

# Analisis Barang Bukti Pada Aplikasi Whatsapp Menggunakan FTK Imager di Kelas Teknik Komputer Universitas Bina Darma

Rahmat Novrianda Dasmen<sup>1)</sup>, Muhammad Fikri<sup>2)</sup>, Rasmila<sup>3)</sup>, Habib Elfariz Tritama<sup>4)</sup>,  
M. Rizky Aulia<sup>5)</sup>, KMS M. Okta Agung Saputra<sup>6)</sup>

<sup>a</sup> Fakultas Vokasi, Program Universitas Bina Darma, Indonesia, Indonesia

<sup>1</sup>[rahmatnovrianda@binadarma.ac.id](mailto:rahmatnovrianda@binadarma.ac.id)

<sup>2</sup>[muhammadfikri040701@gmail.com](mailto:muhammadfikri040701@gmail.com)

<sup>3</sup>[rasmila@binadarma.ac.id](mailto:rasmila@binadarma.ac.id)

<sup>4</sup>[habibelfariz@gmail.com](mailto:habibelfariz@gmail.com)

<sup>5</sup>[rizkyaulia0319@gmail.com](mailto:rizkyaulia0319@gmail.com)

<sup>6</sup>[kmsmoas03@gmail.com](mailto:kmsmoas03@gmail.com)

## Abstract

*Technological advances have both positive and negative impacts, including facilitating communication and increasing the risk of cyberbullying, especially among children and adolescents. This study analyzes the impact of the WhatsApp application on cyberbullying in Indonesia using digital forensic methods. The researchers developed scenarios to identify cyberbullying perpetrators in WhatsApp chat groups, utilizing forensic tools such as FlashDisk and FTK Imager. The analysis process involves collecting, examining, and analyzing cyberbullying-related images, focusing on the size, file name, and width of the image. Forensic data is collected and analyzed through three stages: collection, processing, and storage. The findings show the existence of two images associated with cyberbullying activity, in accordance with the NIST methodology. This study suggests that other forensic methods be explored in further research.*

**Keywords:** FTK Imager, Forensic, Cyberbullying, Whatsapp, NIST

## 1. Pendahuluan

Perkembangan dan perluasan teknologi informasi dan komunikasi yang sangat pesat saat ini telah memberikan berbagai dampak positif dan negatif. Salah satu dampak positif dari kemajuan teknologi informasi dan komunikasi adalah semakin mudahnya orang mendapatkan dan menggunakan informasi, serta berkomunikasi dengan orang-orang di seluruh dunia. [1]. Namun, teknologi informasi ini dapat membawa kerugian dalam bentuk hasil yang tidak diinginkan, salah satunya adalah berkembangnya cyberbullying antara anak-anak dan orang dewasa. Cyberbullying adalah jenis bullying baru yang mirip dengan bullying di dunia nyata dalam hal karakteristik dan efeknya. Cyberbullying didefinisikan sebagai perilaku rekayasa relasional yang merusak yang ditujukan kepada orang atau kelompok melalui penggunaan teknologi informasi dan komunikasi [2]. Penindasan siber dapat terjadi melalui perantara seperti pesan yang berisi komentar yang tidak menyenangkan, yang dapat meningkat menjadi perilaku penindasan. [3]. Cyberbullying memiliki bentuk diantaranya flaming (pesan dengan amarah), harassment (gangguan), denigration (pencemaran nama baik), impersonation (peniruan), outing (penyebaran), trickery (tipu daya), exclusion (pengucilan) dan cyberstalking (penguntitan) [4].

WhatsApp sebagai salah satu platform komunikasi yang paling banyak digunakan di Indonesia, sering kali menjadi alat dalam kasus cyberbullying [5]. Bukti-bukti seperti pesan, gambar, dan video yang dikirim melalui aplikasi ini dapat membantu mengidentifikasi pelaku. Oleh karena itu, penggunaan teknik forensik digital untuk menganalisis data dari aplikasi WhatsApp sangat penting dalam proses investigasi [6]. Forensik digital adalah proses investigasi kejahatan yang berfokus pada objek atau bukti yang diperoleh melalui sistem komputer. Dalam proses penyidikan, berbagai alat digunakan, khususnya dalam investigasi digital. Perangkat lunak digunakan untuk pemulihan data (recovery) guna menemukan barang bukti digital yang dapat mendukung penyelidikan, serta sebagai alat bukti yang akan membantu proses persidangan dalam kasus pidana [7]. Salah satu tantangan dalam menghadapi kejahatan di dunia digital adalah sulitnya mendeteksi secara fisik, sehingga diperlukan analisis digital untuk mengidentifikasinya. Bukti-bukti yang ditinggalkan oleh pelaku terus berkembang menuju bentuk kejahatan asimetris, di mana penjahat siber mampu melakukan kejahatan dengan menggunakan taktik

yang semakin canggih [8]. Hasil dari kejahatan digital umumnya disembunyikan dalam media penyimpanan agar dapat digunakan di kemudian hari. Namun, untuk menutupi dan menghilangkan jejak, pelaku kejahatan siber cenderung menghapus, menyembunyikan, atau memformat seluruh data yang mereka kumpulkan selama melakukan kejahatan [9].

Studi ini berfokus pada penggunaan alat forensik digital seperti FTK Imager untuk mengumpulkan dan menganalisis bukti digital terkait cyberbullying. FTK Imager memungkinkan para peneliti untuk mengambil dan memproses data digital, sehingga bukti yang ditemukan dapat digunakan dalam proses hukum. Penelitian ini bertujuan untuk memperjelas peran forensik digital dalam mengatasi cyberbullying, terutama di platform komunikasi yang digunakan secara luas seperti WhatsApp [10]. Sebuah penelitian yang berjudul Analisis Bukti pada Aplikasi Whatsapp Menggunakan FTK Imager di Kelas Teknik Komputer Universitas Bina Darma dilakukan berdasarkan Penggunaan metode NIST bertujuan untuk membantu dan mempermudah penyidik dalam memahami alur investigasi secara sistematis dan terstruktur. Metode ini dapat berfungsi sebagai panduan yang efektif dalam menyelesaikan berbagai permasalahan yang dihadapi selama proses investigasi [11].

## 2. Metode Penelitian

Pada penelitian ini peneliti membuat sebuah skenario fiktif sendiri yaitu berdasarkan kasus cyberbullying yang sering terjadi melalui aplikasi whatsapp. Dimana si pelaku mulai melakukan mengirimkan gambar dan pesan yang merendahkan korban melalui aplikasi whatsapp, pesan-pesan tersebut termasuk ejekan terhadap penampilan fisik. Pada penelitian ini korban akan melakukan pelaporan terhadap pelaku yang melakukan cyberbullying kepada diri di grup tersebut. Bukti tangkapan layar isi percakapan di grup yang nantinya akan dijadikan sebuah barang bukti. Barang bukti itu disimpan ke dalam sebuah flashdisk, kemudian pelaku mengambil flashdisk tersebut dan menghapus bukti digital tangkapan yang diambil korban. Untuk mengembalikan bukti tersebut menggunakan bantuan tools forensic yaitu FTK Imager. Untuk proses pengembalian bukti digital tersebut perlu adanya sebuah sistem. Peneliti mengacu menggunakan metode NIST untuk mengembalikan tangkapan layar di whatsapp yang tersimpan flashdisk korban. Metode berikut menjelaskan bagaimana alur tahapan metode menggunakan NIST sehingga dapat dilakukan suatu langkah penelitian secara terperinci sehingga dapat digunakan untuk panduan dalam menyelesaikan suatu persoalan yang ada [12]. Pada metode ini terdapat langkah-langkah forensik yang digunakan dan dapat dilihat pada gambar 1.

Penjelasan pada gambar alur metode National Institute of Standards and Technology (NIST), yaitu Collection, Examination, Analysis, dan Reporting sebagai berikut.



**Gambar 1.** Alur Metode Menggunakan NIST

### a. Collection

Pada tahap ini, bukti digital berupa tangkapan layar obrolan grup WhatsApp yang disimpan di flashdisk korban diidentifikasi dan diamankan. FTK Imager digunakan untuk melakukan akuisisi data digital tanpa mengubah integritas asli dari bukti tersebut. FTK Imager memungkinkan peneliti untuk melakukan imaging, yaitu membuat salinan bit-per-bit dari flashdisk untuk memastikan bahwa bukti asli tetap utuh dan tidak berubah selama proses analisis.

### b. Examination

Setelah koleksi bukti selesai, tahap pemeriksaan dilakukan dengan tujuan mengekstraksi data dari disk image yang telah dibuat. FTK Imager memungkinkan peneliti untuk menelusuri isi dari image tanpa mengubah file asli. Di sini, integritas data tetap dijaga, dan seluruh proses dapat dilakukan dengan hati-hati untuk menghindari kerusakan atau perubahan pada bukti digital.

### c. Analysis

Setelah data diperiksa dan bukti yang relevan ditemukan, tahap analisis dilakukan untuk mengevaluasi dan menginterpretasikan data guna menjawab pertanyaan hukum atau investigatif. FTK Imager

memungkinkan peneliti untuk meninjau kembali file gambar yang terlibat dalam kasus cyberbullying. Pada tahap ini, gambar yang diambil sebagai tangkapan layar dari grup WhatsApp dianalisis untuk mengidentifikasi apakah gambar tersebut terkait dengan tindakan bullying. FTK Imager menyediakan fitur untuk menyusun timeline (linimasa) dari aktivitas file. Ini membantu dalam mengidentifikasi kapan gambar tersebut dikirimkan, dihapus, atau diubah. Penggunaan fitur pencarian kata kunci pada FTK Imager memungkinkan peneliti mencari pesan atau gambar yang mengandung kata-kata ejekan atau penghinaan terhadap korban.

#### d. Reporting

Setelah analisis selesai, peneliti melaporkan hasil temuan dengan mendokumentasikan seluruh langkah yang diambil, alat yang digunakan, serta bukti yang ditemukan. FTK Imager dapat menghasilkan laporan forensik otomatis yang merinci proses pengumpulan bukti, gambar yang dipulihkan, dan hasil analisis lainnya. Laporan ini termasuk hash value untuk setiap file dan salinan gambar untuk membuktikan bahwa data tersebut valid dan tidak berubah. Laporan mencakup semua temuan yang dihasilkan dari analisis gambar dan pesan yang terkait dengan tindakan cyberbullying. Hal ini penting dalam proses hukum untuk menguatkan bukti di pengadilan.

Dengan penggunaan FTK Imager yang tepat, penelitian ini dapat memberikan hasil yang valid dan andal dalam mengembalikan serta menganalisis bukti digital terkait cyberbullying di WhatsApp, memperkuat langkah-langkah forensik yang diterapkan.

### 3. Hasil

Investigasi tersebut menghasilkan data forensik yang dijadikan sumber pemikiran dalam proses hukum. Proses pengumpulan barang bukti digital dilakukan melalui perangkat Flash Disk dan menggunakan alat forensik FTK Imager. Di bawah ini adalah hasil yang diperoleh. Berikut Tabel 1 nama barang, spesifikasi, dan bahan yang akan digunakan dalam penelitian ini.

No	Nama Item	Spesifikasi
	Komputer	HP 14s-fq0562AU - Silver
	SanDisk	32gb
	WhatsApp	Aplikasi Android
	FTK Imager	Alat Forensik

#### 3.1 Collection

Pada tahap collection menggunakan hardware SanDisk. SanDisk yang digunakan dalam penelitian ini berkapasitas 32 GB untuk menampung 3 foto bukti cyberbullying.

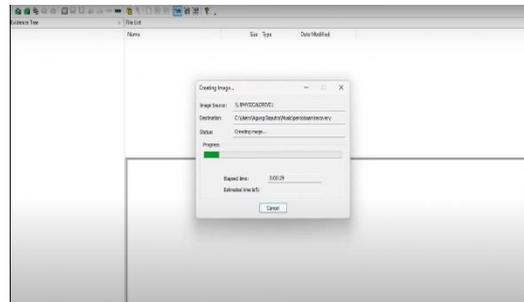


**Gambar 2.** SanDisk yang digunakan

Pada gambar 2. menunjukkan SanDisk yang akan digunakan dalam penelitian ini. Pada tahapan Collection ini tempat terjadinya penghapusan dan juga tempat pengembalian foto barang bukti cyberbullying, dan berlanjut ke tahap peninjauan.

### 3.2 Examination

Tahap pengujian meliputi pemeriksaan perangkat keras komputer menggunakan alat forensik yang disediakan. Tahap otopsi membuat gambar dan dilakukan pada sistem menggunakan alat forensik. Dalam penelitian ini digunakan alat forensik FTK Imager. Gambar 3. menunjukkan proses pemeriksaan menggunakan alat forensik FTK Imager.

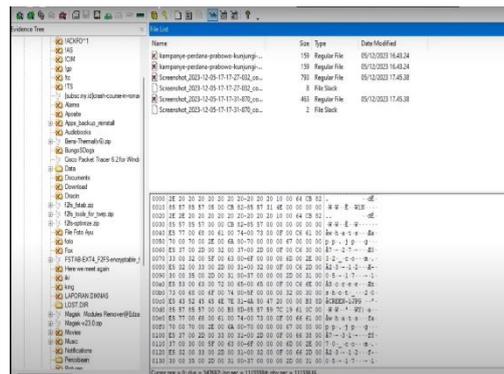


**Gambar 3.** Examination tools forensic

Kemudian, setelah proses pencitraan selesai, menghasilkan file atau laporan lengkap sebagai folder yang di dalam nya ada jpg barang bukti cyberbullying.

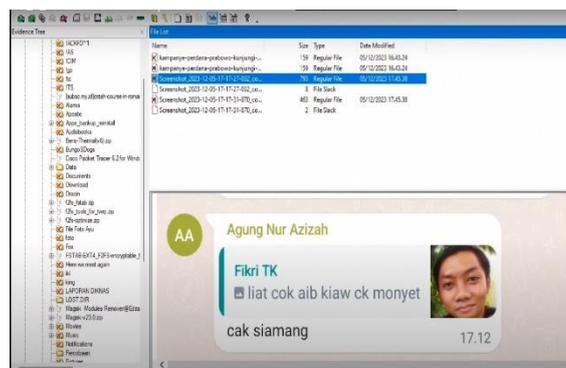
### 3.3 Analysis

Selama analisis berikut, beberapa bukti akan ditemukan dari alat forensik FTK Imager. Ini adalah bukti apa pun yang ditemukan menggunakan alat forensik yang digunakan.



**Gambar 4.** Hasil Image Tools Forensik

Gambar 4. Hasil pencarian yang dilakukan alat FTK Imager menghasilkan data gambar sebanyak 2 gambar yang masing-masing memiliki ukuran, nama file dan lebar yang berbeda.



Gambar 5. Hasil barang bukti

Gambar 5. hasil dari berhasil nya pengembalian barang bukti image cyberbullying dengan menggunakan tools forensic FTK Imager.

Gambar yang terdapat berupa ejekan verbal yang lebih ringan atau gambar yang sifatnya mengejek secara visual, seperti meme atau foto yang diedit untuk mempermalukan korban.

Gambar ini secara langsung terkait dengan perilaku cyberbullying. Dalam konteks ini, gambar pertama mungkin menampilkan *denigration* (pencemaran nama baik) yang mengandung ejekan terkait penampilan fisik korban. Sementara gambar kedua bisa berhubungan dengan *outing* atau *trickery*, di mana informasi pribadi korban disebarluaskan atau diungkapkan tanpa izin di dalam grup, yang bertujuan mempermalukan korban di hadapan orang lain.

### 3.4 Reporting

Langkah pelaporan ini menjelaskan langkah-langkah hasil analisis yang dilakukan pada tahap analisis, serta hasil alat investigasi yang dapat dikelompokkan ke dalam tabel sebagai berikut.

Tabel 2. Hasil FTK Imager

NO	Parameter yang dicari	Tools Forensic
	Image	Yes

Saat ini, skrip pembuatan gambar SanDisk dilakukan menggunakan alat forensik FTK Imager dan gambar dapat ditampilkan menggunakan alat forensik tersebut. Dengan menggunakan FTK Imager, peneliti berhasil memulihkan kedua gambar ini meskipun telah dihapus oleh pelaku. Proses pemulihan dilakukan dengan teknik data carving, di mana FTK Imager mengekstrak data yang masih tersisa di flashdisk meskipun file tersebut sudah tidak terlihat dalam file sistem. Setelah gambar ditemukan, FTK Imager memastikan integritas data melalui verifikasi hash value, memastikan bahwa gambar yang dipulihkan merupakan salinan yang valid dan tidak terubah dari file aslinya.

## 4. Kesimpulan

Berdasarkan hasil penelitian ini dapat disimpulkan menggunakan data forensik untuk mengembalikan gambar bukti tangkapan layar cyberbullying di grup chat yang tersimpan di flashdisk menggunakan alat forensik FTK Imager. Data dikumpulkan dan diolah melalui tiga tahap yaitu Pengumpulan, Pemeriksaan, dan Pelaporan. Penyimpanan menggunakan SanDisk 32GB untuk menyimpan tangkapan layer gambar cyberbullying. Pemeriksaan menggunakan perangkat keras laptop dengan alat FTK Imager untuk membuat mengembalikan data. Pelaporan menggunakan SanDisk untuk membuat gambar dengan ukuran, nama file, dan lebar berbeda. Proses analisis meliputi pembuatan gambar menggunakan alat FTK Imager dan menganalisis gambar. Laporan ini merangkum temuan analisis dan alat forensik yang digunakan. Hasil yang didapatkan di dalam penggunaan tools forensic FTK Imager terdapat 2 image barang bukti cyberbullying dengan menggunakan metode National

Institute Of Standards Technology (NIST). Saran untuk penelitian lebih lanjut dapat membandingkan metode yang digunakan dan menggunakan alat forensic lainnya.

## Referensi

- [1] YUDHANA, A., RIADI, I., ZUHRIYANTO, I., & DAHLAN, A. (2019). Analisis Live Forensics Aplikasi Media Sosial Pada Browser Menggunakan Metode Digital Forensics Research Workshop (DFRWS). 20(2), 125–130. <http://jurnalnasional.ump.ac.id/index.php/Techno>
- [2] BARUS, R. K. I. (2019). Korban Cyberbullying, Siapakah? JURNAL SIMBOLIKA: Research and Learning in Communication Study, 5(1), 35. <https://doi.org/10.31289/simbollika.v5i1.2301>
- [3] WIDIANDANA, P., IMAM RIADI, & SUNARDI. (2020). Implementasi Metode Jaccard pada Analisis Investigasi Cyberbullying WhatsApp Messenger Menggunakan Kerangka Kerja National Institute of Standards and Technology. Jurnal RESTI (Rekayasa Sistem Dan Teknologi Informasi), 4(6), 1046–1051.
- [4] SYAH, R., & HERMAWATI, I. (2018). The Prevention Efforts on Cyberbullying Case for Indonesian Adolescent Social Media Users. Jurnal PKS, 17(2), 131–146. <https://doi.org/10.31105/jpks.v17i2>
- [5] HARIANI. (2017). Analisis Bukti Digital Cyberbullying Pada Jejaring Sosial Menggunakan Naive Bayes Classifier (NBC). In Yogyakarta, Maret, 2017. Universitas Islam Indonesia.
- [6] Majalista, R., & Sutabri, T. (2023). ANALISIS PENCAIRAN DATA SMARTPHONE MENGGUNAKAN NIST UNTUK PENYELIDIKAN DIGITAL FORENSIK. Jurnal Informatika Teknologi dan Sains (Jinteks), 5(1), 81-85.
- [7] Julianto, M., & Servanda, Y. (2024). Kajian Literatur: Analisis Perbandingan Efektivitas Tools Forensik Recovery Data Pada Smartphone Android. *Jurnal Sains Dan Teknologi (JSIT)*, 4(2), 181–188. <https://doi.org/10.47233/jsit.v4i2.1830>
- [8] Analisis Bukti Digital Forensik pada Aplikasi Threads Menggunakan Metode Digital Forensic Research Workshop. (2024). *Jurnal Informatika Komputer, Bisnis Dan Manajemen*, 22(2), 1-10. <https://doi.org/10.61805/fahma.v22i2.118>
- [9] Matondang, J., Maulana, I., & Carudin, C. (2023). Analisis Perbandingan Perangkat Lunak Forensik Digital File Carving Menggunakan NIST. *Innovative: Journal Of Social Science Research*, 3(4), 2154–2165. Retrieved from <https://j-innovative.org/index.php/Innovative/article/view/3708>
- [10] Sidik, M. (2023). ANALISIS INTEGRITAS BUKTI DATA DIGITAL EVIDENCE PADA HASIL PROSES AKUISISI DATA PORTABLE STORAGE MENGGUNAKAN METODE NATIONAL INSTITUTE OF JUSTICE (NIJ) (Doctoral dissertation, Universitas Siliwangi).
- [11] Agustiono, W., Suci, D., & Prastiti, N. (2024). Analisis Forensik Digital Menggunakan Metode NIST untuk Memulihkan Barang Bukti yang Dihapus. *Jurnal Teknologi Dan Informasi*, 14(2), 174-185. <https://doi.org/10.34010/jati.v14i2.12952>
- [12] Bintang, R. A., Umar, R., & Yudhana, A. (2020). Analisis Media Sosial Facebook Lite dengan tools Forensik menggunakan Metode NIST. *Techno (Jurnal Fakultas Teknik, Universitas Muhammadiyah Purwokerto)*, 21(2), 125. <https://doi.org/10.30595/techno.v21i2.8494>