BULLETIN OF COMPUTER SCIENCE RESEARCH
ISSN 2774-3659 (Media Online)
Vol 6, No 3, April 2026 | Hal 1016-1025
https://hostjournals.com/bulletincsr
DOI: 10.47065/bulletincsr.v6i3.1086

Persistensi Artefak Telegram Web pada Memori Setelah Perubahan Sistem dengan Metode NIST SP 800-86

Sigit Puspito Wigati Jarot, Lukman Rosyidi, Haura Tsabitah*

Program Studi Teknik Informatika, Sekolah Tinggi Teknologi Terpadu Nurul Fikri, Depok, Indonesia
Email: [1]sigit.jarot@nurulfikri.ac.id, [2]lukman@nurulfikri.ac.id, [3,*]haur22242ti@student.nurulfikri.ac.id
Email Penulis Korespondensi: haur22242ti@student.nurulfikri.ac.id

Abstrak−Meningkatnya kasus *cyberbullying* melalui platform komunikasi daring menimbulkan tantangan signifikan dalam pembuktian digital, khususnya ketika pelaku menghapus seluruh riwayat pesan. Telegram Web sebagai platform pesan berbasis *browser* menghasilkan artefak digital yang bersifat volatil karena data aktivitasnya tersimpan dalam memori sistem (RAM). Penelitian ini bertujuan menganalisis persistensi artefak digital Telegram Web pada memori volatil berdasarkan enam variasi kondisi perangkat menggunakan *framework* NIST SP 800-86, sebagai upaya mengisi kesenjangan penelitian yang belum mengevaluasi pengaruh kondisi akuisisi secara kuantitatif pada platform berbasis *browser*. Simulasi *cyberbullying* dilakukan melalui *private chat* Telegram yang menghasilkan 10 artefak digital berupa pesan teks, gambar, dokumen, dan *file* audio yang seluruhnya kemudian dihapus oleh pelaku. Akuisisi memori dilakukan menggunakan Exterro FTK Imager pada enam kondisi: sesaat setelah kejadian, *sleep*, *hibernate*, *browser* ditutup, *browser* ditutup disertai penggunaan aplikasi lain, dan *shutdown*. Identifikasi artefak dilakukan melalui *keyword-based analysis* pada *memory image*. Hasil menunjukkan bahwa tiga kondisi pertama menghasilkan tingkat temuan 100% karena RAM mempertahankan data proses Chrome melalui mekanisme *self-refresh* DRAM (ACPI S3) dan penyalinan *byte-for-byte* ke hiberfil.sys (ACPI S4). Penutupan *browser* menurunkan temuan menjadi 40%, penggunaan aplikasi lain mereduksinya menjadi 10% akibat operasi *zero-fill* pada halaman memori yang dialokasikan ulang, dan *shutdown* menghasilkan 0% karena seluruh muatan kapasitor DRAM hilang. Temuan ini membuktikan bahwa tingkat keberadaan artefak dapat diprediksi dari mekanisme arsitektur memori komputer, sekaligus memberikan panduan empiris bagi praktisi forensik digital pada kasus kejahatan siber berbasis platform web.

Kata Kunci: Akuisisi Memori; Cyberbullying; Forensik Digital; NIST SP 800-86; Telegram Web

Abstract−The increasing incidence of cyberbullying on online communication platforms presents significant challenges for digital forensic investigations, particularly when perpetrators delete all message histories. Telegram Web, a browser-based messaging platform, produces volatile digital artifacts because its activity data is stored in system memory (RAM). This study aims to analyze the persistence of Telegram Web digital artifacts in volatile memory under six device condition variations using the NIST SP 800-86 framework, addressing a research gap in the quantitative evaluation of acquisition conditions for browser-based platforms. A cyberbullying simulation was conducted via Telegram private chat, generating 10 digital artifacts text messages, images, a document, and an audio file all subsequently deleted by the perpetrator. Memory acquisition was performed using Exterro FTK Imager under six conditions: immediately post-incident, sleep mode, hibernate mode, browser closed, browser closed with subsequent application use, and shutdown. Artifact identification employed keyword-based analysis on memory images. Results show that the first three conditions yielded 100% artifact recovery, as RAM preserved Chrome process data through DRAM self-refresh (ACPI S3) and byte-for-byte copying to hiberfil.sys (ACPI S4). Closing the browser reduced recovery to 40%, subsequent application use further reduced it to 10% due to zero-fill operations on reallocated memory pages, and shutdown produced 0% as all DRAM capacitor charges were lost. These findings demonstrate that artifact recovery rates are predictable from computer memory architecture, providing empirical guidance for digital forensic practitioners in web-based cybercrime cases.

Keywords: Cyberbullying; Digital Forensics; Memory Acquisition; NIST SP 800-86; Telegram Web

1. PENDAHULUAN

Media sosial telah menjadi infrastruktur komunikasi utama dalam kehidupan digital masyarakat modern karena kemudahan akses dan jangkauannya yang luas [1]. Namun, di balik manfaat tersebut, media sosial juga memunculkan dampak negatif yang signifikan, salah satunya berupa *cyberbullying*—tindakan perundungan yang dilakukan melalui platform komunikasi daring. Berdasarkan laporan Interpol tahun 2024, insiden kejahatan digital di kawasan Asia Tenggara meningkat hingga 60% dibandingkan tahun sebelumnya dan sebagian besar melibatkan platform komunikasi daring [2]. Dampaknya tidak hanya bersifat material, tetapi juga menyentuh kondisi psikologis, reputasi, dan privasi korban di ruang digital [3].

Telegram menjadi salah satu platform yang paling banyak digunakan, dengan lebih dari 900 juta pengguna aktif global dan sekitar 31,5 juta di Indonesia [4]. Fitur *end-to-end encryption*, penyimpanan berbasis *cloud*, dan akses lintas platform menjadikan Telegram populer sekaligus menantang bagi investigasi forensik digital [5]. Selain versi *mobile* dan *desktop*, Telegram juga dapat diakses melalui *browser* (Telegram Web) yang memanfaatkan mekanisme penyimpanan sisi klien (*client-side storage*) seperti *cache* dan IndexedDB, serta data yang tersimpan sementara di RAM selama sesi berlangsung [6], [7]. Karakteristik ini menyebabkan artefak Telegram Web bersifat lebih volatil dan rentan hilang ketika sesi *browser* berakhir, perangkat dimatikan, atau riwayat *browser* dibersihkan [8], [9], [10], [11].

Dalam konteks hukum, meningkatnya kasus kejahatan siber menuntut pembuktian berbasis artefak elektronik yang valid [12]. Di Indonesia, bukti elektronik telah diakui melalui UU ITE No. 11 Tahun 2008 dan Perma No. 1 Tahun 2019 yang mengatur tata cara pengelolaan bukti elektronik dalam persidangan [13], [14]. Permasalahannya, artefak dari aplikasi pesan instan mudah dihapus atau dimanipulasi oleh pelaku, sehingga keaslian dan integritasnya kerap menjadi tantangan dalam proses pembuktian [15], [16], [17]. Secara khusus pada Telegram Web, ketika pelaku menghapus seluruh riwayat percakapan, tidak ada indikator visual penghapusan yang tertinggal berbeda dengan aplikasi seperti WhatsApp

BULLETIN OF COMPUTER SCIENCE RESEARCH
ISSN 2774-3659 (Media Online)
Vol 6, No 3, April 2026 | Hal 1016-1025
https://hostjournals.com/bulletincsr
DOI: 10.47065/bulletincsr.v6i3.1086

yang masih menampilkan keterangan pesan dihapus. Kondisi ini menjadikan RAM sebagai satu-satunya sumber bukti yang dapat dianalisis oleh investigator.

Sejumlah penelitian sebelumnya telah mengkaji forensik digital pada Telegram dengan pendekatan yang beragam. Studi pada platform Android mengidentifikasi artefak pesan, media, dan *metadata* dari basis data SQLite aplikasi [18], sementara penelitian pada kasus perjudian *online* berbasis Android menekankan integritas dan pelaporan forensik [19]. Pada iOS, mekanisme *sandboxing* membatasi akses artefak sehingga bukti yang dapat dipulihkan lebih sedikit [20]. Telegram Desktop menunjukkan persistensi artefak lebih tinggi karena tersimpan pada direktori lokal sistem *file* pengguna [21], [22], sedangkan pendekatan *network forensics* terbukti tidak dapat mengakses isi pesan akibat enkripsi *end-to-end*, menjadikan analisis sisi klien jauh lebih relevan untuk pembuktian konten komunikasi [23]. Kajian pendukung pada forensik *browser* [24] dan analisis IndexedDB berbasis Chromium [8] juga mengonfirmasi bahwa artefak sesi web dapat tersimpan di memori dan diidentifikasi melalui *memory image* relevan langsung dengan cara kerja Telegram Web.

Perbedaan karakteristik penyimpanan antarplatform Telegram menjadi aspek penting yang perlu dipahami dalam konteks forensik digital. Telegram Mobile menyimpan artefak secara persisten dalam basis data SQLite pada *internal storage* perangkat, sementara Telegram Desktop menyimpannya pada direktori lokal sistem *file* pengguna keduanya bersifat *non-volatile* dan dapat diakses bahkan setelah perangkat dimatikan [21], [22]. Sebaliknya, Telegram Web sepenuhnya mengandalkan mekanisme berbasis *browser* sehingga artefak yang dihasilkan bersifat sementara dan sangat bergantung pada kondisi sistem saat sesi berlangsung. Ketika sesi berakhir, *browser* ditutup, atau perangkat mengalami perubahan kondisi, artefak berpotensi hilang tanpa dapat dipulihkan melalui metode konvensional [9], [10]. Perbedaan mendasar ini menjadikan Telegram Web sebagai objek penelitian yang relevan sekaligus menantang, karena belum ada standar pendekatan forensik yang secara khusus mempertimbangkan variasi kondisi sistem dalam analisis artefak berbasis *browser*.

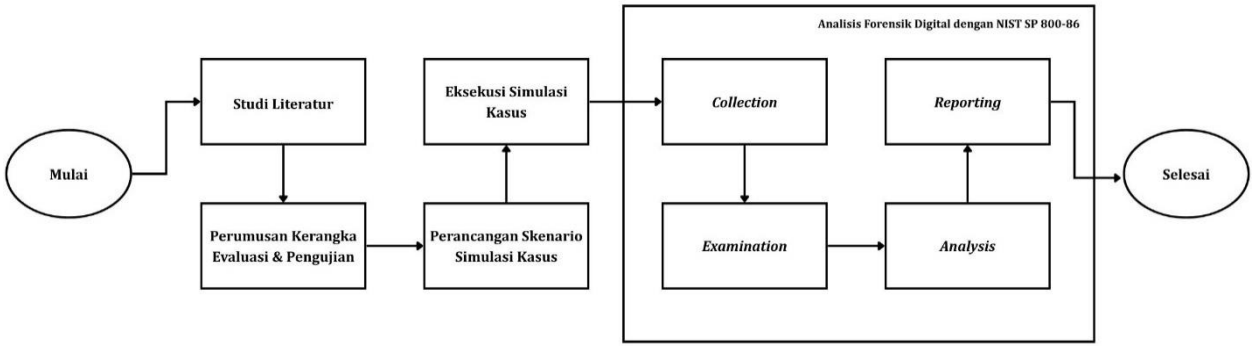
Kajian khusus pada Telegram Web masih sangat terbatas dan sebagian besar bersifat deskriptif. Penelitian [25] mengidentifikasi jenis artefak pada *browser,* namun belum mengevaluasi pengaruh kondisi teknis perangkat. Penelitian [26], [27], [28] menganalisis Telegram Web menggunakan metode DFRWS dalam konteks kasus tertentu, namun tidak mempertimbangkan variasi kondisi akuisisi sebagai variabel. Studi pada WhatsApp Web [29] menunjukkan artefak dapat dipulihkan dari RAM dalam kondisi tertentu, tetapi belum menguji pengaruh perubahan kondisi sistem terhadap ketersediaannya. Dengan demikian, belum ada penelitian yang mengevaluasi secara kuantitatif bagaimana variasi kondisi perangkat seperti *sleep*, *hibernate*, penutupan *browser*, hingga *shutdown* memengaruhi persistensi artefak Telegram Web di RAM. Dari berbagai *framework* forensik yang ada (DFRWS, NIJ, IDFIF, ISO/IEC 27037), NIST SP 800-86 dipilih karena unggul dalam konsistensi analisis artefak volatil dan relevansinya untuk investigasi berbasis memori [30], [31], [32].

Berdasarkan permasalahan tersebut, penelitian ini bertujuan menganalisis persistensi artefak digital Telegram Web pada RAM berdasarkan enam variasi kondisi perangkat sebelum akuisisi dilakukan. Investigasi menggunakan *framework* NIST SP 800-86 yang meliputi tahapan *collection*, *examination*, *analysis*, dan *reporting* [33]. Selain itu, penelitian ini berkontribusi dalam mengisi kesenjangan penelitian terdahulu yang belum mengevaluasi pengaruh variasi kondisi akuisisi terhadap persistensi artefak Telegram Web secara kuantitatif, sekaligus menghasilkan panduan empiris bagi praktisi forensik digital dalam menentukan strategi akuisisi bukti yang efektif pada kasus *cybercrime* berbasis platform web.

2. METODOLOGI PENELITIAN

2.1 Tahapan dan Lingkungan Penelitian

Penelitian ini dirancang sebagai studi komparatif forensik digital dengan pendekatan simulasi skenario yang terkontrol. Alur penelitian disusun secara bertahap mulai dari studi literatur, perancangan skenario simulasi, pelaksanaan simulasi, akuisisi memori pada enam variasi kondisi perangkat, analisis artefak, hingga pelaporan hasil. Gambar 1 merupakan diagram alir penelitian yang menunjukkan tahapan penelitian yang disusun berurutan untuk memastikan keterlacakan antara aktivitas simulasi, artefak yang terbentuk, dan hasil analisis forensik.



Gambar 1. Alur Tahapan Penelitian

BULLETIN OF COMPUTER SCIENCE RESEARCH
ISSN 2774-3659 (Media Online)
Vol 6, No 3, April 2026 | Hal 1016-1025
https://hostjournals.com/bulletincsr
DOI: 10.47065/bulletincsr.v6i3.1086

Seluruh aktivitas investigasi dipusatkan pada perangkat korban (K) yang mengakses Telegram Web melalui Google Chrome, sebagai representasi penggunaan yang paling umum. Penelitian ini secara khusus memosisikan RAM sebagai sumber utama artefak digital yang bersifat volatil, sehingga kondisi sistem saat akuisisi menjadi variabel penelitian yang kritis. Asumsi yang dibangun adalah bahwa artefak yang dianalisis berasal dari aktivitas simulasi yang terkontrol tanpa intervensi eksternal, sehingga akan mencerminkan hubungan langsung antara variasi kondisi sistem dan tingkat persistensi artefak. Spesifikasi perangkat yang digunakan korban ditunjukkan pada Tabel 1, yang merinci komponen utama perangkat yang digunakan, mulai dari spesifikasi perangkat keras hingga versi *browser* yang diuji. Konfigurasi ini dipilih karena merepresentasikan perangkat kelas menengah yang umum digunakan, sehingga hasil penelitian relevan dengan kondisi nyata di lapangan.

Tabel 1. Spesifikasi Sistem Perangkat Korban

Komponen	Spesifikasi
Perangkat	Dell Latitude 5490
Sistem Operasi	Windows 11 Pro 64-bit (Build 26200)
Prosesor	Intel Core i5-8350U @ 1.70 GHz
RAM	16 GB
Browser	Google Chrome
Versi *Browser*	144.0.7559.133 (64-bit)

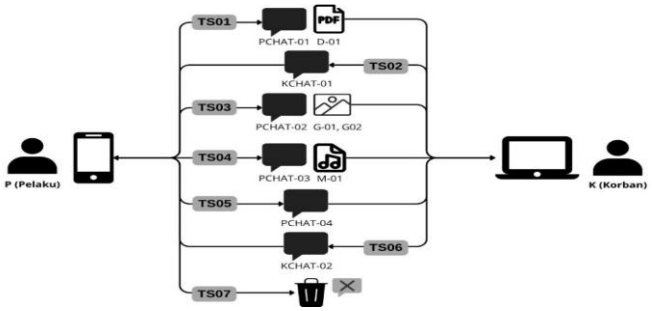
2.2 Perancangan dan Pelaksanaan Skenario Simulasi *Cyberbullying*

Skenario simulasi dirancang untuk merepresentasikan kasus *cyberbullying* nyata yang melibatkan dua aktor, yakni pelaku (P) menggunakan Telegram Mobile pada Android dan korban (K) menggunakan Telegram Web melalui Chrome. Detail aktor beserta seluruh artefak uji yang digunakan dalam simulasi didokumentasikan pada Tabel 2 yang memetakan dua aktor dan 12 item artefak uji yang terdiri dari empat jenis: pesan teks (PCHAT-01–04 dan KCHAT-01–02), gambar (G-01–02), dokumen (D-01), dan *file* audio (M-01). Keberagaman tipe artefak ini dirancang untuk merepresentasikan variasi konten komunikasi yang umum terjadi dalam kasus *cyberbullying* nyata, serta untuk menguji apakah karakteristik format data berpengaruh terhadap tingkat persistensinya di memori.

Tabel 2. Daftar Aktor dan Artefak Uji dalam Skenario Simulasi

Kode	Deskripsi Aktor / Artefak Uji
P	Pelaku *cyberbullying* menggunakan Telegram Mobile (Android)
K	Korban menggunakan Telegram Web melalui Google Chrome (komputer Windows)
PCHAT-01	Pesan *bullying* 1 dari pelaku
PCHAT-02	Pesan *bullying* 2 dari pelaku
PCHAT-03	Pesan *bullying* 3 dari pelaku
PCHAT-04	Pesan *bullying* 4 dari pelaku
KCHAT-01	Pesan balasan 1 dari korban
KCHAT-02	Pesan balasan 2 dari korban
G-01	Gambar *meme* 1 dikirim pelaku (.jpg)
G-02	Gambar *meme* 2 dikirim pelaku (.jpg)
D-01	Dokumen daftar kejelekan korban dikirim pelaku (.pdf)
M-01	*File* audio menjelek-jelekkan korban dikirim pelaku (.mp3)

Interaksi antara pelaku dan korban dijalankan dalam tujuh tahapan kronologis berkode TS01–TS07, mulai dari pengiriman pesan *bullying* pertama (TS01) hingga penghapusan seluruh riwayat percakapan oleh pelaku (TS07). Visualisasi alur interaksi antaraktor ditampilkan pada Gambar 2, yang menggambarkan tujuh tahapan kronologis dari TS01 (pengiriman pesan *bullying* pertama) hingga TS07 (penghapusan seluruh riwayat percakapan oleh pelaku). Pada TS07, seluruh pesan dihapus dari antarmuka Telegram Web di sisi korban tanpa meninggalkan indikator visual—kondisi ini mensimulasikan skenario nyata di mana korban tidak sempat melakukan dokumentasi percakapan sebelum bukti dihapus.



Gambar 2. Diagram Alur Interaksi Skenario Kasus Antara Pelaku (P) dan Korban (K)

BULLETIN OF COMPUTER SCIENCE RESEARCH
ISSN 2774-3659 (Media Online)
Vol 6, No 3, April 2026 | Hal 1016-1025
https://hostjournals.com/bulletincsr
DOI: 10.47065/bulletincsr.v6i3.1086

2.3 Proses Investigasi Forensik Berbasis NIST SP 800-86

Investigasi forensik digital dilaksanakan mengacu pada *framework* NIST SP 800-86. *Framework* ini merupakan panduan yang diterbitkan oleh National Institute of Standards and Technology (NIST) untuk mendukung proses investigasi forensik digital secara sistematis dan terstandar [33]. *Framework* ini mendefinisikan empat tahap utama investigasi digital *collection*, *examination*, *analysis*, dan *reporting* yang dirancang untuk memastikan integritas dan keterlacakan bukti digital dari tahap pengumpulan hingga pelaporan. Dibandingkan dengan *framework* lain seperti DFRWS, NIJ, dan ISO/IEC 27037, NIST SP 800-86 dinilai lebih unggul dalam memberikan panduan teknis yang spesifik untuk penanganan data volatil, termasuk akuisisi memori *live* [30], [31], [32]. Salah satu prinsip kunci dalam NIST SP 800-86 adalah *order of volatility*, yaitu prioritas akuisisi data berdasarkan tingkat volatilitasnya, di mana RAM menjadi prioritas utama karena datanya dapat hilang dalam hitungan milidetik saat daya terputus [9], [11]. Prinsip ini menjadi landasan metodologis penelitian dengan menjadikan kondisi sistem saat akuisisi sebagai variabel penting yang memengaruhi keberhasilan perolehan artefak digital.

Pada tahap *collection*, perangkat korban diamankan sebagai objek investigasi utama untuk mencegah perubahan data yang dapat memengaruhi integritas artefak. Tahap *examination* dilakukan melalui proses *memory acquisition* menggunakan Exterro FTK Imager. *Tool* ini dipilih karena kemampuannya melakukan akuisisi *live* RAM secara *byte-for-byte* tanpa mengubah data pada sistem yang sedang berjalan [34]. Akuisisi dijalankan pada enam variasi kondisi perangkat sebagaimana dirancang dalam penelitian, sehingga menghasilkan enam *file memory image* berformat .mem. Variasi kondisi ini disusun berdasarkan asumsi realistis bahwa dalam praktik investigasi lapangan, perangkat tidak selalu berada dalam kondisi ideal saat pertama kali ditemukan. Ringkasan enam kondisi akuisisi disajikan pada Tabel 3 yang merinci keenam variasi kondisi akuisisi beserta deskripsi teknisnya. Urutan kondisi disusun dari yang paling ideal bagi investigator (kondisi 1) hingga yang paling merugikan dari sisi forensik (kondisi 6), yang merepresentasikan spektrum penuh situasi yang mungkin ditemui dalam investigasi nyata. Proses akuisisi diawali dengan konfigurasi *capture memory* pada antarmuka FTK Imager, di mana pengguna menentukan direktori penyimpanan dan nama *file memory image* sesuai dengan kondisi pengujian. Selama proses berlangsung, FTK Imager menampilkan progres akuisisi secara *real-time* hingga seluruh isi RAM berhasil direkam.

Tabel 3. Variasi Kondisi Perangkat Sebelum Akuisisi Memori

No	Kondisi Akuisisi	Deskripsi
1	Sesaat setelah kejadian	Akuisisi dilakukan segera setelah interaksi selesai; *browser* & sistem masih aktif penuh
2	*Sleep*	Perangkat sempat dalam kondisi *sleep* (ACPI S3) tanpa menutup *browser*
3	*Hibernate*	Perangkat sempat dalam kondisi *hibernate* (ACPI S4) tanpa menutup *browser*
4	*Browser* ditutup	*Browser* ditutup, komputer masih menyala, tanpa aktivitas lanjutan
5	*Browser* ditutup + aktivitas lanjutan	*Browser* ditutup, perangkat digunakan untuk menjalankan aplikasi lain
6	*Shutdown*	Perangkat sempat dimatikan (*shutdown*) sebelum akuisisi dilakukan

2.4 Analisis Artefak dan Perhitungan Kuantitatif

Pada tahap *analysis*, setiap *memory image* diperiksa menggunakan teknik *keyword-based analysis* melalui fitur *Find* pada Exterro FTK Imager. Kata kunci yang digunakan mencakup fragmen isi pesan *bullying* dan nama *file* artefak yang dikirimkan selama simulasi. Pendekatan *keyword-based* dipilih karena data pada *memory image* tidak tersimpan dalam struktur *file* yang utuh, melainkan dalam bentuk fragmen data tersebar, sehingga pencarian berbasis kata kunci merupakan metode yang efektif dan terstandar untuk mengidentifikasi jejak artefak digital [34]. Setiap artefak yang berhasil ditemukan dikonfirmasi melalui tampilan fragmen data yang cocok dengan kata kunci (nilai = 1), sedangkan artefak yang tidak ditemukan menghasilkan kondisi *string not found* (nilai = 0). Persentase keberadaan artefak pada setiap kondisi dihitung menggunakan Persamaan 1 [35]. Tahap terakhir, yakni *reporting* mencakup dokumentasi seluruh proses investigasi secara sistematis sehingga temuan dapat ditelusuri, diverifikasi, dan dipertanggungjawabkan secara ilmiah maupun hukum [36]. Hasil dari setiap kondisi kemudian dibandingkan untuk mengidentifikasi pola persistensi artefak secara lintas kondisi.

$$Persentase(\%) = \frac{\sum Artefak\ Ditemukan}{\sum Total\ Artefak} \quad (1)$$

3. HASIL DAN PEMBAHASAN

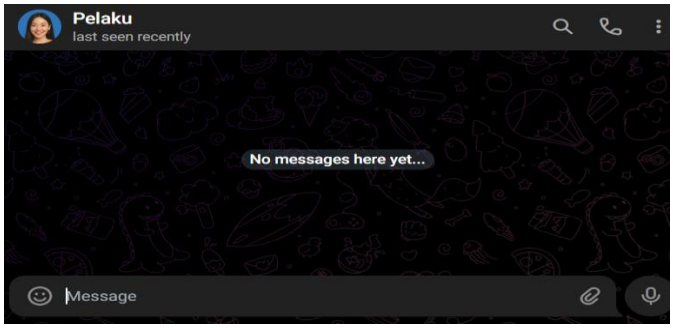
3.1 Pelaksanaan Simulasi Skenario

Seluruh tahapan skenario TS01–TS07 berhasil dijalankan sesuai rancangan penelitian. Interaksi antara pelaku dan korban mencakup pengiriman empat pesan *bullying*, dua pesan balasan korban, dua *file* gambar, satu dokumen PDF, dan satu *file* audio, berlangsung normal tanpa hambatan fungsional pada antarmuka Telegram Web. Gambar 3 menunjukkan tampilan percakapan yang dihasilkan dari eksekusi skenario TS01–TS06, memperlihatkan kondisi komunikasi sebelum penghapusan dilakukan. Pada tahap akhir (TS07), pelaku menghapus seluruh riwayat percakapan sehingga tampilan

BULLETIN OF COMPUTER SCIENCE RESEARCH
ISSN 2774-3659 (Media Online)
Vol 6, No 3, April 2026 | Hal 1016-1025
https://hostjournals.com/bulletincsr
DOI: 10.47065/bulletincsr.v6i3.1086

antarmuka Telegram Web dari sisi korban menjadi kosong. Gambar 4 menunjukkan bahwa pada hasil eksekusi TS07 tidak menampilkan jejak visual yang dikirimkan oleh pelaku kondisi inilah yang menjadikan RAM sebagai satu-satunya sumber bukti yang dapat dianalisis.

Gambar 3. Tampilan Percakapan Telegram Web pada Tahapan TS01–TS06 Sebelum Penghapusan Pesan

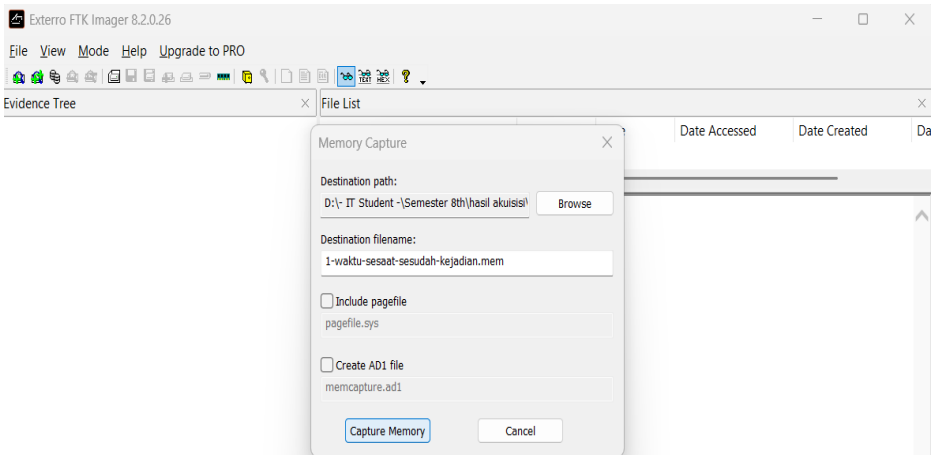


Gambar 4. Tampilan Antarmuka Telegram Web Setelah Penghapusan Pesan pada Skenario TS07

Keberhasilan eksekusi seluruh tahapan skenario ini menjadi landasan penting bagi proses investigasi forensik karena memastikan bahwa artefak yang dianalisis pada tahap berikutnya benar-benar berasal dari interaksi yang telah dirancang. Kondisi setelah TS07, di mana antarmuka Telegram Web terlihat kosong tanpa jejak visual, merepresentasikan situasi nyata dalam kasus *cyberbullying* di mana korban tidak memiliki bukti awal berupa tangkapan layar atau riwayat percakapan. Hal ini secara langsung menempatkan RAM sebagai satu-satunya sumber forensik yang dapat menunjukkan bahwa interaksi tersebut pernah terjadi. Sebelum proses akuisisi memori dilakukan, tahap *collection* dilaksanakan terlebih dahulu dengan mengamankan perangkat korban sebagai objek utama investigasi.

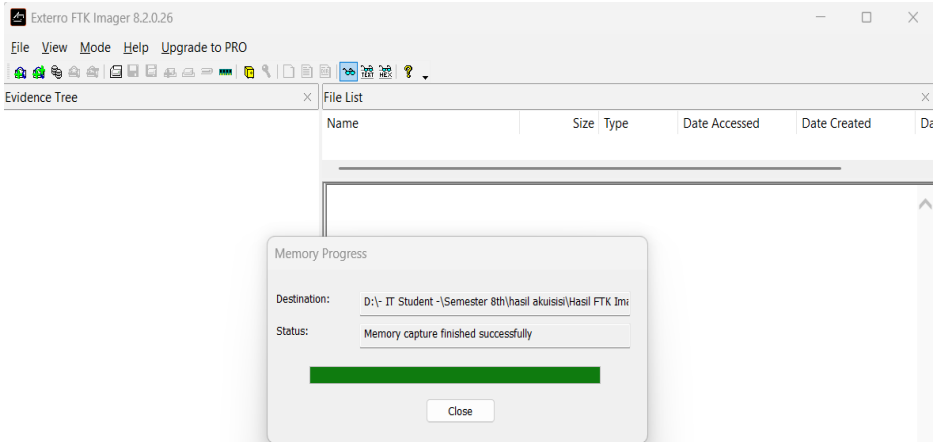
3.2 Akuisisi Memori dan Hasil Identifikasi Artefak

Proses *live acquisition* pada keenam kondisi pengujian berhasil diselesaikan dan menghasilkan enam *file memory image* berformat .mem. Konfigurasi *capture memory* pada antarmuka FTK Imager ditunjukkan pada Gambar 5, sedangkan notifikasi keberhasilan akuisisi ditunjukkan pada Gambar 6. Keenam *file* hasil akuisisi diberi penamaan yang mencerminkan masing-masing kondisi pengujian guna memudahkan proses identifikasi pada tahap analisis.



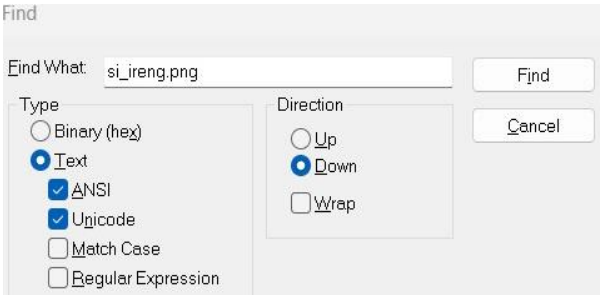
Gambar 5. Antarmuka Konfigurasi *Capture Memory* pada Exterro FTK Imager

BULLETIN OF COMPUTER SCIENCE RESEARCH
ISSN 2774-3659 (Media Online)
Vol 6, No 3, April 2026 | Hal 1016-1025
https://hostjournals.com/bulletincsr
DOI: 10.47065/bulletincsr.v6i3.1086



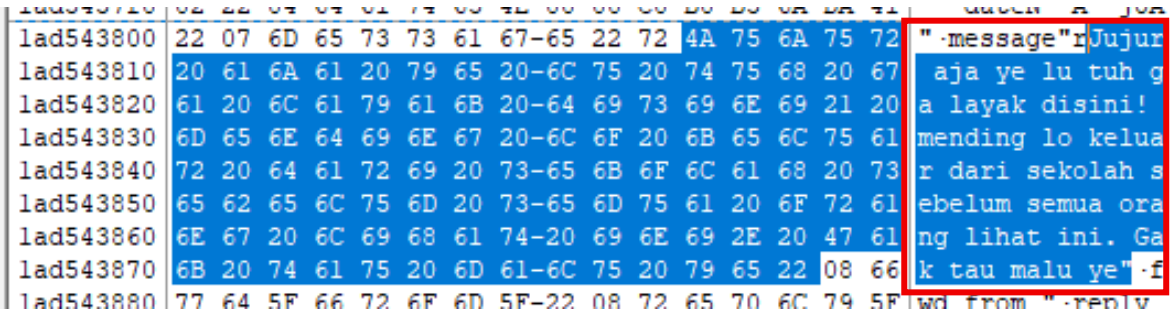
Gambar 6. Notifikasi Keberhasilan Proses *Capture Memory*

Proses identifikasi artefak pada setiap *memory image* dilakukan menggunakan teknik *keyword-based analysis* melalui fitur *Find* pada Exterro FTK Imager, sebagaimana ditunjukkan pada Gambar 7. Kata kunci yang digunakan mencakup fragmen isi pesan *bullying* seperti potongan kalimat percakapan serta nama *file* artefak media yang dikirimkan selama simulasi. Pendekatan ini dipilih karena data pada *memory image* tidak tersimpan dalam struktur *file* yang utuh melainkan terfragmentasi, sehingga pencarian berbasis kata kunci merupakan metode yang efektif dan terstandar. Setiap kata kunci dimasukkan secara individual dan hasilnya dikonfirmasi melalui tampilan fragmen data yang cocok jika ditemukan, diberi nilai 1, dan jika pencarian menghasilkan kondisi *string not found*, diberi nilai 0.



Gambar 7. Konfigurasi *Keyword Search* pada Fitur *Find* Exterro FTK Imager

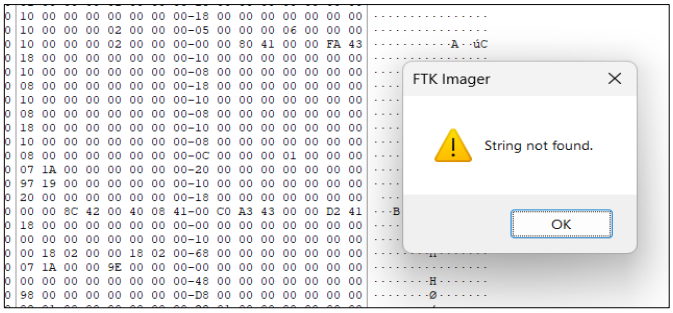
Pada kondisi pertama (sesaat setelah kejadian), seluruh 10 artefak ditemukan lengkap. Pada kondisi kedua (*sleep*) dan ketiga (*hibernate*), hasil yang diperoleh identik seluruh 10 artefak kembali ditemukan dengan persentase 100%. Konsistensi hasil antara ketiga kondisi awal ini bukan kebetulan, melainkan mencerminkan bahwa mekanisme teknis RAM pada mode *sleep* (ACPI S3) dan *hibernate* (ACPI S4) secara efektif mempertahankan seluruh isi memori tanpa kehilangan satu pun fragmen data. Contoh hasil temuan artefak pada kondisi pertama ditunjukkan pada Gambar 8, di mana fragmen pesan *bullying* berhasil diidentifikasi dalam *memory image* sesuai kata kunci yang dimasukkan.



Gambar 8. Contoh Artefak Pesan Teks yang Berhasil Teridentifikasi pada *Memory Image* (Kondisi Sesaat Setelah Kejadian)

Pada kondisi keempat (*browser* ditutup), dari 10 artefak yang diuji, hanya 4 yang berhasil ditemukan: PCHAT-02, PCHAT-04, KCHAT-01, dan D-01. Enam artefak lainnya PCHAT-01, PCHAT-03, KCHAT-02, G-01, G-02, dan M-01 tidak lagi dapat diidentifikasi dalam *memory image*. Pada kondisi kelima (*browser* ditutup + aktivitas lanjutan), hanya KCHAT-01 yang masih dapat ditemukan, sementara seluruh artefak lainnya tidak terdeteksi. Pada kondisi keenam (*shutdown*), seluruh 10 artefak menghasilkan *string not found*, sebagaimana ditunjukkan pada Gambar 9, yang memperlihatkan tampilan antarmuka FTK Imager saat pencarian kata kunci tidak menemukan fragmen data apa pun dalam *memory image*, konfirmasi bahwa artefak telah hilang dari memori.

BULLETIN OF COMPUTER SCIENCE RESEARCH
ISSN 2774-3659 (Media Online)
Vol 6, No 3, April 2026 | Hal 1016-1025
https://hostjournals.com/bulletincsr
DOI: 10.47065/bulletincsr.v6i3.1086



Gambar 9. Hasil Pencarian Menampilkan *String Not Found* pada Kondisi *Browser* Ditutup

Ringkasan hasil identifikasi artefak dari seluruh variasi kondisi akuisisi disajikan pada Tabel 4, di mana nilai 1 menunjukkan artefak ditemukan dalam *memory image*, sedangkan nilai 0 menunjukkan tidak ditemukan. Baris terakhir menyajikan perhitungan persentase berdasarkan keberhasilan temuan artefak pada setiap kondisi pengujian. Pada tiga kondisi pertama, sesaat setelah kejadian, *sleep*, dan *hibernate* menghasilkan persentase temuan artefak 100%, di mana seluruh 10 artefak berhasil diidentifikasi tanpa terkecuali. Pada kondisi keempat (*browser* ditutup), persentase turun menjadi 40% dengan 4 dari 10 artefak yang masih dapat ditemukan. Kondisi kelima (*browser* ditutup disertai penggunaan aplikasi lain) hanya menghasilkan 10%, yaitu 1 dari 10 artefak. Kondisi keenam (*shutdown*) menghasilkan 0% tidak satu pun artefak yang dapat diidentifikasi.

Tabel 4. Ringkasan Hasil Identifikasi Artefak Digital pada Seluruh Kondisi Akuisisi

Kode Aktivitas	Kode Artefak	Sesaat Kejadian	*Sleep*	*Hibernate*	*Browser* Ditutup	*Browser* + Aktivitas	*Shutdown*
TS01	PCHAT-01	1	1	1	0	0	0
TS03	PCHAT-02	1	1	1	1	0	0
TS04	PCHAT-03	1	1	1	0	0	0
TS05	PCHAT-04	1	1	1	1	0	0
TS02	KCHAT-01	1	1	1	1	1	0
TS06	KCHAT-02	1	1	1	0	0	0
TS03	G-01	1	1	1	0	0	0
TS03	G-02	1	1	1	0	0	0
TS01	D-01	1	1	1	1	0	0
TS04	M-01	1	1	1	0	0	0
Persentase Artefak Ditemukan		100%	100%	100%	40%	10%	0%

3.3 Pembahasan

Hasil analisis menunjukkan bahwa tingkat persistensi artefak digital Telegram Web pada RAM sangat ditentukan oleh kondisi sistem saat akuisisi dilakukan. Temuan ini menjadi signifikan mengingat karakteristik Telegram Web yang tidak meninggalkan jejak visual setelah pesan dihapus, sehingga RAM menjadi satu-satunya sumber bukti yang dapat dianalisis dalam proses investigasi forensik digital. Pemahaman terhadap mekanisme teknis penyimpanan data pada tingkat arsitektur memori komputer menjadi kunci dalam menginterpretasikan hasil persentase yang diperoleh pada setiap kondisi akuisisi.

Pada kondisi pertama sesaat setelah kejadian seluruh 10 artefak berhasil ditemukan karena *browser* dan sistem masih dalam kondisi aktif. Ketika pengguna mengakses Telegram Web melalui Chrome, seluruh konten percakapan termasuk teks pesan, *metadata file*, dan fragmen data media dimuat ke dalam memori proses *browser* (*renderer process*) melalui mekanisme JavaScript *heap* dan DOM *tree*. Chrome juga memanfaatkan mekanisme *client-side storage* seperti IndexedDB dan *cache storage* yang turut menyimpan data sesi Telegram Web ke dalam RAM selama proses berlangsung [6], [7]. Selama tidak ada perubahan kondisi sistem apa pun sejak interaksi selesai hingga akuisisi dilakukan, seluruh fragmen artefak masih tersimpan utuh dalam memori proses Chrome, sehingga Exterro FTK Imager dapat mengidentifikasi keseluruhan artefak secara lengkap. Kondisi ini merepresentasikan skenario ideal investigasi *live forensics* di mana investigator tiba di TKP sebelum perangkat mengalami perubahan status apa pun.

Pada kondisi *sleep*, perangkat memasuki mode ACPI S3 (*Suspend to RAM*) di mana sistem operasi Windows mempertahankan daya pada modul RAM dengan tegangan rendah. Pada mode S3 ini, mekanisme *self-refresh* tetap aktif pada *chip* DRAM, sehingga muatan kapasitor pada setiap sel memori terus diperbarui dan seluruh konten RAM dipertahankan secara penuh tanpa perubahan data apa pun [9]. Ini berarti seluruh data proses Chrome termasuk JavaScript *heap*, *renderer process memory*, dan data sesi Telegram Web tetap tersimpan utuh di RAM selama perangkat berada dalam mode *sleep*. Saat perangkat dibangunkan kembali dan akuisisi segera dilakukan, kondisi memori identik dengan kondisi sebelum *sleep* terjadi, sehingga persentase temuan artefak tetap 100%. Temuan ini menunjukkan bahwa mode

sleep tidak memberikan risiko kehilangan artefak selama *browser* tidak ditutup sebelum atau setelah perangkat bangun dari kondisi tersebut.

Kondisi *hibernate* menghasilkan persentase yang sama, yakni 100%, melalui mekanisme teknis yang berbeda secara fundamental dari *sleep*. Pada mode ACPI S4, sistem operasi Windows menyalin seluruh isi RAM secara *byte-for-byte* ke dalam berkas hiberfil.sys yang tersimpan pada *disk*, kemudian mematikan daya sepenuhnya sehingga tidak ada aliran listrik yang masuk ke modul RAM [9]. Proses penyalinan ini bersifat *lossless* tidak ada satu pun data yang dimodifikasi atau dihilangkan selama transisi ke kondisi *hibernate*. Ketika perangkat dihidupkan kembali, Windows membaca hiberfil.sys dan memuatnya kembali ke RAM secara identik, termasuk seluruh fragmen artefak Telegram Web yang sebelumnya tersimpan dalam proses Chrome. Implikasi teknisnya adalah bahwa investigator yang menemukan perangkat dalam kondisi *hibernate* masih memiliki peluang penuh untuk memulihkan seluruh artefak, selama *browser* tidak ditutup sebelum *hibernate* terjadi dan akuisisi segera dilakukan setelah perangkat dihidupkan kembali.

Penurunan signifikan pertama terjadi ketika *browser* ditutup meskipun komputer masih menyala. Penutupan Chrome memicu dua proses bersamaan yang mengurangi ketersediaan artefak. Pertama, Chrome sendiri melakukan proses *cleanup* internal sebelum menutup proses utamanya, termasuk membersihkan sebagian *session data*, *cache* yang ada di memori, serta mengosongkan JavaScript *heap* dari *renderer process*. Kedua, setelah proses Chrome berakhir, sistem operasi menandai seluruh *virtual memory pages* bekas proses tersebut sebagai *free* dan memasukkannya ke dalam *free page list* yang dikelola *Memory Manager* Windows [10]. Halaman-halaman memori berstatus *free* ini belum langsung di-*zero-fill*, sehingga data lama yang sebelumnya tersimpan masih dapat dibaca sementara inilah yang menjelaskan mengapa 40% artefak (PCHAT-02, PCHAT-04, KCHAT-01, D-01) masih dapat ditemukan. Namun, 60% artefak lainnya sudah tertimpa (*overwrite*) oleh proses sistem latar belakang seperti antivirus dan Windows Update yang secara otomatis memanfaatkan halaman memori yang tersedia di *free list*. Kombinasi antara *cleanup* internal *browser* dan *overwrite* pasif oleh proses *background* inilah yang menghasilkan persentase 40%.

Pada kondisi kelima *browser* ditutup disertai aktivitas lanjutan penurunan lebih drastis terjadi karena mekanisme *memory reuse* yang jauh lebih agresif dibandingkan dengan kondisi keempat. Ketika aplikasi baru dijalankan setelah *browser* ditutup, *Memory Manager* Windows mengalokasikan halaman memori dari *free page list* yang tersedia yang merupakan halaman-halaman bekas proses Chrome. Perbedaan krusial dari kondisi keempat adalah: pada kondisi ini Windows secara aktif melakukan *zero-fill* (pengisian nilai nol) pada setiap halaman memori bekas Chrome sebelum diserahkan kepada proses baru [10]. *Zero-fill* merupakan mekanisme keamanan bawaan sistem operasi untuk mencegah kebocoran data antarproses, dan proses ini bersifat permanen data artefak yang telah di-*zero-fill* tidak dapat dipulihkan kembali melalui metode konvensional apa pun. Hanya KCHAT-01 yang masih tersisa karena fragmen tersebut kebetulan berada pada halaman memori yang belum sempat di-*reclaim* oleh *Memory Manager*. Semakin besar kebutuhan memori dari aplikasi yang dijalankan, semakin banyak halaman bekas Chrome yang di-*reclaim* dan di-*zero-fill*, yang menjelaskan mengapa persentase turun hingga hanya 10%.

Pada kondisi *shutdown*, tidak ditemukan satu pun artefak dari 10 artefak yang diuji. Hasil ini dapat dijelaskan langsung dari sifat fisik komponen DRAM. Setiap sel memori pada *chip* DRAM menyimpan satu bit data menggunakan kapasitor kecil yang membutuhkan aliran listrik terus-menerus untuk mempertahankan muatannya melalui mekanisme *self-refresh* [9]. Ketika daya dimatikan melalui proses *shutdown*, kapasitor-kapasitor ini kehilangan muatannya dalam hitungan milidetik, sehingga seluruh data RAM hilang secara permanen tanpa dapat dipulihkan melalui metode forensik konvensional. Berbeda dengan *hibernate* yang menyimpan salinan RAM ke *disk* sebelum mematikan daya, *shutdown* tidak melakukan langkah preservasi memori apa pun. Prosedur *shutdown* Windows juga mencakup pengakhiran semua proses aktif dan penghapusan *pagefile* sementara, yang semakin memastikan tidak ada fragmen artefak yang tersisa dalam bentuk apa pun setelah sistem dinyalakan kembali. Temuan 0% ini konsisten dengan prinsip dasar forensik memori bahwa artefak berbasis RAM tidak dapat dipertahankan setelah daya diputus [9], [10].

Secara keseluruhan, pola persentase 100%–100%–100%–40%–10%–0% yang diperoleh bukan merupakan angka yang bersifat acak, melainkan mencerminkan pola teknis yang dapat diprediksi berdasarkan mekanisme manajemen memori sistem operasi Windows dan karakteristik fisik komponen RAM. Setiap tahapan penurunan memiliki penjelasan teknis yang spesifik dan terverifikasi: dari *self-refresh* DRAM pada mode S3, penyalinan *byte-for-byte* ke hiberfil.sys pada mode S4, *cleanup* internal *browser* dan *overwrite* pasif pada kondisi *browser* ditutup, *zero-fill* aktif pada kondisi aktivitas lanjutan, hingga hilangnya muatan kapasitor saat *shutdown*. Semakin cepat proses akuisisi dilakukan dan semakin sedikit perubahan kondisi sistem yang terjadi, semakin besar kemungkinan artefak digital dapat diperoleh secara lengkap.

Untuk memperkuat validitas temuan, hasil penelitian ini dibandingkan dengan penelitian forensik digital pada platform Telegram lainnya. Pada Telegram Mobile berbasis Android, artefak digital tersimpan secara persisten dalam basis data SQLite pada *internal storage* perangkat yang bersifat *non-volatile* [18], [19]. Artefak tersebut dapat diakses bahkan setelah perangkat dimatikan, karena keberadaannya tidak bergantung pada kondisi daya atau status memori sistem. Hal ini berbeda secara mendasar dengan Telegram Web, di mana seluruh artefak hanya tersedia selama RAM masih mempertahankan data proses *browser*. Pada Telegram Desktop, artefak tersimpan pada direktori lokal sistem *file* pengguna seperti *%AppData%\Telegram Desktop* sehingga persistensinya lebih tinggi dan tidak dipengaruhi oleh perubahan kondisi sistem [19], [20]. Perbandingan ini menunjukkan bahwa Telegram Web memiliki tingkat volatilitas artefak yang jauh lebih tinggi dibandingkan dengan kedua platform lainnya dan menjadikan kondisi sistem saat akuisisi sebagai faktor penentu utama dalam keberhasilan investigasi forensik.

Penelitian terdahulu seperti [25], [26], [27] yang mengkaji artefak pada Telegram Web umumnya bersifat deskriptif dalam mengidentifikasi jenis-jenis artefak yang dapat ditemukan, namun belum melakukan evaluasi kuantitatif terhadap pengaruh variasi kondisi sistem. Penelitian ini melengkapi kesenjangan tersebut dengan membuktikan secara terukur bahwa pola penurunan persentase artefak dari 100% menjadi 40%, 10%, dan akhirnya 0% merupakan konsekuensi deterministik dari mekanisme teknis arsitektur memori komputer, bukan hasil yang bersifat acak. Setiap tahapan penurunan dapat dijelaskan melalui perilaku spesifik sistem operasi Windows dalam mengelola halaman memori, mulai dari mekanisme *free page list*, proses *zero-fill*, hingga sifat fisik kapasitor DRAM saat daya diputus.

Temuan ini memiliki implikasi praktis yang langsung bagi para investigator forensik digital. Pertama, akuisisi memori secara *live* harus menjadi prioritas mutlak dalam setiap investigasi yang melibatkan Telegram Web penundaan sekecil apa pun berpotensi menyebabkan hilangnya bukti secara permanen. Kedua, kondisi *sleep* dan *hibernate* tidak serta-merta menghilangkan artefak, sehingga investigator yang menemukan perangkat dalam kondisi tersebut masih memiliki peluang penuh untuk memulihkan bukti selama *browser* belum ditutup. Ketiga, tindakan sederhana seperti membuka aplikasi lain setelah *browser* ditutup dapat mereduksi peluang perolehan artefak dari 40% menjadi hanya 10%, sebuah perbedaan yang signifikan dalam konteks pembuktian hukum. Temuan ini mengisyaratkan perlunya penyesuaian Standar Prosedur Operasional (SOP) penanganan barang bukti digital untuk mengakomodasi karakteristik spesifik aplikasi berbasis *browser*, khususnya ketentuan yang secara eksplisit melarang penggunaan perangkat dalam bentuk apa pun sebelum proses akuisisi memori diselesaikan.

4. KESIMPULAN

Penelitian ini membuktikan bahwa artefak digital Telegram Web dapat dipertahankan dan diidentifikasi kembali dari RAM meskipun seluruh riwayat percakapan telah dihapus dari antarmuka aplikasi oleh pelaku, dengan tingkat keberhasilan yang sepenuhnya bergantung pada kondisi sistem saat akuisisi dilakukan. Menjawab pertanyaan riset pertama, artefak digital Telegram Web terbukti dapat dipertahankan dalam memori pada kondisi sesaat setelah kejadian, *sleep* (ACPI S3), dan *hibernate* (ACPI S4) dengan persentase 100% RAM mempertahankan data proses Chrome secara utuh melalui mekanisme *self-refresh* DRAM pada mode S3 dan penyalinan *byte-for-byte* ke hiberfil.sys pada mode S4. Menjawab pertanyaan riset kedua, pengaruh masing-masing kondisi akuisisi terhadap tingkat keberadaan artefak terbukti bersifat deterministik: penutupan *browser* menurunkan persentase menjadi 40% akibat *cleanup* internal Chrome dan penandaan *memory pages* sebagai *free* oleh sistem operasi; penggunaan aplikasi lain setelahnya mereduksinya menjadi 10% karena mekanisme *zero-fill* aktif oleh *Memory Manager* Windows yang menimpa halaman memori bekas Chrome; dan kondisi *shutdown* menghilangkan seluruh artefak (0%) karena muatan kapasitor DRAM hilang secara permanen saat daya diputus. Pola persentase 100%–40%–10%–0% bukan angka acak, melainkan cerminan dari mekanisme arsitektur memori komputer yang dapat diprediksi secara teknis. Temuan ini menegaskan bahwa RAM merupakan sumber bukti kritis pada kasus *cyberbullying* berbasis Telegram Web, dan kecepatan serta ketepatan akuisisi *live* menjadi faktor penentu keberhasilan investigasi. Penelitian ini memiliki keterbatasan pada cakupan pengujian yang hanya melibatkan satu konfigurasi perangkat, yaitu *browser* Google Chrome dan sistem operasi Windows 11, sehingga hasil belum dapat digeneralisasikan ke *browser* atau sistem operasi lain. Selain itu, teknik *keyword-based analysis* memiliki keterbatasan dalam mendeteksi artefak yang terenkripsi atau terfragmentasi dan tidak mengandung kata kunci yang dapat dikenali. Penelitian selanjutnya disarankan memperluas pengujian pada *browser* lain (Firefox, Edge), platform web lain (WhatsApp Web, Discord Web), serta mengintegrasikan analisis sumber artefak komplementer seperti pagefile.sys dan IndexedDB pada *disk storage* untuk memperoleh gambaran forensik yang lebih menyeluruh.

REFERENCES

[1] A. A. D. Pitaloka, C. Syahputri, D. Ramadhani, N. P. Anggreani, S. N. Khaira, and G. Supraja, "The Role of Social Media in the Dissemination of Public Information," *Int. J. Econ. Res. Financ. Account,* vol. 3, no. 2, pp. 490–495, Jan. 2025.
[2] Interpol, "Asia and South Pacific Cyberthreat Assessment Report," *Rep., International Criminal Police Organization*, Lyon, France, Aug. 2024.
[3] V. Ibrahim, Y. S. Hasan, and P. Ishak, "Personal Data Protection Policies and Their Impact on Victims of Cybercrime," *Jurnal Ilmu Hukum Kyadiren*, vol. 6, no. 2, pp. 13–25, Jan. 2025, doi: 10.46924/jihk.v6i2.225.
[4] S. Kemp, "Digital 2024: Global Overview Report," DataReportal. Accessed: Apr. 2026. [Online]. Available: https://datareportal.com/reports/digital-2024-global-overview-report
[5] A. R. Onik, J. Brown, C. Walker, and I. Baggili, "A Systematic Literature Review of Secure Instant Messaging Applications from a Digital Forensics Perspective," *ACM Comput. Surv.*, vol. 57, no. 9, pp. 1–36, Sep. 2025, doi: 10.1145/3727641.
[6] M. Prasetio and I. Riadi, "Investigation Telegram Based-on Web using National Institute of Standards and Technology Method," *Int. J. Comput. Appl.*, vol. 183, no. 50, pp. 8–15, Feb. 2022, doi: 10.5120/ijca2022921092.
[7] F. Paligu and C. Varol, "Browser Forensic Investigations of WhatsApp Web Utilizing IndexedDB Persistent Storage," *Future Internet*, vol. 12, no. 11, p. 184, Oct. 2020, doi: 10.3390/fi12110184.
[8] B. Jeong, S. Lee, and J. Park, "MIC: Memory Analysis of IndexedDB Data on Chromium-Based Applications," *Forensic Science International: Digital Investigation*, vol. 50, p. 301809, Oct. 2024, doi: 10.1016/j.fsidi.2024.301809.
[9] H. Nyholm *et al.*, "The Evolution of Volatile Memory Forensics," *Journal of Cybersecurity and Privacy*, vol. 2, no. 3, pp. 556–572, Jul. 2022, doi: 10.3390/jcp2030028.
[10] I. Hamid and M. M. H. Rahman, "A Comprehensive Literature Review on Volatile Memory Forensics," *Electronics*, vol. 13, no. 15, p. 3026, Jul. 2024, doi: 10.3390/electronics13153026.

[11] J. Kävrestad, M. Birath, and N. Clarke, *Fundamentals of Digital Forensics: A Guide to Theory, Research and Applications*, 3rd ed. Cham, Switzerland: Springer International Publishing, 2024, doi: 10.1007/978-3-031-53649-6. [Online]. Available: https://link.springer.com/book/10.1007/978-3-031-53649-6
[12] J. Wiarti, "Legality of Electronic Evidence in Cyber Crime Cases," *Ahmad Dahlan Indonesian Law Journal*, vol. 1, no. 1, pp. 11–19, Jun. 2023, doi: 10.12928/adil.v1i1.572.
[13] Indonesia, "Undang-Undang Informasi dan Transaksi Elektronik, UU No. 11 Tahun 2008," 2008. Accessed: Apr. 2026. [Online]. Available: https://peraturan.bpk.go.id/details/37589/uu-no-11-tahun-2008
[14] Mahkamah Agung, "Peraturan Mahkamah Agung (Perma) Nomor 1 Tahun 2019," 2019, Accessed: Apr. 2026. [Online]. Available: https://peraturan.bpk.go.id/details/206067/perma-no-1-tahun-2019
[15] R. Stoykova, "Digital Evidence: Unaddressed Threats to Fairness and the Presumption of Innocence," *Computer Law & Security Review*, vol. 42, p. 105575, Sep. 2021, doi: 10.1016/j.clsr.2021.105575.
[16] P. Reedy, "Interpol Review of Digital Evidence for 2019–2022," *Forensic Sci. Int. Synergy*, vol. 6, p. 100313, 2023, doi: 10.1016/j.fsisyn.2022.100313.
[17] C. Easttom, *Digital Forensics, Investigation, and Response*, 4th ed. Burlington, MA: Jones & Bartlett Learning, 2022. [Online]. Available: https://www.jblearning.com/catalog/productdetails/9781284226065
[18] A. Raza and M. B. Hassan, "Digital Forensic Analysis of Telegram Messenger App in Android Virtual Environment," *Mobile and Forensics*, vol. 4, no. 1, pp. 31–43, Mar. 2022, doi: 10.12928/mf.v4i1.5537.
[19] E. Purwanto and I. Riadi, "Digital Forensic Mobile Telegram Services in Online Gambling Case using National Institute of Standards and Technology Method," *Int. J. Comput. Appl.*, vol. 186, no. 35, pp. 44–54, Aug. 2024, doi: 10.5120/ijca2024923926.
[20] L. Jaeckel, M. Spranger, and D. Labudde, "Forensic Analysis of Telegram Messenger on iOS Smartphones," *Forensic Science International: Digital Investigation*, vol. 52, p. 301866, Mar. 2025, doi: 10.1016/j.fsidi.2025.301866.
[21] P. Fernández-Álvarez and R. J. Rodríguez, "Extraction and Analysis of Retrievable Memory Artifacts from Windows Telegram Desktop Application," *Forensic Science International: Digital Investigation*, vol. 40, p. 301342, Apr. 2022, doi: 10.1016/j.fsidi.2022.301342.
[22] I. G. N. G. Wicaksana and I. K. G. Suhartana, "Forensic Analysis of Telegram Desktop-based Applications using the National Institute of Justice (NIJ) Method," *JELIKU (Jurnal Elektronik Ilmu Komputer Udayana)*, vol. 8, no. 4, p. 381, Feb. 2020, doi: 10.24843/JLK.2020.v08.i04.p03.
[23] N. C. Dewi, T. Sutabri, and F. Putrawansyah, "Analisis Penyadapan pada Telegram dengan Network Forensik," *JIKO (Jurnal Informatika dan Komputer)*, vol. 7, no. 2, p. 183, Sep. 2023, doi: 10.26798/jiko.v7i2.789.
[24] A. Raza, M. Hussain, H. Tahir, M. Zeeshan, M. A. Raja, and K.-H. Jung, "Forensic Analysis of Web Browsers Lifecycle: A Case Study," *Journal of Information Security and Applications*, vol. 85, p. 103839, Sep. 2024, doi: 10.1016/j.jisa.2024.103839.
[25] L. C. Pakaya and I. Riadi, "Forensic Analysis of Web-based Instant Messenger Applications using National Institute of Justice Method," *IJCA (International Journal of Computer Applications)*, vol. 185, no. 35, pp. 44–51, Sep. 2023, doi: 10.5120/ijca2023923145.
[26] K. A. Arifin and I. Riadi, "Forensic Analysis of Online Fraud on Telegram Web using Digital Forensics Workshop Method," *IJCA (International Journal of Computer Applications)*, vol. 187, no. 30, pp. 4–11, Aug. 2025, doi: 10.5120/ijca2025925515.
[27] B. W. D. Samara, A. Subki, M. Zulpahmi, and L. D. Samsumar, "Analisis Forensik Aplikasi Telegram Menggunakan Metode Digital Forensics Research Workshop," *Journal Of Computer Science And Technology (JOCSTEC)*, vol. 3, no. 2, pp. 112–126, May 2025, doi: 10.59435/jocstec.v3i2.435.
[28] A. Yudhana, I. Riadi, and R. Y. Prasongko, "Forensik WhatsApp Menggunakan Metode Digital Forensic Research Workshop (DFRWS)," *Jurnal Informatika: Jurnal Pengembangan IT*, vol. 7, no. 1, pp. 43–48, Jan. 2022, doi: 10.30591/jpit.v7i1.3639.
[29] D. S. I. Utomo, Y. Prayudi, and E. Ramadhani, "Forensic Web Analysis on The Latest Version of WhatsApp Browser," *Journal of Computer Networks, Architecture and High Performance Computing*, vol. 5, no. 1, pp. 359–367, May 2023, doi: 10.47709/cnahpc.v5i1.2286.
[30] A. Faizal and A. Luthfi, "Comparison Study of NIST SP 800-86 and ISO/IEC 27037 Standards as A Framework for Digital Forensic Evidence Analysis," *Journal of Information Systems and Informatics*, vol. 6, no. 2, pp. 701–718, Jun. 2024, doi: 10.51519/journalisi.v6i2.717.
[31] L. Rzepka, J. Ottmann, R. Stoykova, F. Freiling, and H. Baier, "A Scenario-Based Quality Assessment of Memory Acquisition Tools and its Investigative Implications," *Forensic Science International: Digital Investigation*, vol. 52, p. 301868, Mar. 2025, doi: 10.1016/j.fsidi.2025.301868.
[32] R. A. Ramadhan, P. R. Setiawan, and D. Hariyadi, "Digital Forensic Investigation for Non-Volatile Memory Architecture by Hybrid Evaluation Based on ISO/IEC 27037:2012 and NIST SP800-86 Framework," *IT Journal Research and Development*, pp. 162–168, Feb. 2022, doi: 10.25299/itjrd.2022.8968.
[33] J. R. Lyle, B. Guttman, J. M. Butler, K. Sauerwein, C. Reed, and C. E. Lloyd, "Digital Investigation Techniques: A NIST Scientific Foundation Review," *Nat. Inst. Stand. Technol.*, Gaithersburg, MD, USA, Rep. NIST IR 8354, Nov. 2022. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/ir/2022/NIST.IR.8354.pdf
[34] B. Pandey, A. Kumar, D. B. Acharya, P. Pandey, and W. A. W. A. Bakar, "Memory Forensic: Detecting Unusual Intrusion Activity in Dump of RAM Memory Using FTK Imager," *International Journal of Information Technology*, vol. 17, no. 7, pp. 4209–4216, Sep. 2025, doi: 10.1007/s41870-025-02567-0.
[35] R. Rahmansyah, "Perbandingan Hasil Investigasi Barang Bukti Digital pada Aplikasi Facebook dan Instagram dengan Metode NIST," *Cyber Security dan Forensik Digital*, vol. 4, no. 1, pp. 49–57, Jun. 2021, doi: 10.14421/csecurity.2021.4.1.2421.
[36] W. Agustiono, D. W. Suci, and N. Prastiti, "Analisis Forensik Digital Menggunakan Metode NIST untuk Memulihkan Barang Bukti yang Dihapus," *Jurnal Teknologi dan Informasi*, vol. 14, no. 2, pp. 174–185, Sep. 2024, doi: 10.34010/jati.v14i2.12952.