic, WhatsApp, IDFIF v2, Andriller, SQLite*

1. PENDAHULUAN

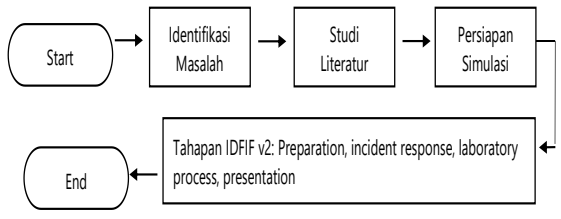
Perkembangan teknologi informasi dan komunikasi telah memberikan dampak yang siginifikan dalam berbagai aspek kehidupan, khususnya dalam aktivitas komunikasi digital. Berdasarkan data tahun 2025, jumlah pengguna internet di Indonesia mencapai 212 juta dengan tingkat penetrasi sebesar 74,6%[1]. Peningkatan penggunaan teknologi tersebut diiringi dengan meningkatnya kejahatan siber, salah satunya adalah penipuan online yang memanfaatkan aplikasi pesan instan[2]. Salah satu *platform* yang paling sering digunakan dalam kejahatan siber adalah *WhatsApp*[3]. Dengan 3miliar pengguna yang menjadikannya target utama pelaku kejahatan siber[4][5]. Meskipun *WhatsApp* menawarkan kemudahan komunikasi, fitur seperti enkripsi end-to-end dan sifat data yang mudah dihapus menjadi tantangan dalam proses investigasi digital. Kondisi ini menyebabkan kesulitan dalam mengidentifikasi pelaku serta mengumpulkan bukti digital yang valid dan dapat dipertanggungjawabkan secara hukum. Oleh karena itu, diperlukan pendekatan forensik digital yang sistematis untuk menelusuri, mengekstraksi, dan menganalisis artefak digital secara efektif. Sejumlah penelitian terdahulu telah dilakukan untuk mengungkap bukti digital pada kasus kejahatan berbasis aplikasi pesan instan, khususnya *WhatsApp*. Penelitian oleh Lee menekankan pentingnya pencegahan dan mitigasi kejahatan siber, namun belum mengelaborasi metode investigasi forensik secara mendalam terutama platform dengan kompleksitas komunikasi terenkripsi seperti *WhatsApp*[6]. Disisi lain Parti menekankan perlunya peningkatan pemahaman teknis dan investigatif terhadap kejahatan dunia maya melalui integrasi metode digital forensik yang sistematis, menerapkan prinsip pengumpulan dan preservasi *digital evidence* untuk menjaga integritas data, serta penyusunan laporan yang mendokumentasikaan tahapan investigasi dan bukti yang ditemukan agar dapat dipertanggungjawabkan dalam proses hukum [7]. penelitian oleh Utami menggunakan metode live forensic pada *WhatsApp* Web untuk pembuktian kasus penipuan transaksi elektronik. Penelitian menunjukkan bahwa waktu akuisisi sangat mempengaruhi keberhasilan pengambilan data karena sifat memori yang *volatile*[8]. Namun penelitian ini masih terbatas pada lingkungan web dan belum menyentuh analisis *database* pada perangkat mobile. Selanjutnya, penelitian oleh Caesar menerapkan metode static forensic untuk menganalisis artefak digital pada media sosial Facebook. Hasilnya menunjukkan bahwa berbagai data metadata dapat ditemukan kembali, namun penelitian ini tidak berfokus pada aplikasi instant messaging seperti *WhatsApp*[9]. Penelitian oleh Sudjayanti menggunakan NIST untuk menganalisis file APK dalam kasus phising berbasis *WhatsApp*. Namun penelitian ini terbatas pada analisis file APK dan tidak mencakup pemulihan artefak komunikasi pengguna[10]. Selain itu, Marzuki menerapkan metode IDFIF pada aplikasi MiChat dengan kombinasi beberapa *tools forensic* seperti MOBILedit, Oxygen Forensic dan SQLite. Dalam penelitian ini, IDFIF berperan dominan sebagai kerangka kerja investigasi yang mengatur seluruh tahapan penanganan barang bukti digital, mulai dari *preparation*, *incident response*, *laboratory process*, hingga *presentation*. Fokus utama penerapan IDFIF adalah memperoleh dan menganalisis bukti digital berupa riwayat percakapan, data aplikasi, serta informasi *smartphone*[11]. Selanjutnya, penelitian oleh Qibriya menemukan bahwa *WhatsApp* memiliki struktur *database* yang memungkinkan proses analisis forensic, berbeda dengan telegram yang tidak menyediakan data percakapan secara local[12]. Hal ini menunjukkan bahwa analisis

berbasis *database* seperti SQLite menjadi pendekatan yang penting dalam investigasi *WhatsApp*.

Berdasarkan telaah penelitian terdahulu, dapat disimpulkan sebagian besar penelitian masih memiliki keterbatasan, seperti fokus pada satu jenis data, penggunaan metode yang belum terintegrasi, atau ketergantungan pada kondisi tertentu dalam proses akuisisi. Oleh arena itu, penelitian ini mengusulkan pendekatan yang lebih terstruktur dengan menerapkan metode IDFIF v2 serta memanfaatkan tools Andriller untuk akuisisi data dan DB Browser for SQLite untuk analisis *database*. Penelitian ini secara khusus pada pemulihan artefak digital berupa pesan teks, gambar, dan video yang telah dihapus pada aplikasi *WhatsApp*, sehingga diharapkan dapat memberikan kontribusi dalam meningkatkan efektivitas investigasi forensic digital.

2. METODE PENELITIAN

Penelitian ini menggunakan pendekatan kualitatif eksperimental dengan skenario simulasi investigasi forensik digital pada perangkat *smartphone* Android yang terpasang aplikasi *WhatsApp*. Tujuan penelitian adalah mengidentifikasi artefak digital yang berkaitan dengan aktivitas pengiriman pesan pada kasus dugaan penipuan online melalui analisis *database* aplikasi. Kerangka kerja investigasi mengacu pada IDFIF v2 yang terdiri dari tahapan *Preparation*, *Incident response*, *Laboratory process*, dan *Presentation*[13]



Gambar 1. Kerangka Berpikir

Tahap *Preparation* dilakukan dengan identifikasi kasus, penyiapan perangkat investigasi, serta penentuan objek bukti digital berupa satu unit *smartphone* Android yang diduga digunakan dalam aktivitas penipuan melalui *WhatsApp*. Perangkat lunak yang digunakan meliputi Andriller sebagai tools akuisisi data perangkat dan DB Browser for SQLite sebagai tool analisis basis data[14][15].

Tahap *incident response* dilakukan dengan mengamankan perangkat, mendokumentasikan kondisi awal, menjaga integritas barang bukti, serta menghubungkan perangkat ke computer investigasi menggunakan kabel USB. Selanjutnya perangkat dipindahkan ke laboratorium forensic untuk proses pemeriksaan lanjutan.

Pada tahap *laboratory process*, dilakukan ekstraksi data menggunakan Andriller. Proses ekstraksi menggunakan Andriller dilakukan melalui beberapa tahapan sistematis. Tahap awal dimulai dengan menghubungkan *smartphone* Android ke komputer investigasi menggunakan kabel USB dan memastikan perangkat telah terdeteksi oleh sistem operasi Kali Linux. Setelah perangkat berhasil dikenali, Andriller digunakan untuk melakukan proses akuisisi logis terhadap data yang tersimpan pada memori perangkat. Hasil ekstraksi menghasilkan sejumlah artefak digital berupa file media, seperti gambar dan video *WhatsApp*, serta file *database* aplikasi Bernama msgstore.db. File *database* tersebut kemudian dianalisis menggunakan SQLite untuk menelusuri riwayat komunikasi pengguna. Analisis difokuskan pada tabel message, chat, jid, dan jid_map. Tahap analisis SQLite dilakukan dengan metode korelasi antar tabel, yaitu menghubungkan data pesan dengan identitas percakapan dan akun tujuan komunikasi. Parameter yang diamati meliputi from_me, chat_row_id, jid_row_id, serta identifier internal @lid yang dipetakan ke nomor telepon.

Tahap terakhir yaitu *presentation*, berupa penyusunan hasil investigasi, dokumentasi artefak digital, interpretasi temuan, dan penarikan kesimpulan.

2.1 Sumber Data

Sumber data terdiri dari data primer berupa hasil ekstraksi langsung dari perangkat Android, serta data sekunder berupa file *database* aplikasi *WhatsApp*. Data primer diperoleh

melalui proses akuisisi menggunakan Andriller yang mengghasilkan artefak digital berupa file media(gambar dan video) serta file *database* utama msgstore.db. data sekunder berupa struktur tabel dan isi *database* dianalisis untuk menemukan hubungan antar data yang relevan dengan aktivitas komunikasi.

Tabel 1. Sumber Data Penelitian

Jenis Data	Sumber	Keterangan
Data Primer	*Smartphone* Androidv(Xiaomi Redmi 4A)	Hasil Akuisisi Langsung
File Media	*WhatsApp*	Gambar dan Video
Database	msgstore.db	Riwayat Komunikasi
Metadata	Tabel SQLite	Informasi aktivitas Pesan
Data Sekunder	Jurnal Literatur	Pendukung Penelitian

2.2 Teknik Pengumpulan Data

Teknik pengumpulan data dilakukan melalui metode akuisisi logis terhadap perangkat, dengan tujuan memperoleh salinan data tanpa mengubah kondisi asli. Tahapan pengumpulan data meliputi identifikasi perangkat, proses ekstraksi data, dokumentasi artefak, dan klasifikasi hasil akuisisi. Tahap pertama dilakukan dengan mengidentifikasi kondisi awal perangkat berupa tipe perangkat, kondisi sistem operasi, serta status aplikasi *WhatsApp* yang digunakan. Tahap berikutnya adalah proses akuisisi menggunakan Andriller untuk memperoleh salinan data yang tersimpan pada perangkat Android. Setelah proses akuisisi selesai, file yang diperoleh diklasifikasikan berdasarkan jenisnya, yaitu media dan *database*. File media digunakan sebagai bukti pendukung aktivitas komunikasi, sedangkan file *database* menjadi objek utama analisis lebih lanjut.

2.3 Analisis Data

Analisis data dilakukan menggunakan DB Browser for SQLite dengan cara menelusuri dan mengkorelasikan beberapa tabel utama dalam *database* msgstore,db, yaitu tabel message, chat, jid, dan jid_map, proses analisis dimulai dengan mengidentifikasi record pada tabel message yang menunjukkan aktivitas pengiriman pesan melalui parameter from_me. Selanjutnya dilakukan penelusuran relasi ke tabel chat untuk mengetahui percakapan yang terlibat, kemudian dilanjutkan ke tabel jid untuk mengidentifikasi akun, dan tabel jid_map untuk memetakan identifier internal ke nomor telepon. Hasil analisis digunakan untuk mengungkap jejak komunikasi yang terjadi pada perangkat.

Penelitian dilakukan menggunakan beberapa komponen yang mendukung proses akuisisi dan analisis data forensic digital. Laptop Lenovo digunakan sebagai perangkat utama untuk menjalankan *tools forensic*, serta sebagai media pengolaan data. Smartohone Xiaomi Redmi 4A berfungsi sebagai objek penelitian yang mengandung artefak digital dari aplikasi *WhatsApp* yang akan dianalisis. Proses akuisis data dilakukan menggunakan Andriller berbasis Linux yang mampu mengekstraksi berbagai jenis data dari perangkat Android. Selanjutnya, analisis data dilakukan menggunakan DB Browser for SQlite untuk mengisentifikasi isi *database* msgstore.db. Kabel USB Micro B digunakan sebagai media penghubung antara *smartphone* dan laptop untuk mendukung proses transfer data. Seluruh proses penelitian dijalankan pada system operasi Kali Linux yang menyediakan lingkungan yang kompatibel dan optimal untuk penggunaan *tools forensic* digital.

Tabel 2. Alat & Bahan

Nama Komponen	Jenis/Tipe	Fungsi
Laptop	Lenovo	Perangkat utama
HP Xiaomi	Redmi 4A	Objek Investigasi
Andriller	Andriller Linux	Tool akuisisi data
SQLite	DB Browser for SQLite	Tool analisis basisdata
Kabel USB	Micro B	Penghubung perangkat
Linux	Kali Linux	Sistem operasi

Penelitian ini menggunakan skenario kasus simulasi penipuan online melalui aplikasi *WhatsApp* pada perangkat Android. Dalam skenario ini, pelaku menyamar sebagai pihak resmi (Bank) dan menghubungi korban melalui pesan *WhatsApp* dengan alasan adanya aktivitas mencurigakan pada akun korban. Pelaku kemudian mengirimkan berbagai bentuk komunikasi berupa pesan teks, gambar tangkapan layar palsu, serta video untuk meyakinkan korban agar mengikuti instruksi yang diberikan. Selanjutnya, korban diminta untuk memberikan kode verifikasi atau melakukan tindakan tertentu yang mengakibatkan kerugian. Setelah berhasil, pelaku mengapus seluruh jeak percakapan, termasuk pesan teks, gambar, dan video untuk menghilangkan bukti digital. Korban kemudian melaporkan kejadian tersebut, dan perangkat *smartphone* korban diamankan sebagai barang bukti untuk dilakukan proses investigasi digital. Adapun *digital evidence* yang dianalisis dalam penelitian ini meliputi file basis data *WhatsApp* (msgstore.db), metadata pesan, informasi akun yang terlibat komunikasi, serta artefak media berupa gambar dan video yang dikirim maupun diterima selama interaksi. Melalui proses akuisisi menggunakan Andriller dan analisis menggunakan DB Browser for SQLite, artefak tersebut diperiksa untuk mengungkap jejak komunikasi yang masih tersimpan maupun yang terhapus. Bukti digital tersebut dianalisis untuk memperoleh informasi mengenai aktivitas komunikasi yang terjadi.

Gambar 2. Simulasi Penipuan Berbasis *WhatsApp*

3. HASIL DAN DISKUSI

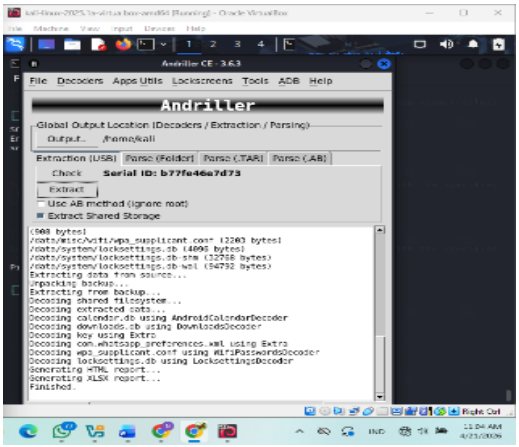
Penelitian ini dilakukan untuk mengungkap dugaan tindak pidana penipuan melalui aplikasi *WhatsApp* pada perangkat Android dengan menerapkan metode Integrated Digital Forensic Investigation Framework v2 (IDFIF v2). Proses investigasi dilakukan melalui tahapan *preparation*, *incident response*, *laboratory process*, dan *presentation*. Hasil penelitian diperoleh dari proses akuisisi menggunakan Andriller serta analisis *database* menggunakan DB Browser for SQLite.

3.1 *Preparation*

Pada tahap *preparation* dilakukan persiapan perangkat investigasi berupa satu unit laptop forensic, kabel USB, *smartphone* Android sebagai barang bukti, serta perangkat lunak Andriller dan DB Browser for SQLite. Selain itu dilakukan penyiapan media penyimpanan hasil ekstraksi dan dokumentasi kondisi awal perangkat.

3.2 *Incident response*

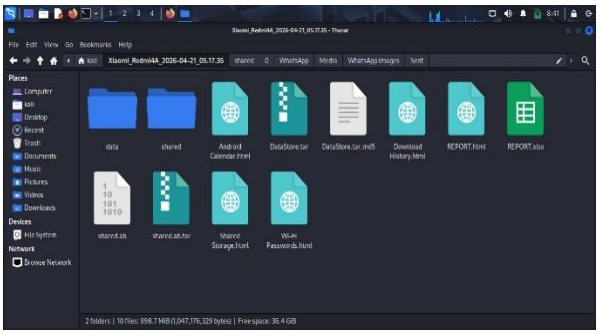
Pada tahap *incident response*, perangkat Android diamankan dan dihubungkan ke computer navigasi. Selanjutnya dilakukan identifikasi kondisi perangkat, status koneksi, dan akses data yang memungkinkan dilakukan ekstraksi. Perangkat kemudian di proses menggunakan Andriller untuk memperoleh data aplikasi *WhatsApp* beserta artefak digital lainnya yang tersimpan pada memori perangkat.



Gambar 3. Proses Ekstraksi Menggunakan Andriller

3.3 *Laboratory process*

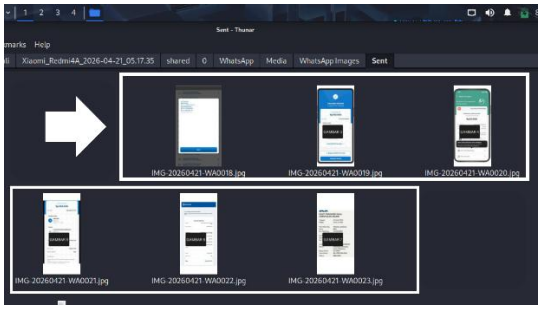
Hasil Ekstraksi Menggunakan Andriller Berdasarkan hasil ekstraksi menggunakan Andriller, diperoleh folder hasil akuisisi dengan total data sebesar 998,7 MiB yang terdiri dari 2 folder dan 10 file. Hasil akuisisi dari andriller menghasilkan file seperti di gambar berikut.



Gambar 4. Folder Hasil Ekstraksi Andriller

Hasil yang berhasil diperoleh dari Andriller yaitu:

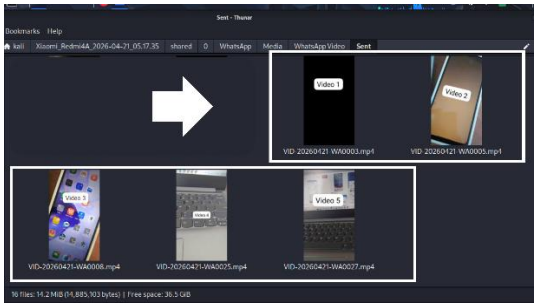
1. Folder data
2. Folder shared
3. File AndroidCalendar.html
4. File DataStore.tar
5. File DataStore.tar.md5
6. File DownloadHistory.html
7. File REPORT.html
8. File REPORT.xlsx
9. File shared.ab
10. File shared.ab.tar
11. File SharedStorage.html
12. File Wi-FiPassword.html



Gambar 5. Folder File Gambar *WhatsApp* yang Terhapus

Gambar menunjukkan Andriller berhasil melakukan akuisisi artefak gambar media *WhatsApp* yang terhapus yaitu:

1. IMG-20260421-WA0018.jpg
2. IMG-20260421-WA0019.jpg
3. IMG-20260421-WA0020.jpg
4. IMG-20260421-WA0021.jpg
5. IMG-20260421-WA0022.jpg
6. IMG-20260421-WA0023.jpg



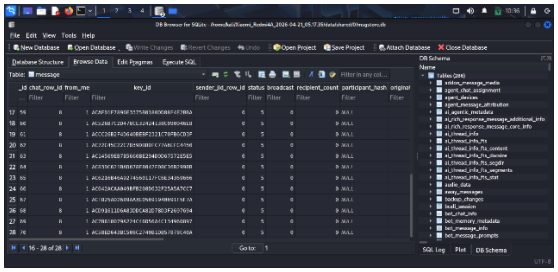
Gambar 6. Folder Video *WhatsApp* yang Terhapus

Gambar tersebut menunjukkan Andriller mampu melakukan Akuisisi terhadap Video Media *WhatsApp* yang terhapus yaitu:

1. VID-20260421-WA0003.mp4
2. VID-20260421-WA0005.mp4
3. VID-20260421-WA0008.mp4
4. VID-20260421-WA0025.mp4
5. VID-20260421-WA0027.mp4

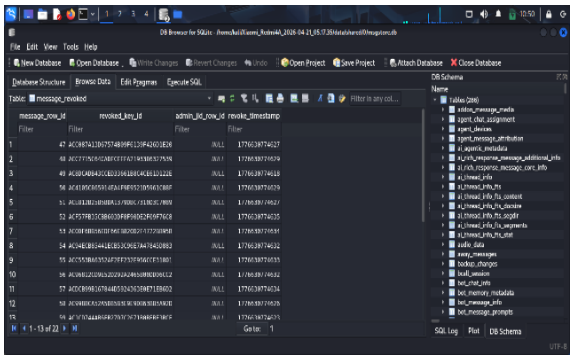
Hasil analisis menggunakan SQLite DB Browser

Dari hasil ekstraksi ditemukan file *database* yaitu msgstore.db. File ini dianalisis menggunakan SQLite untuk mengetahui aktivitas komunikasi yang berkaitan dengan dugaan penipuan



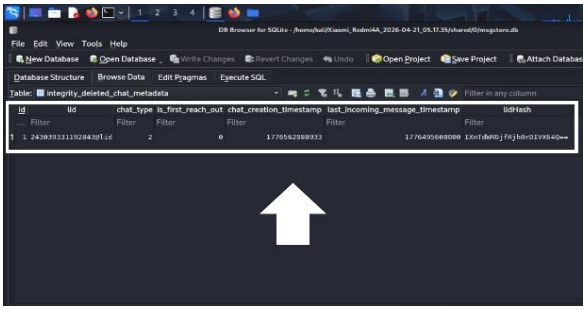
Gambar 7. Gambar Tabel Message

Tabel message merupakan tabel utama yang menyimpan Riwayat komunikasi pada aplikasi *WhatsApp*. Di dalam tabel message menunjukkan adanya sejumlah record dengan nilai from_me=1. Nilai tersebut menunjukkan bahwa perangkat melakukan pengiriman pesan ke akun lain. Beberapa record yang teridentifikasi memiliki ID 47 -68, dengan waktu pengiriman 19 April 2026 sekitar pukul 16.12 WIB. Seluruh pesan tersebut memiliki chat_row_id=8, yang menunjukkan bahwa pesan dikirim dalam satu percakapan yang sama. Nilai chat_row_id pada tabel message ditelusuri ke tabel chat, kemudian dikaitkan ke tabel jid untuk mengetahui identitas tujuan komunikasi. Dari hasil analisis ditemukan identitas 48906926858372@lid. Untuk mengetahui nomor telepon sebenarnya, dilakukan korelasi ke tabel jid_map. Hasil analisis menunjukkan bahwa identitas tersebut dipetakan ke akun: [***17164@s.*WhatsApp*.net](). Dengan demikian dapat dibuktikan bahwa perangkat pernah melakukan komunikasi dengan nomor 62895606417164



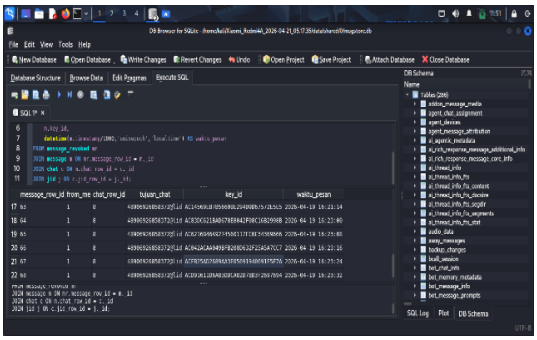
Gambar 8. Tabel message_revooked

Tabel ini menyimpan daftar pesan yang di revoke atau ditarik Kembali menggunakan fitur *WhatsApp*:" Delete for Everyone"



Gambar 9. Tabel Integrity_deleted_chat_metadata

Tabel ini merupakan matadata jejak percakapan yang mengalami penghapusan. Identitas 243039331192843@lid yang terekam di tabel ini.



Gambar 7. Tabel message & message_revooked

Berdasarkan hasil analisis tabel message yang digabungkan dengan message_revoked, ditemukan sebanyak 22 pesan dengan ID 47 hingga 68 yang telah dihapus. Seluruh pesan tersebut memiliki nilai from_me=1, yang menunjukkan bahwa pesan dikirim dari perangkat yang dianalisis. Pesan tersebut ditujukan ke satu identitas yaitu 48906926858372@lid. Selain itu, waktu pengiriman yang berurutan menunjukkan adanya aktivitas komunikasi yang intens sebelum pesan-pesan tersebut dihapus, yang mengindikasikan adanya upaya penghilangan jejak

3.4 *Presentation*

Tabel 3. Artefak Digital Hasil Akuisisi

Jenis Artefak	Jumlah	Keterangan
Gambar	6	Media *WhatsApp* Terhapus

Video	5	Video *WhatsApp* Terhapus
msgstore.db	1	Basisdata Komunikasi
message_revooked	22	Riwayat Pesan Terhapus

Berdasarkan hasil akuisisi, ditemukan beberapa jenis artefak digital yang memiliki keterkaitan dengan aktivitas komunikasi *WhatsApp*. Artefak yang ditemukan meliputi media gambar, video, basisdata, serta metadata penghapusan pesan. Keberadaan artefak tersebut menunjukkan bahwa meskipun pengguna telah melakukan penghapusan data, sebagian informasi masih tersimpan pada struktur sistem aplikasi.

Dari hasil pemeriksaan forensic digital terhadap aplikasi *WhatsApp*, untuk Andriller berhasil mengungkap file media *WhatsApp* berupa gambar dan video. Untuk analisis msgstore.db pada SQLite ditemukan adanya aktivitas komunikasi dengan nomor ***17164 yang disertai penghapusan sejumlah pesan. SQLite tidak mengungkap isi pesan secara langsung, hanya menampilkan jejak pesan yang pernah ada.

4. KESIMPULAN DAN SARAN

Tabel 4. Tingkat Keberhasilan Akuisisi

Jenis Data	Target	Diperoleh	Persentase
Gambar	6	6	100%
Video	5	5	100%
Isi Pesan	10	0	0%
Metadata Pesan	10	10	100%

Berdasarkan hasil akuisisi, tingkat keberhasilan tertinggi terdapat pada pemulihan file media dan metadata pesan, sedangkan isi pesan terhapus belum berhasil dipulihkan secara langsung. Hasil akuisisi menggunakan Andriller berhasil memperoleh artefak digital berupa file media *WhatsApp* yang telah terhapus, yaitu beberapa file gambar berformat .jpg dan video berformat .mp4. temuan ini menunjukkan bahwa data media yang dihapus masih dapat dipulihkan dan dijadikan barang bukti digital. Selanjutnya, analisis basis data msgstore.db menggunakan DB Browser for SQLite berhasil mengungkap adanya aktivitas komunikasi pada aplikasi *WhatsApp*. Dari tabel message ditemukan Riwayat pengiriman pesan dari perangkat yang diperiksa kepada nomor ***17164. Selain itu, melalui tabel message_revoked dan tabel pendukung lainnya ditemukan sebanyak 22 pesan yang telah dihapus menggunakan fitur delete for everyone.Isi pesan tidak dapat dilihat secara langsung di SQLite DB Browser. Metadata yang tersimpan pada *database* mampu menunjukkan identitas lawan komunikasi, waktu aktivitas pesan, serta indikasi penghapusan pesan secara sengaja.

Dengan demikian, kombinasi penggunaan Andriller dan SQLite DB Browser mampu digunakan dalam investigasi forensic digital aplikasi *WhatsApp*, khususnya untuk mengungkap bukti komunikasi, media terhapus, dan indikasi Upaya penghilangan jejak pada kasus dugaan penipuan. Hasil penelitian ini diharapkan dapat menjadi referensi bagi praktisi forensic digital dalam menangani kasus serupa, khususnya dalam pemanfaatan kombinasi tools untuk meningkatkan efektivitas investigasi. Kedepan, studi lanjutan diharapkan dapat mengeksplorasi teknik recovery yang lebih canggih, sehingga mampu meningkatkan keberhasilan dalam mengungkap bukti digital secara lebih komprehensif.

5. DAFTAR PUSTAKA

[1] S. Kemp, “Digital 2025: Indonesia — DataReportal – Wawasan Digital Global,” datareportal.com. Accessed: May 07, 2025. [Online]. Available: https://datareportal.com/reports/digital-2025-indonesia

[2] Wahyuddin, L. F. Ersa, G. Aningsih, T. Hidayat, and A. F. Sonni, “Analisis Jaringan Komunikasi Penipuan Online Melalui Media Sosial *WhatsApp* Messenger,” *Jurnal Netnografi Komunikasi*, vol. 2, no. 2, pp. 33–50, 2024, doi: 10.59408/jnk.v2i2.27.

[3] P. H. Untari, “*WhatsApp* jadi Kanal Terfavorit Penjahat untuk Lakukan Penipuan di Indonesia,” teknologi.bisnis.com. Accessed: Jan. 22, 2026. [Online].

Available: https://teknologi.bisnis.com/read/20251104/84/1926033/*WhatsApp*-jadi-kanal-terfavorit-penjahat-untuk-lakukan-penipuan-di-indonesia

[4] F. Duarte, "Most Popular Messaging Apps (2026)," explodingtopics.com. Accessed: Jan. 21, 2026. [Online]. Available: https://explodingtopics.com/blog/messaging-apps-stats

[5] S. Nishchal, "Forensic Analysis of *WhatsApp*: A Review of Techniques, Challenges, and Future Directions," *Journal of Forensic Science and Research*, vol. 8, no. 1, pp. 019–024, 2024, doi: 10.29328/journal.jfsr.1001059.

[6] C. S. Lee, "Toward Mitigating, Minimizing, and Preventing Cybercrimes and Cybersecurity Risks," *International Journal of Cybersecurity Intelligence & Cybercrime*, vol. 3, no. 2, pp. 1–3, 2020, doi: 10.52306/2578-3289.1072.

[7] K. Parti, D. Ph, and V. Tech, "Book Review: Digital Forensics and Cyber Investigation," *International Journal of Cybersecurity Intelligence & Cybercrime*, vol. 5, no. 3, pp. 68–70, 2022, doi: 10.52306/pybp7047.

[8] S. D. Utami, C. Carudin, and A. A. Ridha, "Analisis Live Forensic Pada *WhatsApp* Web Untuk Pembuktian Kasus Penipuan Transaksi Elektronik," *Cyber Security dan Forensik Digital*, vol. 4, no. 1, pp. 24–32, 2021, doi: 10.14421/csecurity.2021.4.1.2416.

[9] C. R. Caesar, Y. Servanda, and Y. Dwi Atma, "Analisis Forensik Digital Pada Aplikasi Media Sosial Facebook Menggunakan Metode Statik Forensik," *Forbis: Journal Forensic Business Information Systems*, vol. 1, no. 1, pp. 20–26, 2024, [Online]. Available: https://journal.universitasmulia.ac.id/index.php/forbis

[10] S. alya Sudjayanti and D. Hamdani, "Digital Forensic Analysis Of APK Files In Phishing Scams On *WhatsApp* Using The NIST Method," *Brilliance: Research of Artificial Intelligence*, vol. 4, no. 1, pp. 100–110, 2024, doi: 10.47709/brilliance.v4i1.3800.

[11] M. Marzuki and T. Sutabri, "Analisis Forensik Media Sosial Michat Metode Digital Forensik Integrated Investigation Framework (Idfif)," *Blantika : Multidisciplinary Journal*, vol. 2, no. 1, pp. 56–70, 2023, doi: 10.57096/blantika.v2i1.11.

[12] M. R. D. Qibriya, A. Ambarwati, and K. E. Susilo, "Analisis Forensik Digital Pada Aplikasi Instant Messaging Di *Smartphone* Berbasis Android Untuk Bukti Digital," *Jurnal Teknologi Informasi*, vol. 5, no. 2, pp. 114–121, 2021, doi: 10.36294/jurti.v5i2.2200.

[13] F. F. Febrian and J. Sidabutar, "Comparative Analysis of Forensic for *WhatsApp* Desktop on Mac OS and Windows Using IDFIF V2," *Proceedings - 2023 IEEE International Conference on Cryptography, Informatics, and Cybersecurity: Cryptography and Cybersecurity: Roles, Prospects, and Challenges, ICoCICs 2023*, pp. 327–331, 2023, doi: 10.1109/ICOCICS58778.2023.10276727.

[14] M. F. Fadillah, T. Yuniati, F. Informatika, I. Teknologi, and T. Purwokerto, "Perbandingan Hasil Recovery Tools Mobile Forensic Di *Smartphone* Android Menggunakan Metode National Institute Of Justice (NIJ) Comparison Of Mobile Forensic Recovery Tools Results On Android *Smartphone*s Using The National Institute Of Justice (NIJ) Me," vol. 6, no. 2, pp. 54–61, 2023.

[15] N. Hamid, J. Kuswanto, D. Nurani, A. Dwi Putra, F. Mahananing Puri, and S. Tri Atmaja Ramadhani, "Forensic Recovery Techniques on Android Devices with the National Institute of Standards and Technology (NIST) Approach," *JTECS : Jurnal Sistem Telekomunikasi Elektronika Sistem Kontrol Power Sistem dan Komputer*, vol. 4, no. 1, p. 53, 2024, doi: 10.32503/jtecs.v4i1.4676.