Accredited SINTA 5
72/E/KPT/2024

Jurnal Nasional Komputasi dan Teknologi Informasi (JNKTI)
Vol. 8 No. 4, Agustus 2025
P-ISSN 2620-8342
E-ISSN 2621-3052

Analisis Forensik Digital Pada Kasus Penyebaran Konten Ilegal Menggunakan Metode *National Intitute of Justice* (NIJ)

Rapia Yakob Ingahu[1*], Wahyudin Hasyim[2], Hilmansyah Gani[3]
Program Studi Sistem Informasi, Universitas Muhammadiyah Gorontalo
Jl. Prof. Dr. H. Mansoer Pateda, Desa Pentadio Timur, Kec. Telaga Biru, Kab. Gorontalo, Gorontalo 96181, Indonesia
E-mail: rapiaingahu16@gmail.com

Submitted Date : ***Desember 2025*** ***Accepted Date :*** ***Desember 2025***

Abstrak - Perkembangan media sosial meningkatkan risiko penyebaran konten ilegal, seperti kasus *cyberbullying* di *Facebook Messenger*. Penelitian ini bertujuan untuk menganalisis bukti digital pada kasus penyebaran konten ilegal menggunakan metode *National Institute of Justice* (NIJ). Penelitian dilakukan melalui pendekatan kualitatif deskriptif berbasis skenario simulatif dan mengikuti lima tahapan metode NIJ, yaitu identifikasi, pengumpulan, pemeriksaan, analisis, dan pelaporan. Proses investigasi dilakukan menggunakan perangkat lunak *FTK Imager*, *Autopsy*, dan *DB Browser for SQLite*. Hasil penelitian menunjukkan bahwa pesan yang telah dihapus dapat direkonstruksi, metadata dikembalikan, serta identitas pelaku berhasil ditelusuri. Metode NIJ terbukti efektif dalam menyusun proses investigasi digital yang sistematis dan dapat dipertanggungjawabkan. Penelitian ini memberikan kontribusi terhadap praktik forensik digital dalam menanggapi kasus penyebaran konten ilegal melalui media sosial.
Kata kunci : Forensik Digital, Konten Ilegal, Metode NIJ, Cyberbullying, Facebook Messenger

Abstract - *The development of social media increases the risk of the distribution of illegal content, such as cases of cyberbullying on Facebook Messenger. This study aims to analyze digital evidence in cases of illegal content distribution using the National Institute of Justice (NIJ) method. The study was conducted using a descriptive qualitative approach based on simulated scenarios and followed the five stages of the NIJ method: identification, collection, examination, analysis, and reporting. The investigation process was conducted using FTK Imager, Autopsy, and DB Browser for SQLite software. The results showed that deleted messages could be reconstructed, metadata recovered, and the perpetrator's identity successfully traced. The NIJ method has proven effective in establishing a systematic and accountable digital investigation process. This research contributes to digital forensic practice in responding to cases of illegal content distribution via social media.*
Keywords: Digital Forensics, Illegal Content, NIJ Method, Cyberbullying, Facebook Messenger

1. Pendahuluan

Kemajuan pesat dalam bidang Teknologi Informasi dan Komunikasi (TIK) telah membawa transformasi besar dalam berbagai aspek kehidupan manusia. Meski menawarkan kemudahan dan efisiensi dalam komunikasi, bisnis, serta edukasi, perkembangan ini juga membuka peluang baru bagi munculnya tindak kejahatan digital. Salah satu bentuk ancaman yang semakin mengkhawatirkan adalah penyebaran konten ilegal di ranah digital, yang meliputi pornografi, perjudian daring, penipuan digital, serta penyebaran informasi palsu. Keberadaan konten semacam ini tidak hanya meresahkan masyarakat, tetapi juga berpotensi menimbulkan gangguan serius terhadap stabilitas sosial dan keamanan nasional.

Di Indonesia, penyebaran konten ilegal melalui media sosial dan *platform* digital terus meningkat secara signifikan setiap tahun. Laporan Asosiasi Penyelenggara Jasa Internet Indonesia (APJII) menunjukkan bahwa penetrasi internet di Indonesia meningkat dari 64,8% pada tahun 2018 menjadi 73,7% pada tahun 2020, 77,01% pada tahun 2022, 78,19% pada tahun 2023, dan mencapai 79,5% pada tahun 2024 [1]. Pertumbuhan ini menunjukkan bahwa peningkatan jumlah pengguna internet turut memperbesar potensi penyalahgunaan teknologi digital, termasuk distribusi konten ilegal. Untuk merespons persoalan tersebut, pemerintah Indonesia melalui Kementerian Komunikasi dan Digital (Kemenkomdigi) merencanakan implementasi Sistem Kepatuhan Moderasi Konten (SAMAN) pada Februari 2025, yang ditujukan untuk menciptakan lingkungan digital yang aman melalui pemantauan dan pengawasan kepatuhan penyelenggara sistem elektronik berbasis *User Generated Content* [2]. Namun, penegakan hukum atas pelanggaran konten ilegal masih terkendala teknis dan yuridis, sehingga diperlukan pendekatan pendukung yang lebih akurat dan menyeluruh, salah satunya melalui pendekatan forensik digital.

Analisis forensik digital hadir sebagai instrumen penting dalam mengidentifikasi, memperoleh, dan mengevaluasi bukti digital yang berkaitan dengan kejahatan siber, termasuk penyebaran konten ilegal. Metode investigatif yang telah terbukti efektif dalam proses ini adalah pendekatan dari *National Institute of Justice*

Copyright © Jurnal Nasional Komputasi dan Teknologi Informasi (JNKTI)

Jurnal Nasional Komputasi dan Teknologi Informasi (JNKTI)
Vol. 8 No. 4, Agustus 2025
P-ISSN 2620-8342
E-ISSN 2621-3052

(NIJ), yang terdiri dari lima tahap sistematis: identifikasi, pengumpulan, pemeriksaan, analisis, dan pelaporan [3]. Metode NIJ memfasilitasi pendekatan terstruktur dalam menangani bukti digital, memungkinkan hasil yang diperoleh tidak hanya sah secara hukum, tetapi juga dapat dipertanggungjawabkan dalam proses peradilan. Hal ini menjadikan metode NIJ sebagai standar yang dapat diandalkan dalam proses investigasi digital.

Beberapa penelitian sebelumnya menunjukkan keberhasilan penerapan metode NIJ dalam konteks kasus kejahatan siber. Studi yang dilakukan oleh [4] menggunakan metode NIJ untuk mengungkap kasus *cyberbullying* pada aplikasi *Instagram* dan *WhatsApp*. Dengan memanfaatkan perangkat lunak *Autopsy*, *FTK Imager*, dan *MOBILedit,* penelitian tersebut berhasil menemukan sejumlah bukti signifikan, meskipun masih terdapat kendala teknis seperti keterbatasan dalam mendeteksi file tersembunyi atau terhapus. Sementara itu, studi yang dilakukan oleh [5] mengevaluasi pemulihan data digital dari aplikasi *WhatsApp* dan *Line* pada perangkat Android dengan membandingkan efektivitas perangkat yang telah di-*root* dan yang belum. Studi tersebut berhasil memperoleh data digital secara mendalam, akan tetapi fokus penelitiannya masih mencakup dalam konteks kejahatan siber secara umum.

Kesenjangan penelitian yang ada di atas, menunjukkan perlunya studi lebih lanjut mengenai penerapan metode NIJ dalam analisis forensik digital pada kasus penyebaran konten ilegal. Oleh karena itu, tujuan dari penelitian ini adalah untuk menganalisis penerapan metode NIJ dalam investigasi forensik digital pada kasus penyebaran konten ilegal berbentuk *cyberbullying* pada media sosial *Facebook Messenger*. Penelitian ini akan mengeksplorasi bagaimana metode NIJ dapat digunakan untuk mengidentifikasi, mengumpulkan, dan menganalisis bukti digital yang terkait dengan penyebaran konten ilegal, serta mengevaluasi efektivitasnya dalam mendukung proses penegakan hukum.

Penelitian ini diharapkan dapat memberikan kontribusi ilmiah yang signifkan dalam pengembangan ilmu forensik digital, khususnya berfokus pada penanganan konten ilegal di *platform* media sosial. Penelitian ini tidak hanya memperkaya literatur akademik, tetapi juga memberikan wawasan praktis bagi para penegak hukum dan praktisi digital forensik dalam meningkatkan kualitas penyidikan dan penyajian bukti. Dengan demikian, hasil penelitian ini dapat menjadi rujukan dalam penyusunan strategi yang lebih efektif dalam menghadapi tantangan kejahatan siber, serta mendukung upaya perlindungan masyarakat dari dampak negatif distribusi konten ilegal di era digital.

2. Tinjauan Pustaka

2.1. Analisis

Analisis adalah kegiatan yang mencakup berbagai tindakan, seperti mengurai, membedakan, memilah sesuatu untuk digolongkan serta dikelompokkan kembali sesuai dengan standar tertentu. Selanjutnya, tindakan tersebut dilanjutkan dengan mencari hubungan dan interpretasi maknanya [6].

2.2. Forensik

Forensik adalah proses penyelidikan yang bertujuan untuk menentukan fakta-fakta yang berkaitan dengan peristiwa kriminal dan isu hukum lainnya [7].

2.3. Digital

Digital merupakan manifestasi dari modernisasi dalam penggunaan teknologi yang terus berkembang seiring waktu. Digital ini beroperasi dengan cara yang lebih profesional menggunakan sebuah sistem dan mengurangi ketergantungan pada tenaga manusia untuk pengoperasiannya [8].

2.4. Forensik Digital

Forensik digital merupakan cabang dari teknologi informasi dan ilmu pengetahuan yang berfokus pada proses investigasi serta analisis terhadap bukti-bukti digital dan perangkat elektronik yang berkaitan dengan tindak kejahatan siber [9].

2.5. Kasus

Kasus adalah keadaan sebenarnya dari suatu masalah, situasi, serta kondisi-kondisi tertentu yang berkaitan dengan seseorang atau suatu hal [10].

2.6. Penyebaran

Penyebaran didefinisikan sebagai proses distribusi ide baru dari sumber penemuannya kepada pengguna atau penerima akhir. Proses ini bisa memakan waktu cukup lama dan membutuhkan dukungan kuat dari semua pihak yang terlibat [11].

2.7. Konten

Konten adalah informasi atau pengalaman yang disampaikan melalui berbagai media dan format untuk menyampaikan pesan yang bersifat edukatif, menghibur, atau memberikan informasi kepada audiens. Konten bisa berupa teks, gambar, audio, video, atau kombinasi dari semua format tersebut [12].

2.8. Ilegal

Ilegal berarti tidak sah menurut hukum, yang dalam konteks ini mencakup pelanggaran hukum, barang yang diperoleh secara gelap, liar, atau tidak memiliki izin dari pihak yang berwenang [13].

Copyright © Jurnal Nasional Komputasi dan Teknologi Informasi (JNKTI)

Jurnal Nasional Komputasi dan Teknologi Informasi (JNKTI)
Vol. 8 No. 4, Agustus 2025
P-ISSN 2620-8342
E-ISSN 2621-3052

2.9. Konten Ilegal

Konten ilegal merujuk pada informasi atau dokumen elektronik yang mengandung konten yang melanggar norma, seperti perjudian, penghinaan atau pencemaran nama baik, pemerasan dan/atau ancaman, serta penyebaran berita palsu dan menyesatkan yang dapat merugikan pengguna [14].

2.10. Penyebaran Konten Ilegal

Penyebaran konten ilegal merupakan salah satu jenis kejahatan siber yang paling berbahaya bagi masyarakat. Konten yang disebarkan dapat berupa ujaran kebencian, pornografi anak, berita palsu, dan konten yang melanggar hak cipta. Penyebaran konten yang melanggar hukum dapat menimbulkan ketegangan sosial, gangguan psikologis pada korban, dan bahkan tindakan kekerasan [15].

2.11. *Cyberbullying*

Cyberbullying didefinisikan sebagai tindakan yang secara sengaja dan berulang kali menyerang, menghina, atau merugikan individu lain melalui media sosial, aplikasi pesan instan, atau metode lain yang dapat menyebabkan penghinaan terkait SARA [16].

2.12. *Facebook Messenger*

Facebook Messenger adalah aplikasi pesan instan yang memungkinkan pengguna berkomunikasi secara langsung melalui teks, gambar, video, dan suara. Aplikasi ini terhubung dengan *platform Facebook* dan menjadi salah satu media sosial yang paling diminati di kalangan pengguna *smartphone* [17].

2.13. *FTK Imager*

Perangkat lunak forensik *FTK Imager*, berfungsi untuk menghasilkan salinan digital menyeluruh (*image*) dari perangkat penyimpanan, seperti *hard drive* atau USB dengan metode *bit-by-bit*. Hal ini memastikan bahwa seluruh data, termasuk file tersembunyi dan yang dihapus, tersalin tanpa mengubah data asli. *FTK Imager* sangat krusial dalam proses penyidikan forensik digital, karena memungkinkan penyidik untuk memperoleh bukti yang akurat dan utuh dari perangkat yang sedang diselidiki [18].

2.14. *Autopsy*

Autopsy merupakan perangkat lunak forensik sumber terbuka (*open source*) yang dikembangkan oleh *Basis Technology Corp* dan diperbarui secara rutin oleh komunitas pengembang terbuka. Perangkat lunak ini digunakan untuk melakukan analisis pada perangkat keras, perangkat lunak, serta data digital. *Autopsy* sangat bermanfaat bagi profesional forensik, termasuk penegak hukum, tim investigasi keamanan informasi, serta individu yang ingin menganalisis perangkat lunak atau data digital. Perangkat lunak ini kompatibel dengan sistem operasi seperti, *Windows*, *Linux*, dan *MacOS*. Selain itu, *Autopsy* menawarkan berbagai *plugin* yang memungkinkan pengguna untuk memperluas fungsionalitas perangkat lunak sesuai dengan kebutuhan [19].

2.15. *DB Browser for SQLite*

DB Browser for SQLite adalah aplikasi desktop yang dirancang untuk melihat dan mengelola *database SQLite*. Fitur-fitur yang ditawarkan oleh *DB Browser for SQLite* meliputi kemampuan untuk mengelola *database SQLite*, mengeksekusi berbagai jenis *query* SQL, dan melihat serta mencari tabel yang ada dalam *database* [20].

2.16. *Smartphone*

Smartphone adalah perangkat media interaktif yang mengintegrasikan kemampuan komputer dan telepon, menciptakan alat canggih dengan berbagai fitur, seperti pengiriman pesan, kamera, pemutar musik, perekaman, pengalihan, akses email, TV yang terhubung dengan komputer, tampilan layar, pemantauan data pribadi, GPS, layanan telepon melalui web, serta kemampuan untuk digunakan sebagai kartu kredit [21].

2.17. *Flashdisk*

Flashdisk atau yang juga disebut dengan USB *flash drive*, merupakan perangkat penyimpanan data portabel yang memanfaatkan memori *flash* untuk menyimpan data. *Flashdisk* mudah untuk dibawa kemana saja, karena memiliki ukuran yang kecil dan ringan. Perangkat ini dapat dihubungkan ke komputer atau perangkat lain melalui *port* USB, yang memungkinkan pengguna dengan cepat dan efisien dalam menyimpan, mentransfer, serta mengakses data [22].

3. Metode Penelitian

3.1. Objek Penelitian

Objek dalam penelitian ini adalah aktivitas digital yang berkaitan dengan penyebaran konten ilegal berbentuk *cyberbullying* melalui aplikasi *Facebook Messenger*. Aktivitas tersebut dianalisis melalui proses forensik digital terhadap data yang tersimpan dalam perangkat Android (*smartphone*), yang kemudian diakusisi ke media penyimpanan eksternal (*flashdisk*), yang secara khusus telah disimulasikan sebagai alat bukti digital.

3.2. Metode Penelitian

Metode yang digunakan dalam penelitian ini adalah metode kualitatif deskriptif dengan pendekatan studi kasus simulatif. Penelitian ini menggunakan metode *National Institute of Justice* (NIJ) sebagai kerangka kerja dalam proses investigasi forensik digital, yang mencakup lima tahapan sistematis, yaitu: identifikasi, pengumpulan, pemeriksaan, analisis, dan pelaporan.

Copyright © Jurnal Nasional Komputasi dan Teknologi Informasi (JNKTI)

Jurnal Nasional Komputasi dan Teknologi Informasi (JNKTI)
Vol. 8 No. 4, Agustus 2025
P-ISSN 2620-8342
E-ISSN 2621-3052

3.3. Persiapan Simulasi

3.3.1. Alat dan Perangkat

Penelitian ini menggunakan perangkat keras (*hardware*), yaitu *Smartphone*, *Flashdisk*, *Laptop*, dan Kabel USB serta perangkat lunak (*software*), yaitu *FTK Imager*, *Autopsy*, dan *DB Browser for SQLite,* untuk mendukung proses analisis forensik digital.

3.3.2. Rancangan Skenario Kasus

Penelitian ini menggunakan skenario kasus simulatif yang dirancang oleh penulis untuk memperoleh dan menganalisis barang bukti digital. Skenario ini menggambarkan aktivitas penyebaran konten ilegal dalam bentuk *cyberbullying* melalui aplikasi *Facebook Messenger*. Rancangan skenario ini bertujuan untuk menggambarkan proses penyebaran konten ilegal dan mengevaluasi kemampuan perangkat lunak forensik digital dalam merekonstruksi bukti yang telah dihapus, serta memperoleh informasi mengenai data percakapan yang dapat dipulihkan. Rancangan skenario kasus dalam penelitian ini adalah sebagai berikut:

1. Pembuatan akun *Facebook Messenger* milik korban.
2. Pembuatan akun *Facebook Messenger* milik pelaku.
3. Pelaku mengirimkan pesan berisi ancaman dan penghinaan fisik kepada korban melalui *Facebook Messenger*.
4. Pelaku menghapus pesan yang dikirimkan kepada korban melalui *Facebook Messenger*.
5. Pesan yang dihapus oleh pelaku di *Facebook Messenger* akan diungkap menggunakan alat forensik, yaitu *FTK Imager*, *Autopsy*, dan *DB Browser for SQLite*, untuk memperoleh bukti digital.

3.4. Teknik Pengumpulan Data

3.4.1. Observasi

Penulis melakukan observasi secara langsung selama proses investigasi digital dengan memperhatikan setiap tahap penggunaan perangkat lunak forensik yang digunakan, yaitu *FTK Imager*, *Autopsy*, dan *DB Browser for SQLite*. Aktivitas yang diamati meliputi proses instalasi, konfigurasi, ekstraksi data, navigasi file digital, serta pencatatan jejak aktivitas digital pada perangkat yang dianalisis.

3.4.2. Dokumentasi

Dokumentasi dilakukan dengan mengumpulkan data pendukung selama proses investigasi berlangsung, meliputi tangkapan layar dari aplikasi, *log* sistem yang mencatat aktivitas digital, dan laporan hasil analisis yang dihasilkan oleh perangkat lunak forensik dalam berbagai format.

3.5. Proses Tahapan Metode *National Institute of Justice* (NIJ)

3.5.1. Tahap Identifikasi (*Identification*)

Tahap identifikasi diawali dengan penentuan perangkat digital yang relevan dalam skenario simulatif kasus *cyberbullying*, yakni sebuah *smartphone* yang menyimpan riwayat percakapan *Facebook Messenger* yang menjadi media komunikasi pelaku dalam menyampaikan pesan bernada ancaman dan penghinaan. Proses ini dilanjutkan dengan penelusuran bukti digital, terutama file *database* yang berisi rekaman komunikasi antara pelaku dan korban.

3.5.2. Tahap Pengumpulan (*Collection*)

Tahap pengumpulan dilakukan untuk memperoleh dan mengamankan bukti digital secara terstruktur dalam skenario simulatif. Proses dimulai dengan menghubungkan *smartphone* ke *laptop* untuk melakukan akuisisi *database Facebook Messenger* melalui *Minimal ADB & Fastboot* di *Command Prompt*. Hasil akuisisi kemudian dipindahkan ke *flashdisk* sebagai media penyimpanan terpisah guna menjaga keamanan data. Selanjutnya, *FTK Imager* digunakan untuk membuat *forensic image* dari media tersebut sehingga integritas dan keaslian bukti tetap terjamin.

3.5.3. Tahap Pemeriksaan (*Examination*)

Tahap pemeriksaan difokuskan pada verifikasi integritas dan kelayakan bukti digital sebelum dianalisis lebih lanjut. *Forensic image* ditinjau menggunakan *FTK Imager* untuk memvalidasi nilai hash, memeriksa struktur file, dan mengekspor folder *database* sebagai objek utama penelitian. Berkas yang diekstraksi kemudian diperiksa melalui *Autopsy* guna mengidentifikasi artefak tersembunyi maupun data yang telah terhapus. Selanjutnya, *database* diperiksa menggunakan *DB Browser for SQLite* untuk memastikan konsistensi struktur dan keutuhan data sehingga siap digunakan pada tahap analisis.

3.5.4. Tahap Analisis (*Analysis*)

Tahap analisis berfokus pada pengolahan dan penafsiran data untuk mengungkap keterkaitan antara artefak digital dalam skenario simulatif. File *database* berformat *.db* dibuka menggunakan *DB Browser for SQLite* untuk menelusuri struktur tabel dan isi pesan secara menyeluruh. Metadata pesan termasuk waktu pengiriman, identitas pengirim, dan penerima ditelaah guna memetakan pola komunikasi dalam insiden yang disimulasikan. Hasil penelusuran kemudian dikaitkan dengan aktivitas pelaku, sehingga hubungan kronologis dan indikasi keterlibatan dapat diidentifikasi secara sistematis dan mendukung tujuan analisis forensik.

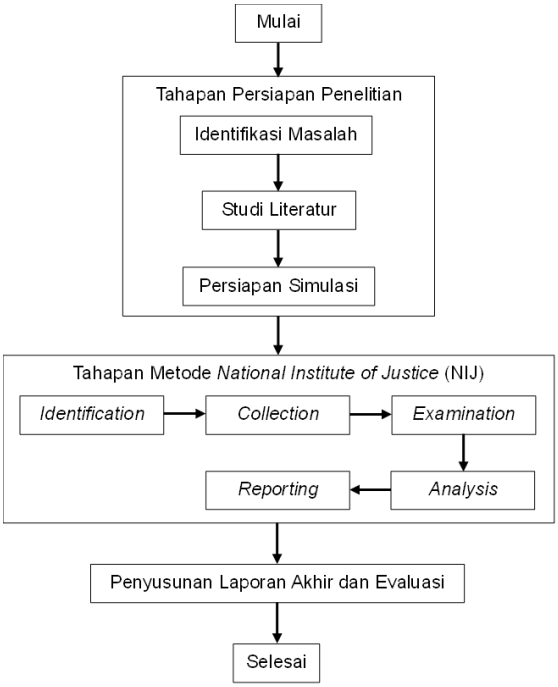
Copyright © Jurnal Nasional Komputasi dan Teknologi Informasi (JNKTI)

Jurnal Nasional Komputasi dan Teknologi Informasi (JNKTI)
Vol. 8 No. 4, Agustus 2025
P-ISSN 2620-8342
E-ISSN 2621-3052

3.5.5. Tahap Pelaporan (*Reporting*)

Tahap pelaporan menjadi langkah akhir yang merangkum seluruh hasil investigasi forensik digital dalam format yang terstruktur dan dapat dipertanggungjawabkan. Pada tahap ini, *FTK Imager* digunakan untuk menampilkan *forensic image* sekaligus memverifikasi nilai *hash* sebagai dasar keabsahan data. *Autopsy* kemudian dimanfaatkan untuk mendokumentasikan artefak digital yang diperoleh dari proses analisis, sedangkan *DB Browser for SQLite* berperan dalam menyusun ringkasan temuan terkait struktur dan isi *database*. Seluruh hasil tersebut dihimpun dalam laporan akhir yang disajikan dalam format PDF agar siap digunakan sebagai dokumen pendukung dalam proses penegakan hukum.

3.6. Tahapan Penelitian



Gambar 1. Tahapan Penelitian

4. Hasil dan Pembahasan

Bagian ini menyajikan hasil penelitian forensik digital berdasarkan lima tahapan metode *National Institute of Justice* (NIJ), yaitu identifikasi, pengumpulan, pemeriksaan, analisis, dan pelaporan. Seluruh temuan diperoleh dari skenario simulatif yang merepresentasikan kasus penyebaran konten ilegal berbentuk *cyberbullying* melalui aplikasi *Facebook Messenger*.

4.1. Tahap Identifikasi (*Identification*)

Tahap identifikasi berhasil menentukan perangkat dan aplikasi yang digunakan, serta bukti digital yang relevan pada simulasi kasus *cyberbullying*. Perangkat yang digunakan, yaitu sebuah *smartphone* yang telah di-*root* menggunakan *Magisk*, memungkinkan akses penuh terhadap direktori sistem internal yang umumnya terlindungi.

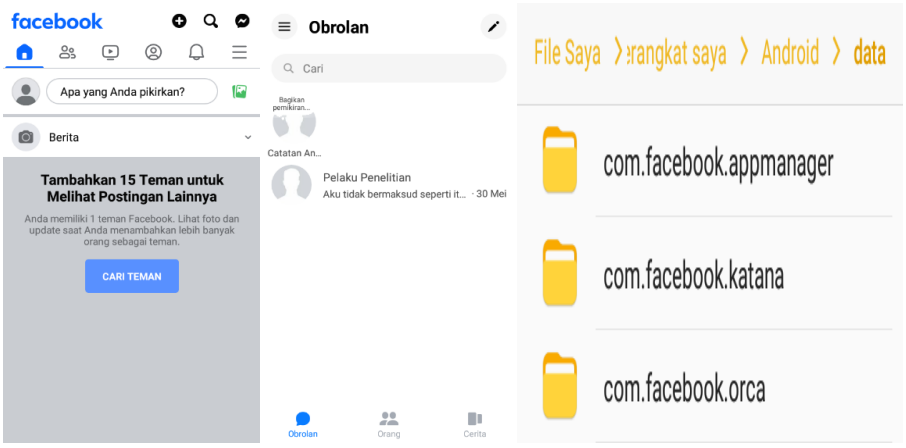


Gambar 2. Perangkat Android Simulasi

Copyright © Jurnal Nasional Komputasi dan Teknologi Informasi (JNKTI)

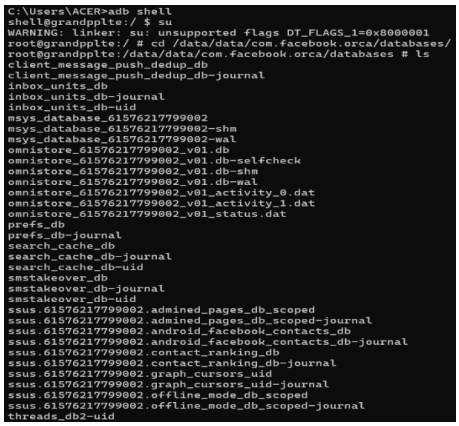
Jurnal Nasional Komputasi dan Teknologi Informasi (JNKTI)
Vol. 8 No. 4, Agustus 2025
P-ISSN 2620-8342
E-ISSN 2621-3052

Aplikasi yang diidentifikasi sebagai media komunikasi pelaku dalam melakukan *cyberbullying*, yaitu *Facebook Messenger* dengan nama paket *com.facebook.orca* yang menyediakan struktur direktori dan basis data lokal yang dapat diakses secara utuh dalam konteks forensik.



Gambar 3. Tampilan *Facebook Messenger* dan Struktur Direktori Android

Bukti digital yang relevan, yaitu file *database Facebook Messenger* berhasil diidentifikasi melalui perintah ADB di CMD. Hasil dari perintah tersebut menunjukkan keberadaan file *msys_database_61576217799002*, *threads_db2-uid*, dan file lainnya yang mengindikasikan penyimpanan riwayat pesan dan metadata aplikasi.



Gambar 4. Perintah ADB dan Daftar File *Database* di CMD

4.2. Tahap Pengumpulan (*Collection*)

Tahap pengumpulan menghasilkan akuisisi bukti digital secara lengkap dan terverifikasi dari perangkat yang digunakan dalam skenario simutalif. File *database* yang berada di direktori *com.facebook.orca/databases/* berhasil disalin ke direktori umum */sdcard/* menggunakan ADB di CMD, kemudian dipindahkan ke *flashdisk* sebagai media penyimpanan terpisah. Pemindahan ini memastikan bahwa bukti digital tidak lagi bersentuhan langsung dengan perangkat sumber, sehingga risiko perubahan data dapat diminimalkan.

```
C:\Users\ACER>adb shell
shell@grandpplte:/ $ su
WARNING: linker: su: unsupported flags DT_FLAGS_1=0x8000001
root@grandpplte:/ # cd /data/data/com.facebook.orca/
root@grandpplte:/data/data/com.facebook.orca # cp -r databases /sdcard/msg_db
```

Gambar 5. Proses Penyalinan File *Database* ke Direktori Umum

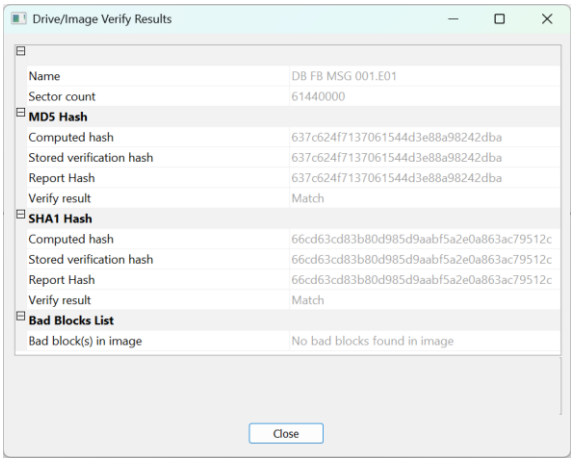
```
C:\Users\ACER>adb pull /sdcard/msg_db "F:\File DB"
/sdcard/msg_db/: 34 files pulled, 0 skipped. 2.7 MB/s (13418157 bytes in 4.710s)
```

Gambar 6.Proses Penyalinan File *Database* dari *Smartphone* ke *Flashdisk*

Selanjutnya, pembuatan *forensic image* dilakukan menggunakan *FTK Imager* terhadap *flashdisk* yang berisi folder *database* yang bernama *msg_db*. Proses akuisisi menghasilkan *image* berformat E01 yang kemudian diverifikasi melalui perhitungan nilai *hash* MD5 dan SHA1. Hasil verifikasi menunjukkan kecocokan nilai *hash* antara media sumber dan *image* forensik, menegaskan bahwa data tidak mengalami perubahan selama proses akuisisi.

Copyright © Jurnal Nasional Komputasi dan Teknologi Informasi (JNKTI)

Jurnal Nasional Komputasi dan Teknologi Informasi (JNKTI)
Vol. 8 No. 4, Agustus 2025
P-ISSN 2620-8342
E-ISSN 2621-3052

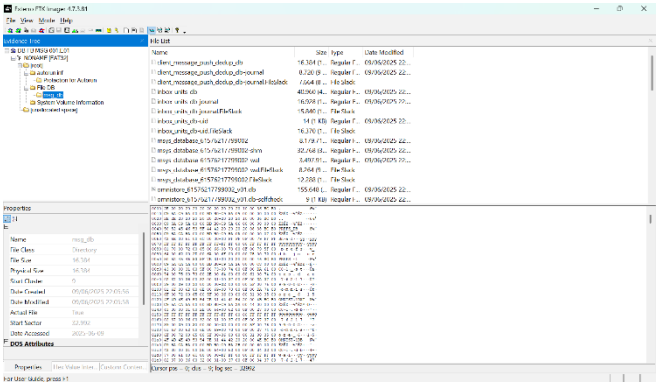


Gambar 7. Hasil Verifikasi Nilai *Hash* MD5 dan SHA1 di *FTK Imager*

Tahap ini memperlihatkan bahwa seluruh bukti digital berhasil diamankan dalam kondisi utuh dan dapat dipertanggungjawabkan. Integritas data yang terjamin menjadi dasar penting bagi tahapan pemeriksaan dan analisis berikutnya, sekaligus menunjukkan keberhasilan proses tahapan pengumpulan.

4.3. Tahap Pemeriksaan (*Examination*)

Tahap pemeriksaan berhasil memverifikasi keaslian bukti digital serta memeriksa struktur data yang terdapat dalam file *database*. FTK *Imager* digunakan untuk memverifikasi nilai *hash* MD5 dan SHA1 dan membuka struktur direktori secara aman, menunjukkan bahwa folder *database* dengan nama *msg_db* dapat diakses tanpa kerusakan maupun modifikasi.



Gambar 8. Tampilan Struktur File di *FTK Imager*

Table 1. Hasil Perbandingan Nilai *Hash* MD5 dan SHA1 di *FTK Imager*

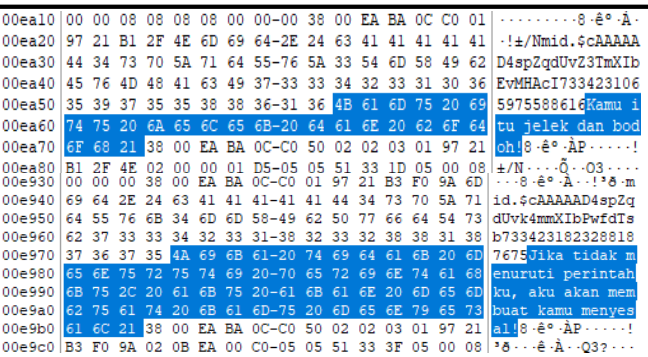
Algoritma Hash	Nilai Hash saat Akuisisi	Nilai Hash saat Pemeriksaan	Hasil Verifikasi
MD5	637c624f7137061544d3e88a98242dba	637c624f7137061544d3e88a98242dba	Cocok (*Match*)
SHA1	66cd63cd83b80d985d9aabf5a2e0a863ac79512c	66cd63cd83b80d985d9aabf5a2e0a863ac79512c	Cocok (*Match*)

Melalui tampilan *Hex Viewer* pada file *msys_database_61576217799002* sebagai *database* utama, ditemukan artefak pesan yang telah dihapus, termasuk fragmen teks yang mengandung hinaan dan ancaman, serta jejak pembatalan pengiriman pesan. Temuan ini mengonfirmasi bahwa residu digital dari pesan yang telah terhapus masih tersimpan dalam struktur file, meskipun tidak terlihat lagi oleh pengguna.

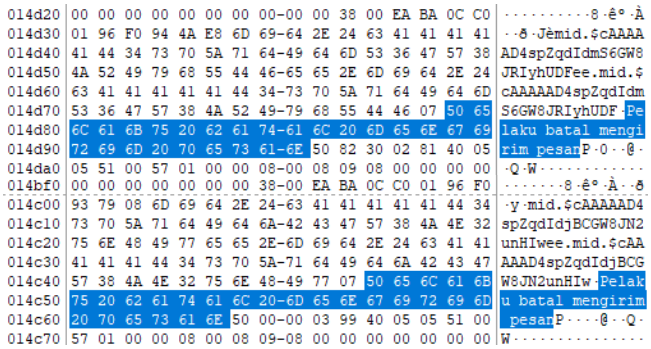
Copyright © Jurnal Nasional Komputasi dan Teknologi Informasi (JNKTI)

Accredited SINTA 5
72/E/KPT/2024

Jurnal Nasional Komputasi dan Teknologi Informasi (JNKTI)
Vol. 8 No. 4, Agustus 2025
P-ISSN 2620-8342
E-ISSN 2621-3052

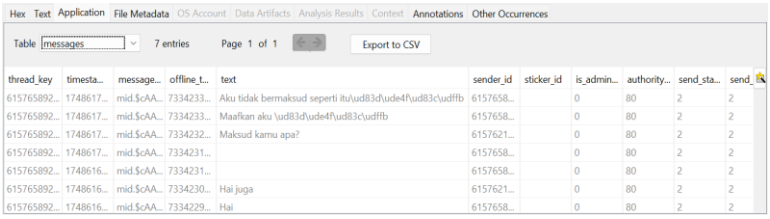


Gambar 9. Temuan Pesan yang Telah Dihapus di *FTK Imager*



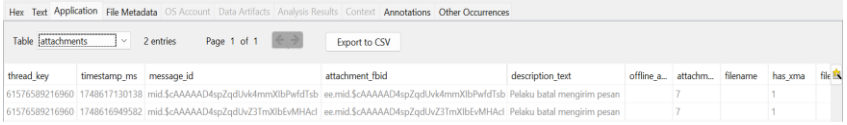
Gambar 10. Temuan Jejak Pembatalan Pengiriman Pesan di *FTK Imager*

Pemeriksaan dilanjutkan menggunakan *Autopsy* terhadap file *msys_database_61576217799002*, ditemukan sejumlah entri yang menunjukkan isi komunikasi yang masih aktif, termasuk isi pesan (*text*), identitas pengirim (*sender_id*), serta waktu dalam format *timestamp_ms* pada tabel *messages*. Selain itu, terdapat entri-entri kosong yang mengindikasikan adanya pesan yang telah dihapus namun strukturnya masih tertinggal dalam *database*.



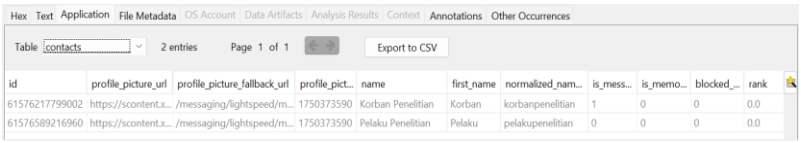
Gambar 11. Temuan pada Tabel *Messages* di *Autopsy*

Pemeriksaan juga dilakukan terhadap tabel *attachments*, yang berhasil menampilkan entri pada kolom *description_text* dengan isi "Pelaku batal mengirim pesan". Hal ini memperkuat bahwa pembatalan pesan terekam secara eksplisit dalam sistem internal aplikasi. Selain itu, kolom *message_id*, *thread_key*, dan *timestamp_ms* menunjukkan hubungan yang kuat antara entri tersebut dan aktivitas komunikasi aktual.



Gambar 12. Temuan pada Tabel *Attachments* di *Autopsy*

Autopsy juga berhasil mengidentifikasi entri dalam tabel *contacts*, yang menampilkan data identitas pelaku dan korban, seperti nama asli (*name*) dan nama yang telah dinormalisasi (*normalized_name*). Ini memungkinkan keterkaitan antara subjek dengan isi pesan yang dianalisis.

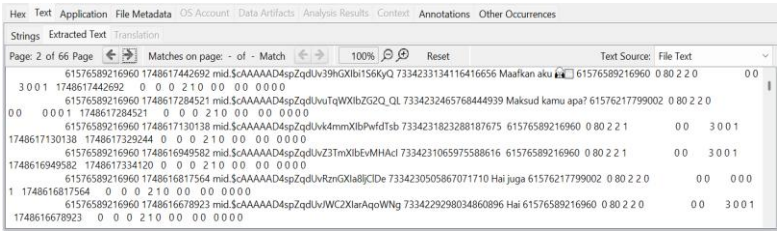


Gambar 13. Temuan pada Tabel *Contacts* di *Autopsy*

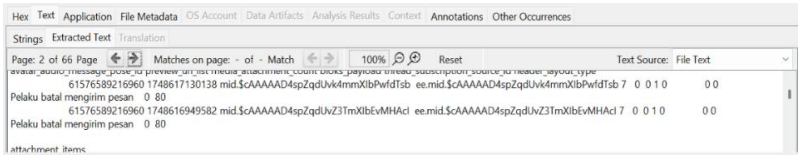
Copyright © Jurnal Nasional Komputasi dan Teknologi Informasi (JNKTI)

Jurnal Nasional Komputasi dan Teknologi Informasi (JNKTI)
Vol. 8 No. 4, Agustus 2025
P-ISSN 2620-8342
E-ISSN 2621-3052

Pada tampilan tab *Extracted Text*, ditemukan artefak pesan aktif yang masih tersimpan utuh dalam file *database*, dan artefak pesan yang telah dihapus yang ditunjukkan oleh baris-baris kosong tanpa teks tetapi masih menyimpan metadata pesan. Selain itu, ditemukan juga jejak artefak teks yang menunjukkan aktivitas pembatalan pengiriman pesan oleh pelaku. Temuan ini memberikan bukti tambahan bahwa artefak komunikasi tetap tersimpan dalam sistem meskipun tidak lagi muncul di aplikasi pengguna.

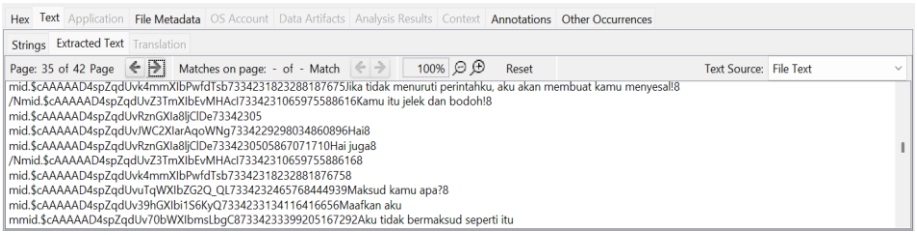


Gambar 14. Temuan Artefak Pesan Aktif dan Dihapus di *Autopsy*

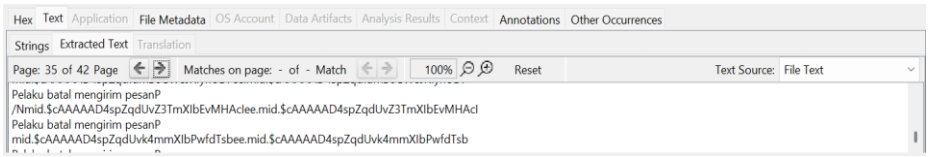


Gambar 15. Temuan Awal Jejak Pembatalan Pengiriman Pesan di *Autopsy*

Selanjutnya, pada file *msys_database_61576217799002-wal*, ditemukan sejumlah artefak penting melalui tab *Extracted Text*. Artefak tersebut mencakup pesan-pesan yang mengandung unsur hinaan dan ancaman, seperti “Kamu itu jelek dan bodoh” dan “Jika tidak menuruti perintahku, aku akan membuat kamu menyesal.” Selain itu, jejak teks yang menunjukkan bahwa pelaku membatalkan pengiriman pesan juga ditemukan pada tab *Extracted Text*, seperti halnya pada file *msys_database_61576217799002*. Temuan ini memperkuat bukti bahwa file *wal* menyimpan jejak aktivitas yang belum tertulis secara permanen dalam *database* utama.



Gambar 16. Temuan Pesan yang Telah Dihapus di *Autopsy*



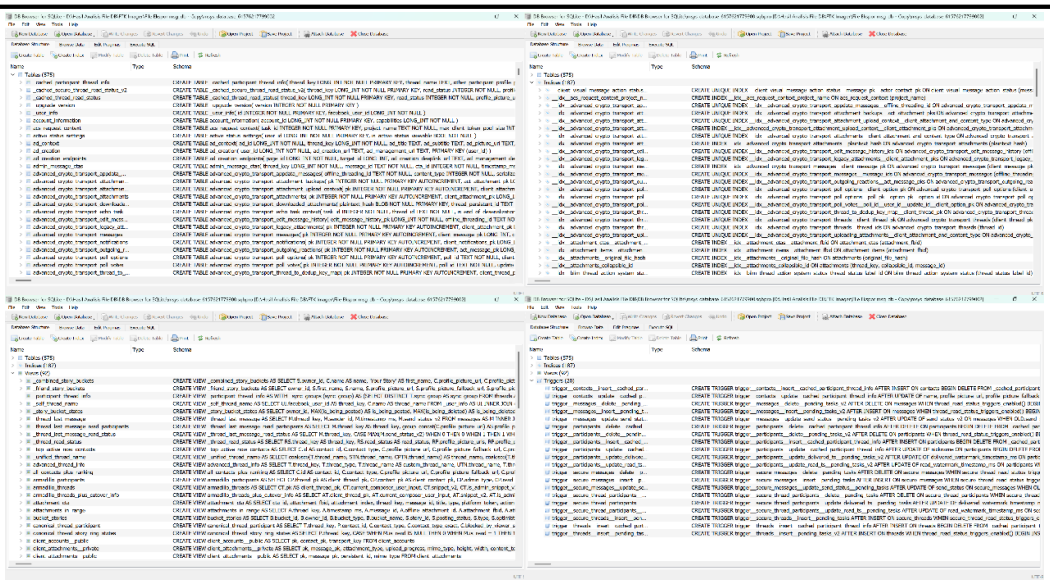
Gambar 17. Temuan Lanjutan Jejak Pembatalan Pengiriman Pesan di *Autopsy*

Keberadaan artefak baik pada file utama maupun file *wal* menunjukkan bahwa *Autopsy* mampu mengakses tidak hanya file yang telah disimpan secara permanen, tetapi juga file *log* sementara yang merekam aktivitas terbaru pengguna sebelum dituliskan secara permanen ke dalam *database* utama. Hal ini menjadikan kedua file tersebut sebagai sumber data penting dalam mendeteksi komunikasi yang dihapus secara sengaja oleh pelaku.

Pemeriksaan selanjutnya dilakukan menggunakan *DB Browser for SQLite* yang menunjukkan bahwa seluruh bagian struktur internal *database* berhasil dimuat secara utuh dan ditampilkan sesuai struktur standar *database*, termasuk objek penting, seperti tabel, indeks, *trigger*, dan *view*. Tidak ditemukan adanya kerusakan struktur atau ketidaksesuaian data, yang menandakan bahwa file *database* berada dalam kondisi baik dan siap untuk dianalisis lebih lanjut.

Copyright © Jurnal Nasional Komputasi dan Teknologi Informasi (JNKTI)

Accredited SINTA 5 72/E/KPT/2024
Jurnal Nasional Komputasi dan Teknologi Informasi (JNKTI)
Vol. 8 No. 4, Agustus 2025
P-ISSN 2620-8342
E-ISSN 2621-3052

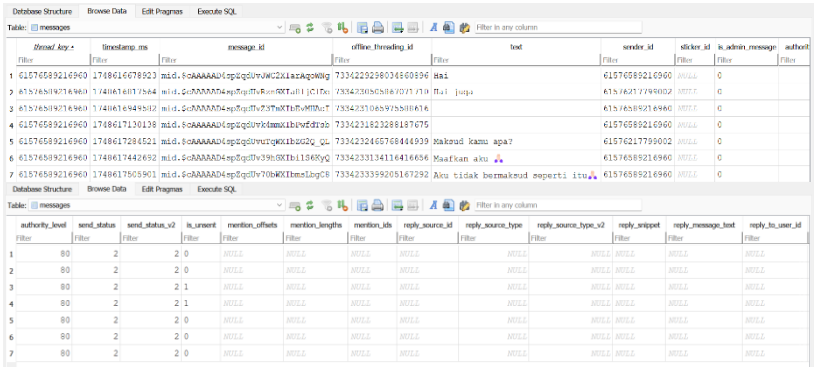


Gambar 18. Struktur File *Database* di *DB Browser for SQLite*

Tahap pemeriksaan ini menghasilkan validasi integritas bukti digital, identifikasi pesan yang telah dihapus dan jejak pembatalan pengiriman pesan, serta pemetaan struktur internal *database* yang utuh dan dapat dianalisis lebih lanjut. Temuan-temuan ini menjadi dasar yang kuat untuk dilanjutkan pada tahap analisis guna menginterpretasikan keterkaitan artefak digital dengan aktivitas pelaku dalam kasus penyebaran konten ilegal.

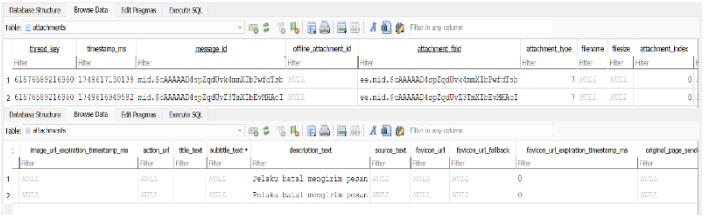
4.4. Tahap Analisis (*Analysis*)

Tahap analisis menafsirkan seluruh artefak digital yang telah diperiksa untuk memahami pola komunikasi dan aktivitas pelaku dalam simulasi kasus *cyberbullying*. Proses analisis dilakukan melalui *DB Browser for SQLite* yang memperlihatkan bahwa tabel *messages* memiliki metadata seperti *timestamp_ms* menunjukkan waktu pengiriman, sedangkan *sender_id* mengidentifikasi akun pengirim. Kolom *is_unsent* pada beberapa entri bernilai 1, yang menjadi indikator bahwa pesan tersebut telah dihapus setelah dikirim oleh pelaku. Hal ini menunjukkan bahwa meskipun isi pesan tidak lagi tampil, upaya penghapusan masih dapat ditelusuri melalui metadata.



Gambar 19. Temuan pada Tabel *Messages* di *DB Browser for SQLite*

Analisis terhadap tabel *attachments* menunjukkan adanya entri yang memiliki relasi dengan *message_id*, namun tidak menampilkan file media aktif. Kolom *description_text* memberikan informasi bahwa pengiriman pesan dibatalkan oleh pelaku. Meskipun tidak ditemukan nama atau jenis file yang dikirimkan, keterhubungan antara pesan dan entri dalam tabel tersebut mengindikasikan adanya upaya pengiriman pesan yang kemudian dibatalkan.

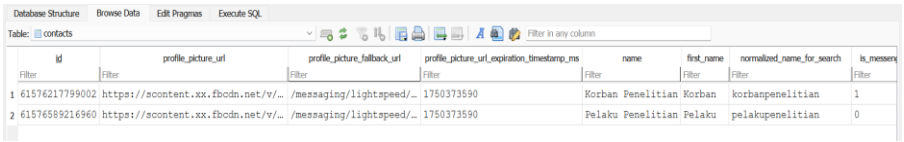


Gambar 20. Temuan pada Tabel *Attachment* di *DB Browser for SQLite*

Copyright © Jurnal Nasional Komputasi dan Teknologi Informasi (JNKTI)

Jurnal Nasional Komputasi dan Teknologi Informasi (JNKTI)
Vol. 8 No. 4, Agustus 2025
P-ISSN 2620-8342
E-ISSN 2621-3052

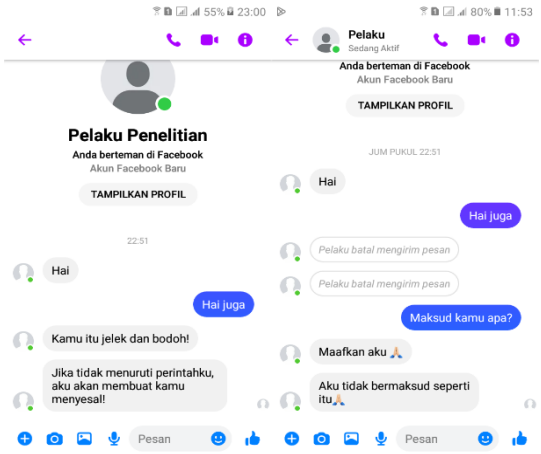
Pada tabel *contacts* berisi informasi akun pengguna yang terlibat dalam percakapan. Berdasarkan hasil analisis, ditemukan dua entri akun yang mengindikasikan pihak pelaku dan korban. Masing-masing akun ditampilkan dengan ID dan nama pengguna, sehingga memperkuat hubungan antarentitas yang terlibat dalam komunikasi digital.



Gambar 21. Temuan pada Tabel *Contacts* di *DB Browser for SQLite*

Hasil analisis selanjutnya diperkuat dengan temuan dari *FTK Imager* dan *Autopsy* yang mengungkap pesan berisi hinaan dan ancaman melalui tampilan *hexadecimal*, *extracted text*, dan fragmen dalam file WAL. Konsistensi temuan dari ketiga perangkat lunak ini menunjukkan bahwa meslipun pesan dihapus, jejak digital tetap dapat dipulihkan.

Tangkapan layar aplikasi *Facebook Messenger* pada perangkat simulasi kemudian mengonfirmasi bahwa pesan aktif memiliki kesesuaian dengan entri pada *database SQLite*. Sementara pesan terhapus yang ditampilkan sebagai "Pelaku batal mengirim pesan" pada aplikasi terbukti memiliki jejak metadata dan fragmen teks pada artefak forensik.



Gambar 22. Tangkapan Layar Pesan Aktif & Dihapus di *Facebook Messenger*

Dengan demikian, tahap analisis ini berhasil mengungkap keterkaitan antara aktivitas pelaku dengan artefak digital yang tersimpan, serta membangun pemahaman bahwa proses komunikasi dalam skenario cyberbullying tetap dapat direkonstruksi secara utuh melalui korelasi antara database utama, file WAL, dan visualisasi biner.

4.5. Tahap Pelaporan (*Reporting*)

Tahap pelaporan menyajikan seluruh temuan dalam bentuk dokumentasi komprehensif yang mengintegrasikan bukti dari *FTK Imager*, *Autopsy*, dan *DB Browser for SQLite*. *FTK Imager* memberikan dasar verifikasi integritas melalui nilai *hash* dan ringkasan struktur *image*. *Autopsy* menunjukkan dokumentasi artefak pesan aktif, pesan terhapus, pembatalan pengiriman pesan, serta data identitas pengguna. *DB Browser for SQLite* menyediakan rincian struktur tabel dan relasi metadata yang memperkuat konteks analisis. Seluruh hasil tersebut kemudian dirangkum dalam laporan final berformat PDF agar tidak dapat dimodifikasi dan dapat dipertanggungjawabkan secara akademik maupun forensik. Tahap pelaporan ini menegaskan transparansi proses investigasi serta memastikan bahwa seluruh rangkaian analisis mengikuti prosedur NIJ secara konsisten.

5. Kesimpulan

Berdasarkan hasil analisis dan pembahasan yang telah dilakukan, beberapa kesimpulan dapat diambil sebagai berikut:

Pentingnya pendekatan forensik digital dalam menangani kasus penyebaran konten ilegal berbentuk *cyberbullying* melalui aplikasi *Facebook Messenger* terbukti signifikan. Pendekatan ini memungkinkan proses identifikasi, pengumpulan, pemeriksaan, analisis, dan pelaporan bukti digital dilakukan secara sistematis, terstruktur, dan dapat dipertanggungjawabkan secara hukum. Keberadaan data digital yang bersifat sementara dan mudah dihapus menuntut adanya metode forensik untuk mendokumentasikan dan memverifikasi aktivitas pengguna secara valid.

Penerapan metode *National Institute of Justice* (NIJ) terbukti efektif digunakan dalam proses investigasi forensik digital. Lima tahapan metode ini yang meliputi identifikasi, pengumpulan, pemeriksaan, analisis, dan

Copyright © Jurnal Nasional Komputasi dan Teknologi Informasi (JNKTI)

pelaporan dapat diimplementasikan secara menyeluruh untuk mengungkap interaksi komunikasi antara pelaku dan korban. Temuan berupa metadata, pesan yang telah dihapus, dan *log* aktivitas, mendukung proses penelusuran kembali alur kejadian digital sesuai dengan skenario kasus yang disusun dalam penelitian ini.

Efektivitas perangkat lunak *FTK Imager*, *Autopsy*, dan *DB Browser for SQLite* sangat mendukung proses forensik digital. *FTK Imager* berhasil membuat salinan forensik dan memverifikasi integritas data dengan nilai *hash*. *Autopsy* mendeteksi artefak digital dan aktivitas penghapusan pesan, sementara *DB Browser for SQLite* mengungkap metadata dan struktur *database Facebook Messenger*, termasuk identifikasi pesan yang telah dihapus oleh pelaku. Kombinasi ketiga alat ini mampu mengungkap bukti meskipun sebagian data telah dihapus dari antarmuka pengguna.

Daftar Pustaka

[1] APJII, "APJII Jumlah Pengguna Internet Indonesia Tembus 221 Juta Orang," apjii.or.id. Accessed: Apr. 06, 2025. [Online]. Available: https://apjii.or.id/berita/d/apjii-jumlah-pengguna-internet-indonesia-tembus-221-juta-orang

[2] KOMDIGI, "Terapkan SAMAN pada Februari 2025, MENKOMDIGI Perkuat Perlindungan Masyarakat di Ruang Digital," komdigi.go.id. Accessed: Jan. 28, 2025. [Online]. Available: https://www.komdigi.go.id/berita/siaran-pers/detail/terapkan-saman-pada-februari-2025-menkomdigi-perkuat-perlindungan-masyarakat-di-ruang-digital

[3] S. Marcellino, H. B. Seta, and I. W. Widi, "Analisis Forensik Digital *Recovery* Data *Smartphone* pada Kasus Penghapusan Berkas Menggunakan Metode *National Institute of Justice* (NIJ)," *Inform. J. Ilmu Komput.*, vol. 19, no. 2, pp. 141–156, 2023, doi: 10.52958/iftk.v19i2.4676.

[4] D. Yuliana, T. Yuniati, and B. Parga Zen, "Analisis Forensik Terhadap Kasus *Cyberbullying* pada *Instagram* dan *Whatsapp* Menggunakan Metode *National Institute of Justice* (NIJ)," *Cyber Secur. dan Forensik Digit.*, vol. 5, no. 2, pp. 52–59, 2023, doi: 10.14421/csecurity.2022.5.2.3734.

[5] R. Prasetyawan and R. Indrayani, "Analisis dan *Recovery* Bukti Digital pada Media Sosial di Perangkat *Mobile* Berbasis Android," *EXPLORE*, vol. 13, no. 2, pp. 74–78, 2023.

[6] D. Darmawati, "Analisis Manajemen Pembelajaran Pendidikan Pancasila Dalam Meningkatkan Pemahaman Nilai-Nilai Pancasila Pada Mahasiswa Semester I Prodi Pendidikan Jasmani Unimerz Tahun 2022," *J. Innov. Res. Knowl.*, vol. 2, no. 10, pp. 3937–3946, 2023, doi: 10.53625/jirk.v2i10.5239.

[7] A. Baene and H. Manullang, "Strategi Jaksa Penuntut Umum dalam Membuktikan Tindak Pidana Perjudian *Online*," *J. Dimens. Huk.*, vol. 8, no. 11, pp. 140–147, 2024.

[8] T. A. Nuryadi, "Implementasi Ilmu Manajemen Perkantoran dalam Menghadapi Dunia Bisnis Digital," *Lensa Ilm. J. Manaj. dan Sumberd.*, vol. 2, no. 3, pp. 78–82, 2023, doi: 10.54371/jms.v2i3.297.

[9] S. Sunardi, I. Riadi, and J. Triyanto, "Analisis Forensik Layanan *Signal Private Messenger* pada *Smartwatch* Menggunakan Metode *National Institute of Justice*," *J. Edukasi dan Penelit. Inform.*, vol. 7, no. 3, p. 305, 2021, doi: 10.26418/jp.v7i3.47740.

[10] W. Ayu Putri, P. Qomariyah Dewi Kumala, and F. Qorib, "Perlindungan Hukum Terhadap Saksi dan Korban Pencabulan Menurut UU No 31 Tahun 2014," *JUSTNESS (Jurnal Huk. Polit. dan Agama)*, vol. 4, no. 01, pp. 1–16, 2024.

[11] G. Isnarizanah, N. Fathan, R. A. Mutaqin, and C. Carsiwan, "Peran Teknologi dalam Inovasi Pendidikan di Indonesia," *JIIP - J. Ilm. Ilmu Pendidik.*, vol. 7, no. 8, pp. 8635–8639, 2024, doi: 10.54371/jiip.v7i8.5073.

[12] R. T. Pakpahan, "Pelatihan *Conten Cretaor* Pemula Dalam Memasuki Indsutri Konten Digital," *J. Pustaka Dianmas*, vol. 4, no. 1, pp. 36–44, 2024, doi: 10.32509/dianmas.v4i1.4363.

[13] A. D. Aprilliya, S. Kamariyah, and ..., "Kolaborasi antar Aktor dalam Penanganan Peredaran Rokok Ilegal di Provinsi Jawa Timur," *Soetomo Adm. ...*, no. 7, pp. 501–512, 2023, [Online]. Available: https://ejournal.unitomo.ac.id/index.php/sap/article/download/7265/3412

[14] E. Perwirawati, "Menyikapi Konten Negatif Pada *Platform* Media Sosial *Tiktok*," *J. Kaganga J. Ilm. Sos. dan Hum.*, vol. 7, no. 1, pp. 18–29, 2023, doi: 10.33369/jkaganga.7.1.18-29.

[15] K. Charlaes Bego, F. Rahmat Aziz, R. Asra Rahmad, Sunarto, and H. Budianto, "Tindak Pidana *Cybercrime* : Tantangan Hukum Pidana Menanggulangi Kejahatan di Dunia Maya (Desember 2024) dalam *Cybercrime* : *Criminal Law Challenges in Tackling Cybercrime* (*December*," *J. Kolaboratif Sains*, vol. 8, no. 1, pp. 506–511, 2025, doi: 10.56338/jks.v8i1.6740.

[16] S. Soni, Y. Fatma, and R. Anwar, "Akuisisi Bukti Digital Aplikasi Pesan Instan '*BiP*' Menggunakan Metode *National Institute of Justice* (NIJ)," *J. CoSciTech (Computer Sci. Inf. Technol.*, vol. 3, no. 1, pp. 34–42, 2022, doi: 10.37859/coscitech.v3i1.3694.

[17] S. R. Ardiningtias, S. Sunardi, and H. Herman, "Forensik Digital Kasus Penyebaran Pornografi pada Aplikasi *Facebook Messenger* Berbasis Android Menggunakan Kerangka Kerja *National Institute of Justice*," *J. Edukasi dan Penelit. Inform.*, vol. 7, no. 3, p. 322, 2021, doi: 10.26418/jp.v7i3.48805.

Copyright © Jurnal Nasional Komputasi dan Teknologi Informasi (JNKTI)

[18] A. Tofik, G. Z. Muflih, and T. Informatika, "Akuisisi Barang Bukti Digital pada Aplikasi *Discord*," *JATI (Jurnal Mhs. Tek. Inform.*, vol. 8, no. 6, pp. 12122–12128, 2024.
[19] Mega Rosita, "Analisis Komparatif Performa *FTK Imager* dan *Autopsy* dalam Forensik Digital pada *Flashdisk*," *Info Kripto*, vol. 17, no. 3, 2023, doi: 10.56706/ik.v17i3.83.
[20] N. Anggraini, S. U. Masruroh, and H. Tiaraningtias, "Analisa Forensik *Whatsapp Messanger* pada *Smartphone* Android," *J. Ilm. FIFO*, vol. 12, no. 1, p. 83, 2020, doi: 10.22441/fifo.2020.v12i1.008.
[21] F. Isnaeni *et al.*, "Analisis Forensik *Smarphone* Android pada Aplikasi *TikTok* Menggunakan Metode NIST," *JATI (Jurnal Mhs. Tek. Inform.*, vol. 9, no. 1, pp. 1404–1410, 2025.
[22] R. N. Dasmen, A. Rahman, A. Dwi, and M. Saputra, "Analisis Digital Forensik *Recovery* File yang Terhapus Menggunakan *Tools Autopsy* dengan Metode *National Institute of Justice*," *J. Ilm. Komputasi*, vol. 23, no. 2, pp. 213–218, 2024, doi: 10.32409/jikstik.23.2.3553.

Copyright © Jurnal Nasional Komputasi dan Teknologi Informasi (JNKTI)