Journal of Science and Social Research ISSN 2615 – 4307 (Print)
April 2026, IX (2): 2021 – 2027 ISSN 2615 – 3262 (Online)
Available online at http://jurnal.goretanpena.com/index.php/JSSR

KERANGKA INVESTIGASI FORENSIK WHATSAPP WEB DAN TELEGRAM UNTUK HACKING INVESTIGATION

Syukriadi[1], Romy Aulia[2], Melissa Triandini[3], Amrizal[4]
[1,2,3,4]Politeknik Pertanian Negeri Payakumbuh
e-mail: dosen.syukriadi@gmail.com

Abstract: *Instant messaging platforms are frequently involved in cyber incidents, including attacker coordination, credential sharing, and post-compromise extortion. This study develops a digital forensic investigation framework for WhatsApp Web and Telegram to support hacking investigation through artifact mapping, evidence acquisition, and chain of custody management. The method uses a focused literature review, scenario-based investigation design, and comparative analysis of artifacts across browser, operating system, and application layers. The results produce an artifact taxonomy, an acquisition decision matrix covering logical, file-system, and memory approaches, and concise standard operating procedures to preserve evidence integrity, traceability, and reproducibility. The proposed framework can support institutional incident response teams, internal investigators, and digital forensic practitioners in improving evidence quality and investigation effectiveness.*

Keywords: *Digital Forensics; Whatsapp Web; Telegram; Chain of Custody; Cyber Incident.*

Abstrak: Aplikasi pesan instan sering terlibat dalam insiden keamanan siber, termasuk koordinasi serangan, distribusi kredensial hasil kompromi, dan pemerasan pascainsiden. Penelitian ini mengembangkan kerangka investigasi forensik digital pada WhatsApp Web dan Telegram untuk mendukung hacking investigation melalui pemetaan artefak, akuisisi bukti, dan pengelolaan chain of custody. Metode yang digunakan berupa studi literatur terarah, perancangan skenario investigasi, dan analisis perbandingan artefak pada lapisan browser, sistem operasi, dan aplikasi. Hasil penelitian menghasilkan taksonomi artefak, matriks keputusan akuisisi yang mencakup pendekatan logis, file- system, dan memori, serta prosedur operasional ringkas untuk menjaga integritas, keterlacakan, dan reprodusibilitas bukti. Kerangka yang diusulkan dapat membantu tim respons insiden, penyidik internal, dan praktisi forensik digital dalam meningkatkan kualitas bukti dan efektivitas investigasi.

Kata Kunci: Digital Forensics; Whatsapp Web; Telegram; Chain of Custody; Insiden Siber

PENDAHULUAN

Aplikasi pesan instan (instant messaging/IM) telah menjadi medium komunikasi utama pada lingkungan personal maupun organisasi. Pada saat yang sama, IM kerap muncul sebagai kanal pendukung aktivitas kejahatan siber, mulai dari pengiriman tautan phishing, rekayasa sosial, hingga koordinasi aksi peretasan dan monetisasi akses ilegal. Dari perspektif investigasi, kondisi ini menuntut ketersediaan bukti digital yang valid, baik berupa konten pesan, metadata komunikasi, maupun artefak pendukung seperti berkas lampiran, log akses, dan jejak browser, untuk merekonstruksi kejadian dan menetapkan hipotesis investigasi.

Tantangan utama muncul karena platform IM modern mengedepankan keamanan, seperti end-to-end encryption, tokenisasi sesi, dan arsitektur berbasis cloud, serta memiliki

ragam klien mobile, desktop, dan web. Karakteristik artefak forensik sangat dipengaruhi oleh versi aplikasi, sistem operasi, serta metode penggunaan. Oleh karena itu, pemetaan artefak yang kontekstual menjadi prasyarat penting sebelum proses akuisisi dilakukan (Onik et al., 2025).

WhatsApp Web bergantung pada browser dan mekanisme sinkronisasi dengan perangkat utama. Penelitian terdahulu menunjukkan bahwa artefak penting dapat ditemukan pada penyimpanan browser serta jejak aktivitas pengguna selama sesi berjalan (Utami et al., 2021; Soares, 2022). Analisis forensik browser pada versi terbaru WhatsApp juga mengindikasikan bahwa lokasi dan struktur artefak dapat berubah mengikuti pembaruan platform, sehingga investigasi membutuhkan pendekatan yang adaptif (Utomo et al., 2023).

Telegram memiliki ekosistem berbeda dengan dukungan multi-device dan sinkronisasi berbasis cloud. Artefak penting masih dapat ditemukan pada basis data lokal, direktori aplikasi, dan lingkungan browser, tetapi tingkat keterpulihan data dipengaruhi oleh versi aplikasi dan konfigurasi perangkat (Raza & Hassan, 2022; Pakaya & Riadi, 2023).

Di luar aspek teknis, kualitas pembuktian juga ditentukan oleh integritas dan keterlacakan bukti. Praktik hashing, dokumentasi chain of custody, dan kontrol akses atas barang bukti merupakan elemen kunci untuk menjaga validitas bukti digital. Sejumlah riset bahkan mengusulkan pemanfaatan blockchain untuk memperkuat preservasi bukti multimedia dan mencegah manipulasi pihak ketiga, sementara legalitas bukti elektronik dalam perkara siber tetap mensyaratkan due process dan autentikasi yang dapat diuji di pengadilan (Sakshi et al., 2023; Legality of Electronic Evidence in Cyber Crime Cases, 2024).

Berdasarkan latar tersebut, penelitian ini bertujuan menyusun kerangka investigasi yang memetakan artefak WhatsApp Web dan Telegram, menawarkan matriks pemilihan metode akuisisi logis, berkas, dan memori, serta merumuskan rekomendasi SOP ringkas untuk menjaga integritas dan akuntabilitas proses. Rumusan masalah yang diajukan meliputi artefak apa saja yang relevan untuk investigasi insiden, bagaimana strategi akuisisi yang sejalan dengan prinsip NIJ/NIST, dan bagaimana perancangan chain of custody yang praktis namun tetap dapat dipertanggungjawabkan.

METODE

Desain Kajian Dan Lingkup

Penelitian ini merupakan studi pengembangan kerangka (framework-oriented study) dengan pendekatan studi literatur terarah pada publikasi 2021–2025 yang membahas artefak forensik WhatsApp, WhatsApp Web, Telegram, serta forensik browser. Sintesis literatur tersebut dipadukan dengan prinsip National Institute of Justice (NIJ) dan National Institute of Standards and Technology (NIST) untuk memetakan artefak, memilih metode akuisisi, dan merumuskan prosedur chain of custody. Penelitian tidak memaparkan teknik peretasan, tetapi berfokus pada fase investigasi, preservasi, dan validasi bukti digital.

Skenario Investigasi Dan Sumber Data

Untuk menjaga relevansi terhadap hacking investigation, penelitian menggunakan tiga pola kejadian umum, yaitu komunikasi koordinasi insiden, distribusi berkas atau tautan berisiko, serta pemerasan yang memanfaatkan percakapan dan lampiran digital. Pada setiap skenario, fokus bukti mencakup konten pesan, metadata komunikasi, riwayat akses, cache media, dan jejak unduhan. Sumber data dalam penelitian ini berasal dari publikasi ilmiah, dokumentasi praktik forensik, dan hasil

sintesis konseptual atas artefak yang lazim ditemukan pada browser, sistem operasi, dan aplikasi pesan instan.

Metode Akuisisi Dan Validasi Integritas

Metode akuisisi dibagi menjadi tiga kelas. Pertama, akuisisi logis berupa ekspor percakapan dan ekstraksi artefak yang tersedia melalui fitur resmi. Kedua, akuisisi berkas (file- system acquisition) melalui penyalinan terkontrol terhadap direktori aplikasi atau profil browser sesuai otorisasi. Ketiga, akuisisi memori pada kondisi khusus untuk menangkap konteks sesi yang sedang berjalan. Validasi integritas dilakukan dengan hashing MD5 dan SHA-256 pada setiap artefak, serta pencatatan berjenjang berupa log pengumpulan, log pemrosesan, dan log analisis agar keterlacakan bukti tetap terjaga (Barkem & Sidabutar, 2023; Pakaya & Riadi, 2023; Setiawan & Riadi, 2024; Purwanto & Riadi, 2024).

Analisis Artefak Dan Pemetaan

Analisis artefak memadukan dua sudut pandang, yaitu pemetaan lokasi dan format artefak pada masing-masing platform serta analisis siklus hidup browser sejak instalasi, penggunaan, penutupan, pembersihan, hingga uninstal. Pendekatan ini digunakan untuk memahami persistensi dan volatilitas artefak, sekaligus menyusun taksonomi dan matriks keputusan akuisisi yang relevan bagi konteks investigasi (Raza et al., 2024).

Desain Kajian Dan Lingkup

Penelitian ini merupakan studi pengembangan kerangka (framework-orientedstudy) dengan pendekatan studi literatur terarah pada publikasi 2021–2025 yang membahas artefak forensik WhatsApp, WhatsApp Web, Telegram, serta forensik browser. Sintesis literatur tersebut dipadukan dengan prinsip National Institute of Justice (NIJ) dan National Institute of Standards and Technology (NIST) untuk memetakan artefak, memilih metode akuisisi, dan merumuskan prosedur chain of custody. Penelitian tidak memaparkan Teknik peretasan, tetapi berfokus pada fase investigasi, preservasi, dan validasi bukti digital.

Skenario Investigasi Dan Sumber Data

Untuk menjaga relevansi terhadap hacking investigation, penelitian menggunakan tiga pola kejadian umum, yaitu komunikasi koordinasi insiden, distribusi berkas atau tautan berisiko, serta pemerasan yang memanfaatkan percakapan dan lampiran digital. Pada setiap skenario, fokus bukti mencakup konten pesan, metadata komunikasi, riwayat akses, cache media, dan jejak unduhan. Sumber data dalam penelitian ini berasal dari publikasi ilmiah, dokumentasi praktik forensik, dan hasil sintesis konseptual atas artefak yang lazim ditemukan pada browser, sistem operasi, dan aplikasi pesan instan.

Metode akuisisi dan validasi integritas. Metode akuisisi dibagi menjadi tiga kelas. Pertama, akuisisi logis berupa ekspor percakapan dan ekstraksi artefak yang tersedia melalui fitur resmi. Kedua, akuisisi berkas (files ystem acquisition) melalui penyalinan terkontrol terhadap direktori aplikasi atau profil browser sesuai otorisasi. Ketiga, akuisisi memori pada kondisi khusus untuk menangkap konteks sesi yang sedang berjalan. Validasi integritas dilakukan dengan hashing MD5 dan SHA-256 pada setiap artefak, serta pencatatan berjenjang berupa log pengumpulan, log pemrosesan, dan log analisis agar keterlacakan bukti tetap terjaga (Barkem & Sidabutar, 2023; Pakaya & Riadi, 2023; Setiawan & Riadi, 2024; Purwanto & Riadi, 2024). Analisis artefak dan pemetaan.

Analisis artefak memadukan dua sudut pandang, yaitu pemetaan lokasi dan format artefak pada masing-masing platform serta analisis siklus hidup browser sejak instalasi,

penggunaan, penutupan, pembersihan, hingga uninstal. Pendekatan ini digunakan untuk memahami persistensi dan volatilitas artefak, sekaligus menyusun taksonomi dan matriks keputusan akuisisi yang relevan bagi konteks investigasi (Raza et al., 2024).

HASIL DAN PEMBAHASAN

Taksonomi Artefak WhatsApp Web dan Telegram

Artefak investigasi dikelompokkan ke dalam empat domain utama, yaitu identitas akun dan sesi, konten dan metadata pesan, media dan lampiran, serta jejak aktivitas browser dan sistem. Pengelompokan ini menunjukkan bahwa investigasi pada WhatsApp Web lebih banyak bertumpu pada artefak browser, sedangkan Telegram memerlukan korelasi antara artefak lokal dan sinkronisasi cloud (Utami et al., 2021; Soares, 2022; Raza & Hassan, 2022; Utomo et al., 2023).

Tabel 1. Taksonomi Artefak Investigasi pada WhatsApp Web dan Telegram

Domain Artefak	Contoh Artefak	Sumber	Volatilitas	Catatan Investigasi
Identitas & sesi	ID/nomor akun, token sesi, cookie, waktu login	Profil browser/direktori/ aplikasi	Sedang–tinggi	Memerlukan preservasi cepat serta kontrol privasi dan otorisasi.
Konten & metadata pesan	Teks chat, stempel waktu, kontak, grup/channel	Ekspor chat/basis data aplikasi	Rendah–sedang	Struktur artefak berbeda antara WhatsApp dan Telegram, serta dipengaruhi multi-device.
Media & lampiran	Gambar, dokumen, voice note, thumbnail, path unduhan	Cache browser/folder media	Sedang	Perlu hashing dan korelasi dengan log unduhan serta metadata berkas.
Jejak aktivitas	History, download record, service worker cache, IndexedDB/local storage	Artefak browser & OS	Sedang–tinggi	Sangat dipengaruhi siklus hidup browser dan kebijakan pembersihan data.

Perbandingan Artefak Web Dan Mobile

Perbandingan web dan mobile menunjukkan bahwa WhatsApp Web didominasi oleh artefak cache, cookie, IndexedDB, local storage, dan riwayat unduhan, sedangkan WhatsApp Mobile lebih banyak menyimpan bukti pada basis data aplikasi dan folder media. Telegram cenderung menampilkan kombinasi artefak lokal dan sinkronisasi cloud. Temuan ini menegaskan bahwa strategi akuisisi harus menyesuaikan arsitektur klien dan tingkat volatilitas bukti (Fathiyana et al., 2022; Raza & Hassan, 2022; Pakaya & Riadi, 2023).

Tabel 2. Ringkasan Perbandingan Artefak Dan Metode Pada Web Vs Mobile

Aspek	WhatsApp Web (Browser)	WhatsApp Mobile	Telegram (Mobile/Web)
Artefak dominan	Cache, IndexedDB/storage, cookie, history	Basis data aplikasi, folder media, backup	Basis data lokal, cache, dan web storage yang terhubung sinkronisasi cloud
Risiko hilang	Tinggi akibat logout atau pembersihan data	Sedang akibat penghapusan chat atau overwrite	Sedang karena perbedaan sinkronisasi lokal dan cloud
Metode rujukan	Live/web forensics dan NIJ web IM	NIST/DFRWS mobile forensics	NIST mobile forensics, artefak Android, dan NIJ web IM
Strategi validasi	Hash dan korelasi timeline browser	Hash dan korelasi media serta basis data	Hash dan korelasi artefak lokal-cloud sesuai kewenangan

Integritas, Chain of Custody, dan Kesiapan Pembuktian

Berdasarkan literatur, isu yang paling sering mempengaruhi keterterimaan bukti adalah integritas dan keterlacakan. Pada investigasi berbasis browser, perubahan kecil seperti refresh halaman, pembersihan cache, atau logout dapat mengubah atau menghapus artefak penting. Karena itu, analisis siklus hidup browser membantu menentukan prioritas pengumpulan dan mencegah kontaminasi bukti (Raza et al., 2024).

Penguatan chain of custody dapat dilakukan melalui praktik minimal berupa identifikasi barang bukti, pencatatan kronologi tindakan, hashing artefak, serta penyimpanan pada media terproteksi. Untuk organisasi yang memerlukan assurance lebih kuat, preservasi berbasis ledger atau blockchain dapat diadaptasi sebagai mekanisme pencatatan hash dan jejak akses yang lebih sulit dimodifikasi (Sakshi et al., 2023).

Dari sisi hukum, legalitas bukti elektronik pada perkara kejahatan siber mensyaratkan bahwa bukti diperoleh secara sah, relevan, dan dapat diautentikasi. Oleh sebab itu, SOP investigasi harus menjamin adanya dasar otorisasi, prinsip minimalisasi data, dan dokumentasi lengkap agar proses dapat diuji secara adversarial (Legality of Electronic Evidence in Cyber Crime Cases, 2024).

Di samping itu, visualisasi berbasis exploratory data analysis dapat membantu penyidik memahami pola waktu, relasi pengirim-penerima, serta distribusi media pada volume data percakapan yang besar tanpa mengubah bukti asli (Pirzada et al., 2024).

Rekomendasi Implementasi dan SOP Ringkas

Kerangka yang diusulkan menghasilkan matriks keputusan akuisisi yang dapat diterapkan secara praktis. Prinsip utamanya adalah memilih metode paling minimal namun tetap memadai untuk menjawab pertanyaan investigasi, kemudian melakukan eskalasi ke metode yang lebih invasif hanya ketika diperlukan dan telah memiliki otorisasi.

- Jika tujuan hanya untuk verifikasi konteks komunikasi, investigator dapat memprioritaskan ekspor chat atau metadata resmi, disertai dokumentasi visual dan hashing berkas hasil ekspor.
- Jika kasus menuntut rekonstruksi aktivitas sesi web, preservasi profil browser, cache, dan web storage

perlu diprioritaskan dengan meminimalkan interaksi yang dapat memicu logout atau perubahan data.
- Jika terdapat indikasi penghapusan bukti atau volatilitas tinggi, akuisisi memori atau snapshot sistem dapat dipertimbangkan melalui prosedur forensik internal yang terdokumentasi.
- Selalu lakukan korelasi lintas-sumber antara ekspor chat, cache media, riwayat unduhan, dan timeline browser atau sistem untuk meningkatkan keyakinan temuan.

Rekomendasi SOP minimum yang dihasilkan mencakup lima langkah utama: penetapan otorisasi dan ruang lingkup, isolasi serta stabilisasi perangkat, akuisisi terukur sesuai matriks keputusan, hashing dan penyimpanan artefak pada media terproteksi, serta analisis pada working copy dengan pelaporan metode, batasan, dan indikator keyakinan. Secara institusional, implementasi kerangka ini dapat ditindaklanjuti melalui penyusunan kebijakan evidence handling, pelatihan tim respons insiden, pembuatan checklist akuisisi per-platform, serta pembaruan berkala terhadap perubahan versi aplikasi dan browser (Sihombing et al., 2024).

SIMPULAN

Penelitian ini menghasilkan kerangka investigasi forensik untuk WhatsApp Web dan Telegram yang relevan bagi kebutuhan incident investigation dan hacking investigation di organisasi. Kerangka tersebut memadukan taksonomi artefak, strategi akuisisi berdasarkan prinsip NIJ/NIST, serta perhatian khusus pada siklus hidup browser dan chain of custody. Luaran praktis berupa matriks keputusan akuisisi dan SOP minimum dapat membantu menjaga integritas dan keterlacakan bukti digital, sekaligus meningkatkan efektivitas investigasi. Keterbatasan penelitian terletak pada belum dilakukannya uji eksperimental lintas-perangkat, lintas-versi aplikasi, dan lintas-browser secara menyeluruh, sehingga penelitian berikutnya perlu melakukan benchmarking terkontrol untuk memperkaya basis bukti empiris.

UCAPAN TERIMA KASIH

Penulis menyampaikan terima kasih kepada institusi dan rekan sejawat yang telah memberikan masukan dalam penyusunan kerangka kerja ini.

DAFTAR PUSTAKA

Barkem, W., & Sidabutar, J. (2023). Digital forensic analysis of WhatsApp Business applications on Android-based smartphones using NIST. MATRIK: Jurnal Manajemen Teknik Informatika dan Rekayasa Komputer, 22(3), 615–626. https://doi.org/10.30812/matrik.v22i3.3033

Fathiyana, R. Z., Yudiansyah, Cahyadi, N., & Hidayat, D. J. (2022). A comparative study and analysis of forensic artifacts of WhatsApp and Telegram on Android devices. Journal of Informatics and Communication Technology, 4(2), 109–118.

Legality of electronic evidence in cyber crime cases. (2024). Ahmad Dahlan Indonesian Law Journal, 1(2), 11–19. https://doi.org/10.12928/adil.v1i1.572

Onik, A. R., Brown, J., Walker, C., & Baggili, I. (2025). A systematic literature review of secure instant messaging applications from a digital forensics perspective. ACM Computing Surveys. https://doi.org/10.1145/3727641

Pakaya, L. C., & Riadi, I. (2023). Forensic analysis of web-based instant messenger applications using the National Institute of

Justice method. International Journal of Computer Applications, 185(35), 44–51. https://doi.org/10.5120/ijca2023923145

Pirzada, S., Ab Rahman, N. H., Cahyani, N. D. W., & Othman, M. F. (2024). A framework of forensic analysis and visualization: Using WhatsApp chat data as a case study. Journal of Object, Vision and Information, 8(3-2), 1834–1848. https://doi.org/10.62527/joiv.8.3-2.2868

Purwanto, E., & Riadi, I. (2024). Digital forensic mobile Telegram services in online gambling case using National Institute of Standards and Technology method. International Journal of Computer Applications, 186(35), 44–54. https://doi.org/10.5120/ijca2024923926

Raza, A., & Hassan, M. B. (2022). Digital forensic analysis of Telegram Messenger app in Android virtual environment. Mobile and Forensics, 4(1), 31–43. https://doi.org/10.12928/mf.v4i1.5537

Raza, A., Hussain, M., Tahir, H., Zeeshan, M., Raja, M. A., & Jung, K.-H. (2024). Forensic analysis of web browsers lifecycle: A case study. Journal of Information Security and Applications, 85, 103839. https://doi.org/10.1016/j.jisa.2024.103839

Sakshi, Malik, A., & Sharma, A. K. (2023). Blockchain-based digital chain of custody multimedia evidence preservation framework for Internet-of-Things. Journal of Information Security and Applications. https://doi.org/10.1016/j.jisa.2023.103579

Setiawan, D., & Riadi, I. (2024). Mobile forensic WhatsApp services in online fraud cases using Digital Forensics Research Workshop methods. International Journal of Computer Applications, 186(34), 49–56. https://doi.org/10.5120/ijca2024923908

Sihombing, R. P., Kusno, & Siregar, A. A. (2024). Investigative effectiveness in the digital era: A case study of technological innovation at the Rokan Hilir Police Resort. SIGn Jurnal Hukum, 6(2), 52–67. https://doi.org/10.37276/sjh.v6i2.368

Soares, A. M. M. (2022). WhatsApp Web client live forensics technique. In Proceedings of the 8th International Conference on Information Systems Security and Privacy. https://doi.org/10.5220/0010972100003122

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.2021.4.1.241 6

Utomo, L., Prayudi, Y., & Ramadhani, S. (2023). Forensic web analysis on the latest version of WhatsApp Browser. Journal of Computer Networks, Architecture and High Performance Computing, 5(1), 673–682. https://doi.org/10.47709/cnahpc.v5i1.2286