

Komparasi FTK Imager dan Autopsy dalam Investigasi Cyberbullying Telegram Menggunakan Framework DFRWS

¹Arinaa Manaasika, ²Fahmi Fachri

^{1,2}Universitas Ma'arif Nahdlatul Ulama Kebumen, Indonesia

¹manaasikaa@gmail.com; ²fahmifachriumnu@gmail.com;

Article Info

Article history:

Received, 2026-04-30

Revised, 2026-06-02

Accepted, 2026-06-05

Kata Kunci:

digital_forensik
cyberbullying
FTK Imager
Autopsy
telegram
DFRWS

Keywords:

digital_forensics
cyberbullying
FTK Imager
Autopsy
telegram
DFRWS

ABSTRAK

Penelitian ini bertujuan untuk melakukan investigasi digital forensik pada kasus cyberbullying Telegram menggunakan *framework Digital Forensic Research Workshop (DFRWS)* dengan melakukan komparasi *tools* FTK Imager dan Autopsy. Tahapan penelitian meliputi *identification, preservation, collection, examination, analysis*, dan *presentation* untuk memperoleh bukti digital dari perangkat Android. Hasil investigasi menunjukkan bahwa FTK Imager berhasil memperoleh artefak berupa *chat, voice note*, dan *metadata file* dengan tingkat keberhasilan sebesar 100% pada artefak teks dan *metadata*, namun tidak berhasil menemukan file multimedia seperti foto dan video. Sementara itu, Autopsy berhasil memperoleh artefak berupa *chat, foto, video, metadata*, serta *recovery file* terhapus dengan tingkat keberhasilan mencapai 100% pada artefak multimedia dan *recovery file*. Secara keseluruhan, FTK Imager memperoleh tingkat *recovery* sebesar 58,3%, sedangkan Autopsy memperoleh tingkat *recovery* sebesar 83,3%. Validasi integritas bukti digital menggunakan algoritma hash MD5 dan SHA1 menunjukkan nilai identik sebelum dan sesudah proses investigasi sehingga integritas data tetap terjaga. Hasil penelitian menunjukkan bahwa penggunaan FTK Imager dan Autopsy secara bersamaan mampu memberikan hasil investigasi digital forensik yang lebih optimal, sistematis, dan komprehensif dalam menangani kasus cyberbullying Telegram.

ABSTRACT

This study aims to investigate cyberbullying cases on the Telegram application using the Digital Forensic Research Workshop (DFRWS) framework by comparing the performance of FTK Imager and Autopsy forensic tools. The investigation process consisted of identification, preservation, collection, examination, analysis, and presentation stages to obtain digital evidence from Android devices. The results showed that FTK Imager successfully recovered text chats, voice notes, and metadata with a 100% success rate for text-based artifacts, but failed to recover multimedia files such as photos and videos. Meanwhile, Autopsy successfully recovered chats, photos, videos, metadata, and deleted files with a 100% success rate for multimedia artifacts and deleted file recovery. Overall, FTK Imager achieved a digital evidence recovery rate of 58.3%, while Autopsy achieved 83.3%. Digital evidence integrity validation using MD5 and SHA1 hashing produced identical hash values before and after the investigation process, indicating that the integrity and authenticity of the evidence were successfully maintained. The findings demonstrate that the combined use of FTK Imager and Autopsy provides a more effective, systematic, and comprehensive digital forensic investigation process for handling cyberbullying cases on Telegram.

This is an open access article under the [CC BY-SA](https://creativecommons.org/licenses/by-nc-nd/4.0/) license.



Penulis Korespondensi:

Arinaa Manaasika,
Program Studi Teknik Informatika,
Universitas Ma'arif Nahdlatul 'Ulama Kebumen,
Email: manaasikaa@gmail.com

1. PENDAHULUAN

Perkembangan teknologi digital telah mendorong peningkatan penggunaan media sosial dan aplikasi pesan instan sebagai sarana utama komunikasi daring masyarakat modern [1]. Media sosial menjadi ruang interaksi

yang memungkinkan komunikasi antarindividu maupun kelompok tanpa dibatasi ruang dan waktu. Interaksi tersebut dapat terjadi karena hubungan pertemanan, keluarga, bisnis, maupun faktor sosial lainnya. Kehadiran media sosial memberikan berbagai dampak positif, seperti mempermudah penyebaran informasi dan memperluas jaringan komunikasi. Tetapi di sisi lain, media sosial juga sering disalahgunakan untuk tindakan negatif, salah satunya adalah *cyberbullying* [2]. *Cyberbullying* merupakan tindakan perundungan yang dilakukan secara sengaja melalui teknologi informasi dan komunikasi untuk menyakiti, mengintimidasi, menghina, atau merugikan orang lain secara berulang [3]. Tindakan tersebut dapat dilakukan oleh individu maupun kelompok melalui pesan teks, gambar, video, maupun media digital lainnya yang menyerang kondisi psikologis korban. Di tengah meningkatnya penggunaan media sosial, kasus *cyberbullying* menjadi salah satu permasalahan serius di era digital [2]. Dampak *cyberbullying* tidak hanya memengaruhi kondisi emosional korban, tetapi juga berdampak terhadap kesehatan fisik dan mental. Korban *cyberbullying* cenderung mengalami gangguan tidur, sakit kepala, rasa malu, kehilangan rasa percaya diri, hingga depresi dan kecemasan sosial [4].

Berdasarkan data dari *Cyberbullying Research Center*, tingkat perundungan siber mengalami peningkatan yang cukup signifikan dalam satu dekade terakhir. Pada tahun 2016, sekitar 16,5% siswa dilaporkan pernah menjadi korban *cyberbullying*, sedangkan pada tahun 2025 angka tersebut meningkat menjadi 32,7%. Dari tahun 2016 hingga 2025, rata-rata 23,3% siswa dilaporkan pernah mengalami *cyberbullying* [5]. Peningkatan penggunaan smartphone dan kemudahan akses internet turut memengaruhi tingginya aktivitas komunikasi digital masyarakat [6]. Salah satu aplikasi pesan instan yang banyak digunakan saat ini adalah Telegram [7]. Telegram merupakan aplikasi komunikasi berbasis cloud yang menyediakan fitur keamanan berupa enkripsi data untuk menjaga privasi pengguna [8]. Meskipun demikian, fitur komunikasi privat pada Telegram juga berpotensi dimanfaatkan sebagai media penyebaran *cyberbullying* melalui pesan pribadi maupun grup percakapan [1].

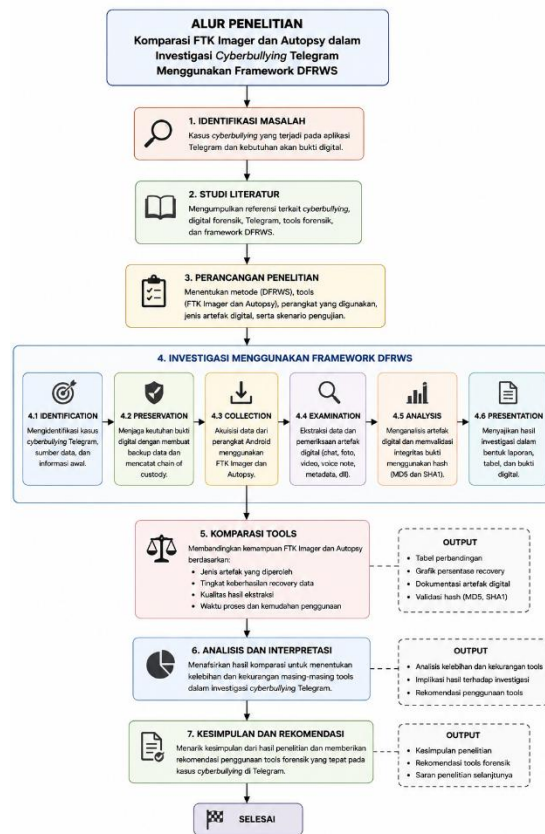
Penanganan kasus *cyberbullying* memerlukan proses investigasi digital forensik untuk memperoleh bukti digital yang valid dan dapat dipertanggungjawabkan. Investigasi digital forensik bertujuan untuk mengidentifikasi, mengumpulkan, menganalisis, dan mendokumentasikan bukti digital yang berkaitan dengan tindak kejahatan siber. Dalam penelitian sebelumnya, investigasi digital forensik pada aplikasi Telegram menggunakan FTK *Imager* menunjukkan bahwa *tools* tersebut hanya mampu memperoleh artefak berupa pesan percakapan, sedangkan file multimedia seperti foto, video, dan voice note tidak berhasil ditemukan [9]. Penelitian lain menunjukkan bahwa *tools Autopsy* mampu mengidentifikasi keberadaan file yang telah dihapus, namun proses pemulihan data belum dapat dilakukan secara optimal sehingga beberapa file tidak dapat dibuka kembali secara utuh [10]. Hasil penelitian tersebut menunjukkan bahwa setiap *tools* digital forensik memiliki kemampuan yang berbeda dalam memperoleh artefak digital tertentu.

Penelitian ini menggunakan *framework Digital Forensic Research Workshop* (DFRWS) karena memiliki tahapan investigasi yang sistematis dalam proses identifikasi, pengumpulan, pemeriksaan, analisis, dan pelaporan bukti digital [11]. *Framework* DFRWS juga menyediakan mekanisme dokumentasi yang terstruktur sehingga setiap proses investigasi dapat dicatat secara lengkap dan terorganisasi [12]. Selain itu, beberapa penelitian sebelumnya menunjukkan bahwa *framework* DFRWS efektif digunakan dalam investigasi digital forensik pada berbagai platform komunikasi digital seperti aplikasi IMO Messenger, Discord, dan Twitter [13], [14], [15]. Hal tersebut menunjukkan bahwa *framework* DFRWS memiliki kemampuan yang baik dalam mendukung proses investigasi digital forensik secara sistematis dan komprehensif.

Berdasarkan permasalahan tersebut, penelitian ini bertujuan untuk melakukan komparasi FTK *Imager* dan *Autopsy* dalam investigasi *cyberbullying* Telegram menggunakan *framework* DFRWS. Penelitian difokuskan pada kemampuan kedua *tools* dalam memperoleh artefak digital berupa pesan teks, foto, video, *voice note*, dan metadata dari perangkat Android. Selain itu, penelitian ini juga bertujuan untuk mengetahui efektivitas masing-masing *tools* dalam proses *recovery* data dan validasi integritas bukti digital. Dengan demikian, hasil penelitian diharapkan dapat memberikan kontribusi dalam pengembangan investigasi digital forensik, khususnya pada kasus *cyberbullying* di aplikasi Telegram menggunakan *framework* DFRWS.

2. METODE PENELITIAN

Gambar 1 menunjukkan alur penelitian investigasi digital forensik pada kasus *cyberbullying* Telegram menggunakan *framework Digital Forensic Research Workshop* (DFRWS). Penelitian dilakukan secara sistematis mulai dari identifikasi permasalahan hingga penarikan kesimpulan berdasarkan hasil investigasi digital. Dalam penelitian ini digunakan dua *tools* digital forensik, yaitu FTK *Imager* dan *Autopsy*, untuk memperoleh serta membandingkan artefak digital berupa pesan teks, foto, video, *voice note*, dan metadata dari perangkat Android. *Framework* DFRWS digunakan karena memiliki tahapan investigasi yang terstruktur dalam proses identifikasi, pengumpulan, pemeriksaan, analisis, hingga penyajian bukti digital sehingga integritas bukti dapat terjaga selama proses investigasi berlangsung.



Gambar 1 Alur Penelitian

Tahap identifikasi masalah dilakukan untuk menentukan fokus penelitian berdasarkan kasus *cyberbullying* yang terjadi pada aplikasi Telegram. Pada tahap ini peneliti mengidentifikasi bentuk *cyberbullying*, kebutuhan investigasi digital, serta pentingnya bukti digital dalam proses investigasi kejahatan siber. Tahap studi literatur dilakukan dengan mengumpulkan berbagai referensi yang berkaitan dengan *cyberbullying*, digital forensik, aplikasi Telegram, framework DFRWS, serta penelitian terdahulu yang menggunakan FTK *Imager* dan *Autopsy*. Studi literatur bertujuan untuk memperkuat dasar teori dan mengetahui perkembangan penelitian terkait investigasi digital forensik.

Pada tahap penyusunan rancangan penelitian meliputi penentuan metode investigasi, *tools* yang digunakan, perangkat Android sebagai objek penelitian, jenis artefak digital yang dianalisis, serta skenario pengujian *cyberbullying* Telegram. Tahap ini bertujuan agar penelitian berjalan secara sistematis dan terarah.

Tahap *identification* dilakukan dengan mengidentifikasi kasus *cyberbullying*, sumber data digital, akun Telegram yang terlibat, serta informasi awal yang berkaitan dengan aktivitas komunikasi digital pada perangkat Android. Tahap *preservation* bertujuan menjaga keutuhan dan integritas bukti digital agar tidak mengalami perubahan selama proses investigasi. Pada tahap ini dilakukan pencatatan *chain of custody*, pengamanan perangkat, dan proses *backup* data sebelum investigasi dilakukan. Tahap *collection* dilakukan dengan proses akuisisi data dari perangkat Android menggunakan FTK *Imager* dan *Autopsy*. Data yang dikumpulkan meliputi pesan teks, foto, video, *voice note*, database Telegram, serta metadeta yang berkaitan dengan aktivitas *cyberbullying*.

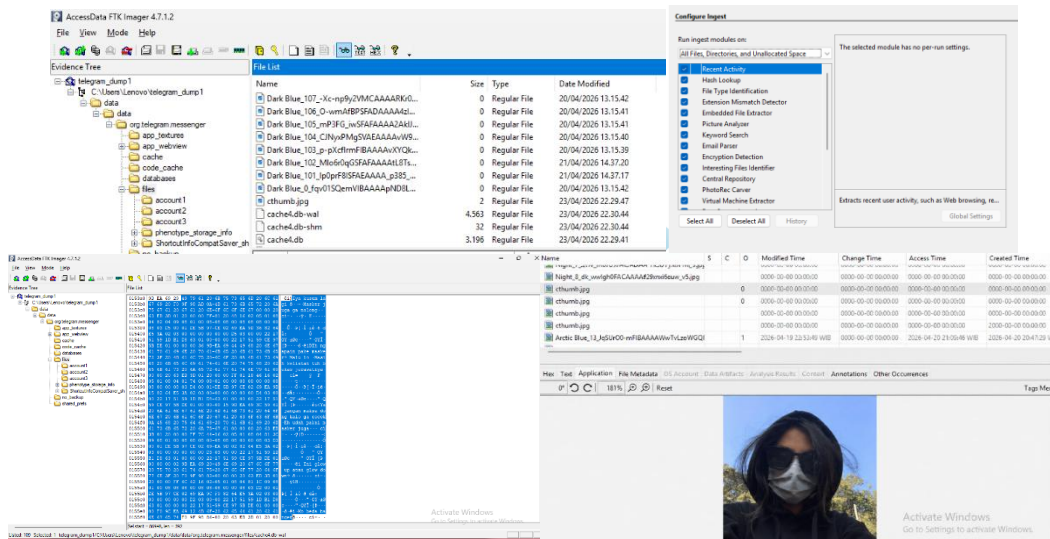
Tahap *examination* dilakukan dengan mengekstraksi dan memeriksa artefak digital hasil akuisisi. Proses pemeriksaan dilakukan untuk menemukan file, pesan, maupun media digital yang berkaitan dengan kasus *cyberbullying* Telegram. Tahap *analysis* dilakukan dengan menganalisis artefak digital yang berhasil ditemukan oleh masing-masing *tools*. Pada tahap ini juga dilakukan validasi integritas bukti digital menggunakan metode hashing MD5 dan SHA1 untuk memastikan bahwa data tidak mengalami perubahan selama proses investigasi berlangsung. Tahap *presentation* dilakukan dengan menyajikan hasil investigasi digital forensik dalam bentuk laporan, tabel, gambar, dan dokumentasi bukti digital. Tahap ini bertujuan mempermudah proses interpretasi hasil investigasi dan penyampaian informasi secara sistematis.

Tahap komparasi tools dilakukan untuk membandingkan kemampuan FTK *Imager* dan *Autopsy* dalam memperoleh artefak digital. Perbandingan dilakukan berdasarkan jenis artefak yang berhasil ditemukan, tingkat

keberhasilan *recovery* data, kualitas hasil ekstraksi, waktu proses investigasi, serta validitas bukti digital. Selanjutnya tahap analisis dilakukan interpretasi terhadap hasil komparasi kedua *tools*. Peneliti menganalisis kelebihan dan kekurangan FTK *Imager* dan *Autopsy* dalam proses investigasi *cyberbullying* Telegram sehingga dapat diketahui efektivitas masing-masing *tools* dalam memperoleh bukti digital. Tahap akhir penelitian dilakukan dengan menarik kesimpulan berdasarkan hasil investigasi dan komparasi *tools*. Selain itu, peneliti memberikan rekomendasi penggunaan *tools* digital forensik yang sesuai untuk investigasi *cyberbullying* pada aplikasi Telegram serta saran untuk penelitian selanjutnya.

3. HASIL DAN ANALISIS

Pada penelitian ini dilakukan investigasi digital forensik terhadap kasus *cyberbullying* pada aplikasi Telegram menggunakan *framework Digital Forensic Research Workshop (DFRWS)*. Proses investigasi dilakukan melalui tahapan *identification, preservation, collection, examination, analysis, dan presentation*. Investigasi memanfaatkan dua *tools* digital forensik, yaitu FTK *Imager* dan *Autopsy*, untuk memperoleh serta membandingkan artefak digital dari perangkat Android.



Gambar 2 Penggunaan *Tools FTK Imager* dan *Tools Autopsy*

Tahap *examination* dilakukan dengan proses akuisisi dan pemeriksaan data digital menggunakan FTK *Imager* dan *Autopsy*. Berdasarkan hasil pemeriksaan pada Gambar 2, kedua *tools* berhasil melakukan ekstraksi data dari perangkat yang diinvestigasi. FTK *Imager* digunakan untuk memperoleh struktur file, metadata, serta data hexadecimal dari aplikasi Telegram. Sementara itu, *Autopsy* digunakan untuk melakukan pemeriksaan artefak digital dan *recovery* file multimedia yang ditemukan pada perangkat. Hasil investigasi menunjukkan bahwa masing-masing *tools* memiliki kemampuan yang berbeda dalam memperoleh bukti digital. FTK *Imager* lebih optimal dalam menemukan artefak berupa pesan teks, *voice note*, dan metadata file, sedangkan *Autopsy* lebih optimal dalam menemukan file multimedia seperti foto dan video yang berkaitan dengan aktivitas *cyberbullying* Telegram.

Tabel 1. Hasil Perbandingan *Tools Digital Forensik*

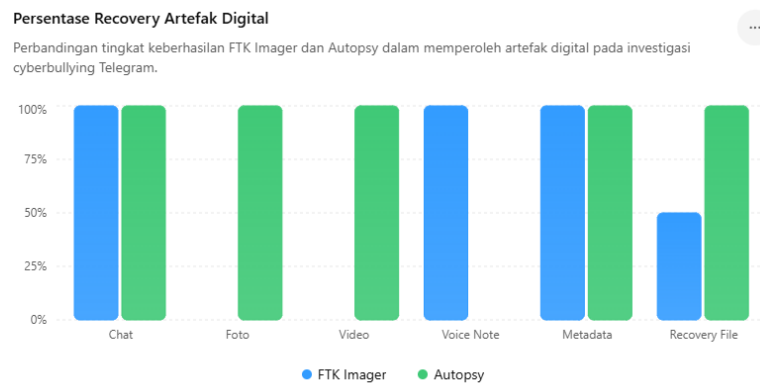
Bukti Digital	FTK Imager	Autopsy
Chat (Teks)	Ditemukan	Ditemukan
Foto	Tidak Ditemukan	Ditemukan
Video	Tidak Ditemukan	Ditemukan
Voice Note	Ditemukan	Tidak Ditemukan
Metadata File	Ditemukan	Ditemukan
Recovery File Terhapus	Terbatas	Ditemukan

Berdasarkan Tabel 1, FTK *Imager* berhasil memperoleh artefak berupa *chat, voice note*, dan metadata file, namun belum mampu melakukan *recovery* file multimedia secara optimal. Sebaliknya, *Autopsy* berhasil menemukan foto, video, metadata, serta file yang telah terhapus dari perangkat. Hasil tersebut menunjukkan bahwa kedua *tools* memiliki karakteristik investigasi yang berbeda sesuai dengan kemampuan ekstraksi masing-masing. Untuk memperjelas tingkat keberhasilan masing-masing *tools*, dilakukan perhitungan persentase *recovery* terhadap setiap artefak digital yang berhasil ditemukan.

Tabel 2. Persentase *Recovery* Artefak Digital

Jenis Artefak	FTK Imager	Autopsy
Chat (Teks)	100%	100%
Foto	0%	100%
Video	0%	100%
Voice Note	100%	0%
Metadata File	100%	100%
Recovery File Terhapus	50%	100%

Berdasarkan Tabel 2, FTK *Imager* memiliki tingkat keberhasilan tinggi dalam menemukan artefak berbasis teks dan metadata, sedangkan *Autopsy* memiliki tingkat keberhasilan lebih tinggi dalam melakukan *recovery* file multimedia dan file terhapus. Berdasarkan grafik dibawah ini dapat terlihat jelas *Autopsy* menunjukkan tingkat *recovery* yang lebih tinggi terhadap file multimedia seperti foto dan video. Sementara itu, FTK *Imager* lebih optimal dalam memperoleh artefak berupa pesan teks, *voice note*, dan struktur metadata file.



Gambar 3. Grafik Perbandingan *Recovery Tools*

Berdasarkan hasil pemeriksaan menggunakan FTK *Imager*, tools ini berhasil menampilkan struktur direktori, metadata file, serta data *hexadecimal* dari aplikasi Telegram. FTK *Imager* mampu memperoleh bukti digital berupa pesan teks dan *voice note* yang tersimpan pada direktori aplikasi. Selain itu, tools ini juga mampu menampilkan informasi metadata seperti ukuran file, waktu modifikasi, dan lokasi penyimpanan data. Keunggulan FTK *Imager* terletak pada kemampuannya dalam melakukan akuisisi data secara stabil dan menjaga integritas bukti digital selama proses investigasi berlangsung. FTK *Imager* juga efektif digunakan untuk analisis struktur file system dan data *hexadecimal* yang berkaitan dengan aktivitas komunikasi pengguna. Namun, pada penelitian ini FTK *Imager* memiliki keterbatasan dalam melakukan *recovery* file multimedia seperti foto dan video yang telah terhapus dari perangkat.

Berdasarkan hasil pemeriksaan menggunakan *Autopsy*, tools ini berhasil menemukan artefak digital berupa foto, video, dan file multimedia lain yang berkaitan dengan aktivitas *cyberbullying* Telegram. *Autopsy* juga mampu melakukan identifikasi dan *recovery* terhadap file yang sebelumnya telah dihapus dari perangkat. Keunggulan utama *Autopsy* terletak pada kemampuan *recovery* file dan analisis artefak multimedia secara lebih mendalam dibandingkan FTK *Imager*. Selain itu, *Autopsy* menyediakan fitur *indexing* dan *timeline analysis* yang membantu investigator dalam menelusuri aktivitas pengguna pada aplikasi Telegram. Namun demikian, pada penelitian ini *Autopsy* memiliki keterbatasan dalam memperoleh *voice note* dan beberapa data percakapan secara lengkap.

Perbedaan hasil *recovery* antara FTK *Imager* dan *Autopsy* dipengaruhi oleh metode ekstraksi dan kemampuan parsing artefak yang dimiliki masing-masing tools. FTK *Imager* lebih berfokus pada proses *imaging* dan pembacaan struktur file *system* secara langsung sehingga lebih optimal dalam memperoleh data teks, metadata, dan data *hexadecimal*. Sementara itu, *Autopsy* memiliki kemampuan *indexing* dan file *carving* yang lebih baik sehingga lebih efektif dalam melakukan *recovery* file multimedia seperti foto dan video. Selain itu, FTK *Imager* bekerja dengan pendekatan akuisisi forensik berbasis image file yang mempertahankan struktur asli data, sedangkan *Autopsy* menggunakan modul analisis otomatis untuk melakukan identifikasi artefak digital secara lebih mendalam. Perbedaan mekanisme tersebut menyebabkan masing-masing *tools* memiliki keunggulan dan keterbatasan yang berbeda dalam proses investigasi *cyberbullying* Telegram.

Untuk memastikan integritas bukti digital tetap terjaga selama proses investigasi, dilakukan validasi menggunakan algoritma hashing MD5 dan SHA1 terhadap hasil akuisisi data. Validasi dilakukan sebelum dan sesudah proses analisis untuk memastikan tidak terjadi perubahan data pada barang bukti digital.

Tabel 3. Validasi Integritas Bukti Digital

Jenis Validasi	Nilai Hash Sebelum Analisis	Nilai Hash Sesudah Analisis	Status
MD5	Identik	Identik	Valid
SHA1	Identik	Identik	Valid

Hasil validasi menunjukkan bahwa nilai hash MD5 dan SHA1 tetap identik sebelum dan sesudah proses investigasi dilakukan. Hal ini membuktikan bahwa proses investigasi menggunakan *framework* DFRWS berhasil menjaga keaslian dan integritas bukti digital sehingga data yang diperoleh dapat dipertanggungjawabkan secara forensik.

Berdasarkan hasil investigasi digital forensik menggunakan *framework* DFRWS, FTK Imager dan *Autopsy* berhasil memperoleh artefak digital yang berkaitan dengan kasus *cyberbullying* Telegram. FTK Imager unggul dalam analisis struktur file, metadata, pesan teks, dan *voice note*, sedangkan *Autopsy* lebih unggul dalam *recovery* file multimedia dan identifikasi file terhapus. Hasil penelitian menunjukkan bahwa penggunaan kedua *tools* secara bersamaan mampu memberikan hasil investigasi yang lebih optimal dibandingkan hanya menggunakan satu *tools* saja. Kombinasi FTK Imager dan *Autopsy* dapat membantu investigator memperoleh bukti digital secara lebih lengkap sehingga proses investigasi *cyberbullying* Telegram dapat dilakukan secara lebih efektif, sistematis, dan komprehensif.

4. KESIMPULAN

Penelitian ini berhasil menerapkan *framework Digital Forensic Research Workshop* (DFRWS) dalam investigasi kasus *cyberbullying* pada aplikasi Telegram menggunakan *tools* FTK Imager dan *Autopsy*. Proses investigasi dilakukan melalui tahapan *identification, preservation, collection, examination, analysis, dan presentation* untuk memperoleh bukti digital dari perangkat Android. Hasil penelitian menunjukkan bahwa FTK Imager mampu memperoleh artefak berupa *chat, voice note, dan metadata* dengan tingkat keberhasilan sebesar 100% pada artefak berbasis teks, namun tidak berhasil menemukan file multimedia berupa foto dan video. Sementara itu, *Autopsy* berhasil memperoleh artefak berupa *chat, foto, video, metadata, serta recovery file terhapus* dengan tingkat keberhasilan mencapai 100% pada artefak multimedia dan *recovery file*. Secara keseluruhan, FTK Imager memperoleh tingkat *recovery* bukti digital sebesar 58,3%, sedangkan *Autopsy* memperoleh tingkat *recovery* sebesar 83,3%. Validasi integritas data menggunakan algoritma hash MD5 dan SHA1 menunjukkan nilai hash yang identik sebelum dan sesudah proses investigasi, sehingga keaslian dan integritas bukti digital tetap terjaga. Berdasarkan hasil tersebut, penggunaan FTK Imager dan *Autopsy* secara bersamaan mampu memberikan proses investigasi digital forensik yang lebih optimal, sistematis, dan komprehensif dalam menangani kasus *cyberbullying* pada aplikasi Telegram.

REFERENSI

- [1] T. Filikano, A. Gunawan, dan A. Wijaya, “Deteksi Cyberbullying Dalam Grup Telegram Menggunakan Support Vector Machine (SVM),” *J. Sist. Informasi, Manaj. dan Teknol. Inf.*, vol. 2, no. 1, hal. 67–74, 2024, doi: 10.33020/jsimtek.v2i1.532.
- [2] S. Y. Sekarayu dan M. B. Santoso, “Remaja Sebagai Pelaku Cyberbullying Dalam Media Sosial,” *J. Penelit. dan Pengabd. Kpd. Masy.*, vol. 3, no. 1, hal. 1, 2022, doi: 10.24198/jppm.v3i1.39558.
- [3] I. O. Dewi, “Pengaturan Tindak Pidana Cyberbullying di Indonesia,” vol. 6, no. 2, hal. 4533–4539, 2023, doi: 10.31933/unesrev.v6i2.
- [4] N. D. Purba dan S. O. Turnip, “Dampak Negatif Cyberbullying dan Upaya Pencegahannya,” vol. 06, no. 01, hal. 17–33, 2024, doi: <https://doi.org/10.60146/kaluteros.v6i1.75>.
- [5] Cyberbullying Reach Senter, “Ringkasan Penelitian Kami tentang Perundungan Siber (2007-2025).” [Daring]. Tersedia pada: <https://cyberbullying.org/summary-of-our-cyberbullying-research>
- [6] L. Fazry dan N. C. Apsari, “Cdik,” vol. 2, no. 1, hal. 28–36, 2021, [Daring]. Tersedia pada: <http://journal.unpad.ac.id/jppm/article/view/33435/15459>
- [7] M. E. Sutrahity, S. S. Kuahaty, dan A. Balik, “Perlindungan Hukum Pemegang Hak Cipta terhadap Pelanggaran Melalui Aplikasi Telegram,” *J. Ilmu Huk.*, vol. 1, no. 5, hal. 346–355, 2021.
- [8] N. C. Dewi, T. Sutabri, dan F. Putrawansyah, “Analisis Penyadapan pada Telegram dengan Network Forensic,” vol. 7, no. 2, hal. 183–190, 2023, doi: 10.26798/jiko.v7i2.789.
- [9] D. M. Syafitri dan F. Fachri, “Analisis forensik digital telegram pada android untuk,” vol. 10, no. 1,

- hal. 41–50, 2025, doi: <https://doi.org/10.36341/rabit.v10i1.5402>.
- [10] A. Z. Ifani, A. M. Sumardi, N. Baytikhalishah, dan Nurlela., “Perbandingan Keamanan dan Performa Aplikasi WhatsApp dan Telegram dengan Menggunakan Metode NIJ,” *J. Cyber Heal. Comput.*, vol. 1, no. 1, hal. 1–5, 2023, doi: 10.64163/jochac.v1i1.1.
- [11] W. Y. Sulistyono, S. A. Pratiwi, M. Haedar, dan Z. Hidayatullah, “Analisis Forensik Citra di Platform X menggunakan Metode Digital Forensic Research Workshop (DFRWS),” vol. 8, hal. 10–20, 2025, doi: 10.36080/idealisis.v8i1.3293.
- [12] A. Yudhana, I. Riadi, dan R. Y. Prasongko, “Forensik WhatsApp Menggunakan Metode Digital Forensic Research Workshop (DFRWS),” *J. Inform. J. Pengemb. IT*, vol. 7, no. 1, hal. 43–48, 2022, doi: 10.30591/jpit.v7i1.3639.
- [13] I. Riadi, Sunardi, dan Y. Safitri, “Analisis Forensik Cyberbullying pada Aplikasi IMO Messenger Menggunakan Metode Association of Chief Police Office,” *J. Bumigora Inf. Technol.*, vol. 5, no. 1, hal. 1–8, 2023, doi: 10.30812/bite/v5i1.2977.
- [14] M. Wibowo, M. R. Firmansyah, dan R. S. Efendi, “Analisis Bukti Digital pada Aplikasi DISCORD dengan Menggunakan Framework DFRWS,” vol. 15, no. 1, hal. 98–111, 2024, doi: 10.51903/jtikp.v15i1.826.
- [15] I. Zuhriyanto, Anton Yudhana, dan Imam Riadi, “Comparative analysis of Forensic Tools on Twitter applications using the DFRWS method,” *J. RESTI (Rekayasa Sist. dan Teknol. Informasi)*, vol. 4, no. 5, hal. 829–836, 2020, doi: 10.29207/resti.v4i5.2152.