INSECT: Jurnal Teknik Informatika
INFORMATICS AND SECURITY e-ISSN. 2614-431X

Forensik *Digital Cyberbullying* pada Grup WhatsApp Menggunakan *National Institute of Standards and Technology*

Panggah Widiandana*[1], Sunardi[2], Imam Riadi[3]
[1]Program Studi Informatika, Universitas Islam Mulia Yogyakarta, Yogyakarta
[1]Program Studi Informatika, Universitas Ahmad Dahlan, Yogyakarta
[2]Program Studi Teknik Elektro, Universitas Ahmad Dahlan, Yogyakarta
[3]Program Studi Sistem Informasi, Universitas Ahmad Dahlan, Yogyakarta

E-mail: ***[1]panggah.widiandana@uim-yogya.ac.id**, [1]2537083006@webmail.uad.ac.id,
[2]sunardi@mti.uad.ac.id, [3]imam.riadi@is.uad.ac.id

Abstrak

Cyberbullying pada platform pesan instan seperti WhatsApp menjadi permasalahan serius karena dampaknya terhadap psikologis korban dan sulitnya pembuktian digital yang valid. Penelitian ini bertujuan untuk menganalisis dan mengungkap bukti digital cyberbullying pada grup WhatsApp menggunakan metode forensik digital berbasis kerangka kerja National Institute of Standards and Technology (NIST) yang meliputi tahapan collection, examination, analysis, dan reporting. Objek penelitian berupa data simulasi percakapan WhatsApp yang diperoleh melalui proses logical acquisition pada perangkat Android. Akuisisi dan analisis dilakukan menggunakan alat forensik digital Autopsy, SQLite Viewer, dan Cellebrite UFED. Tahapan penelitian dilakukan dengan melakukan simulasi kasus cyberbullying yang kemudian hasil simulasi tersebut diakuisisi menggunakan tahapan NIST. Data yang diteliti dalam grup terdapat 243 pesan. Hasil penelitian menunjukkan bahwa metode NIST mampu mengidentifikasi artefak digital penting berupa basis data percakapan dan metadata pengguna, serta mengungkap 77 pesan yang mengandung unsur cyberbullying, yang terdiri atas 39 penghinaan verbal, 25 ejekan, dan 14 komentar merendahkan. Verifikasi integritas data dilakukan menggunakan nilai hash SHA-256 yang menunjukkan konsistensi sebelum dan sesudah proses ekstraksi, sehingga memenuhi prinsip forensic soundness. Temuan ini membuktikan bahwa penerapan metode forensik digital berbasis NIST efektif dalam mendukung investigasi cyberbullying pada grup WhatsApp dan relevan digunakan dalam konteks akademik, hukum, dan keamanan siber.

Kata kunci : *Forensik Digital; Cyberbullying; WhatsApp; NIST; Logical Acquisition*

1. PENDAHULUAN

Penggunaan media sosial dan aplikasi pesan instan telah menjadi bagian yang tidak terpisahkan dari kehidupan anak dan remaja. Intensitas penggunaan yang tinggi memberikan kemudahan dalam berkomunikasi, namun juga meningkatkan potensi risiko psikososial [1]. *Cyberbullying* pada peserta didik tingkat sekolah dasar dan menengah menjadi fenomena yang meluas dan berulang, dengan dampak negatif terhadap kesejahteraan emosional korban[2]. Sejumlah penelitian menunjukkan bahwa paparan *cyberbullying* dapat menyebabkan gangguan psikologis jangka panjang, sehingga upaya pencegahan dan penanganannya perlu dilakukan secara sistematis dan berbasis bukti ilmiah [3]. Salah satu *platform* yang sering digunakan sebagai media terjadinya *cyberbullying* adalah WhatsApp, terutama karena karakteristik komunikasinya yang cepat, tertutup, dan berbasis grup [4].

WhatsApp memungkinkan terjadinya interaksi intensif antaranggota grup, yang pada kondisi tertentu dapat memicu tindakan perundungan verbal, pelecehan, dan intimidasi berulang terhadap individu tertentu [5]. WhatsApp Web dan WhatsApp Desktop memiliki karakteristik artefak digital yang kompleks, sehingga memerlukan pendekatan forensik yang tepat dalam proses investigasi [6].

Pada konteks hukum dan keamanan siber, tindakan *cyberbullying* memerlukan pembuktian yang kuat melalui bukti digital yang valid dan dapat dipertanggungjawabkan secara forensik [7]. Forensik digital berperan penting dalam proses pengumpulan, pemeriksaan, analisis, dan pelaporan bukti elektronik yang berkaitan dengan suatu insiden digital [8].

Indonesia memiliki urgensi pembuktian digital dalam kasus perundungan siber berkaitan erat dengan Undang-Undang Informasi dan Transaksi Elektronik (UU ITE), khususnya Pasal 27 ayat (3) mengenai penghinaan dan pencemaran nama baik, serta Pasal 45 ayat (3) yang mengatur sanksi pidananya. Bukti digital bersifat *volatile* (mudah berubah), penerapan standar forensik yang baku menjadi syarat mutlak agar bukti tersebut memiliki nilai pembuktian yang sah di depan hukum sesuai dengan Pasal 5 UU ITE.

Kerangka kerja yang banyak digunakan dalam investigasi forensik digital adalah metode *National Institute of Standards and Technology* (NIST), karena menyediakan tahapan investigasi yang sistematis dan menjaga prinsip *forensic soundness* [9]. Metode ini telah diterapkan dalam berbagai kasus forensik digital, termasuk analisis WhatsApp Web secara *live forensics* [10].

Penelitian sebelumnya juga menunjukkan bahwa artefak WhatsApp dapat dianalisis untuk mengidentifikasi pola komunikasi dan bentuk *cyberbullying* yang terjadi dalam grup media sosial [11]. Tantangan utama dalam investigasi WhatsApp adalah mekanisme enkripsi *end-to-end* yang membatasi akses langsung terhadap data, sehingga diperlukan metode akuisisi yang tepat [12].

Beberapa pendekatan forensik alternatif telah dikembangkan, seperti *framework* D4I dan metode DFRWS, namun metode NIST masih menjadi rujukan utama karena fleksibilitas dan keterstrukturannya [13]. Perkembangan pendekatan otomatis berbasis deep learning menunjukkan potensi besar dalam mendeteksi *cyberbullying*[14][15], namun masih memerlukan validasi forensik untuk kepentingan hukum [16].

Berdasarkan uraian tersebut, penelitian ini difokuskan pada penerapan metode NIST dalam menganalisis *cyberbullying* pada grup WhatsApp menggunakan data simulasi. Penelitian ini diharapkan dapat memberikan kontribusi metodologis dalam pengembangan investigasi forensik digital yang terstandarisasi, baik untuk kepentingan akademik maupun praktik penegakan hukum [17].

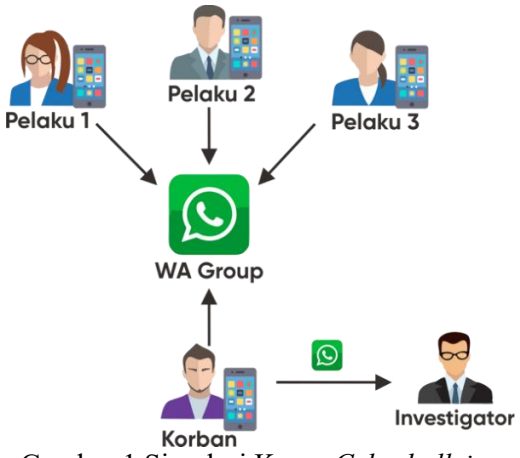
2. METODE PENELITIAN

2.1 Pendekatan Penelitian

Penelitian ini menggunakan pendekatan eksperimental-deskriptif dengan mengacu pada metode NIST sebagai kerangka kerja utama dalam investigasi forensik digital [18]. Pendekatan ini dipilih karena mampu memberikan alur kerja yang sistematis mulai dari pengumpulan hingga pelaporan bukti digital secara terstruktur.

2.2 Objek dan Data Penelitian

Objek penelitian berupa data percakapan grup WhatsApp yang bersifat data simulasi, yang dirancang untuk merepresentasikan skenario *cyberbullying* secara terkontrol. Data simulasi ini disimpan pada basis data WhatsApp dan berisi pesan teks, metadata waktu, dan identitas pengguna yang telah dianonimkan [19]. Simulasi kasus *cyberbullying* dapat dilihat pada Gambar 1.

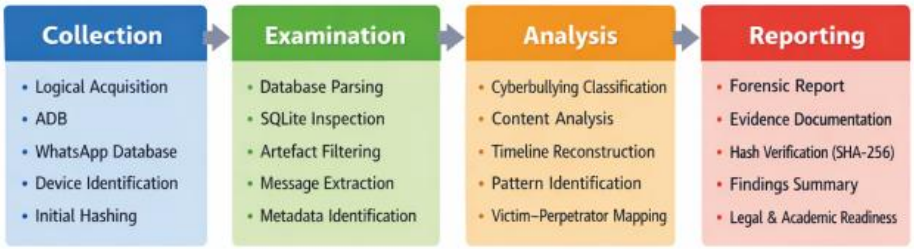


Gambar 1 Simulasi Kasus *Cyberbullying*

Gambar 1 menjelaskan simulasi dalam sebuah grup terdapat 4 orang yang menyerang salah satu anggotanya, kemudian korban melaporkan kepada *investigator* dan data diolah oleh *investigator*.

2.3 Tahapan Penelitian Berdasarkan Metode NIST

Metode NIST terdiri atas empat tahapan utama, yaitu *collection, examination, analysis*, dan *reporting*, yang diterapkan secara berurutan dalam penelitian ini. Tahapan NIST dapat dilihat pada Gambar 2.



Gambar 2 Tahapan NIST

Gambar 2 menggambarkan tahapan metode NIST yang digunakan dalam penelitian ini, yang meliputi *collection, examination, analysis,* dan *reporting*. Setiap tahapan memiliki aktivitas kunci yang saling berkaitan sebagai berikut:

a. *Collection* dilakukan melalui proses *logical acquisition* menggunakan Android Debug Bridge (ADB) untuk menyalin basis data WhatsApp dari perangkat Android. Aktivitas pada tahap ini meliputi identifikasi perangkat, ekstraksi data, serta pembuatan nilai hash awal guna menjaga integritas data digital [20].
b. *Examination* bertujuan untuk memeriksa dan menyaring data hasil akuisisi dengan menganalisis struktur basis data WhatsApp menggunakan perangkat lunak forensik. Tahap ini berfokus pada identifikasi artefak digital penting, seperti pesan, metadata waktu, serta identitas pengirim dan penerima.
c. *Analysis* difokuskan pada analisis konten percakapan untuk mengidentifikasi bentuk *cyberbullying*, rekonstruksi kronologi kejadian, serta penentuan pola perundungan yang terjadi di dalam grup WhatsApp berdasarkan artefak yang telah diverifikasi. Tahap ini, data yang telah diekstraksi dari file *_chat.txt* dianalisis untuk mengidentifikasi kategori perundungan. Agar analisis bersifat objektif dan konsisten, penelitian ini menetapkan parameter klasifikasi konten berdasarkan indikator kata kunci dapat dilihat pada Tabel 1.

Tabel 1. Parameter Klasifikasi Objektif

Kategori	Deskripsi Operasional	Contoh Potongan Chat dari Data
Penghinaan Verbal	Penggunaan kata kasar atau pelabelan negatif secara langsung untuk menyerang harga diri.	*"Lo mah cuma numpang doang", "lo beban", "gak punya malu".*

Ejekan	Mengolok-olok kapasitas intelektual atau perilaku korban dengan nada sarkastik.	*"Minta dua hari (buat tugas)"*, *"keliatan pinter"*, *"gampang ketipu"*.
Komentar Merendahkan	Upaya pengucilan (*exclusion*) dan meremehkan peran korban dalam kelompok.	*"Mending kamu fokus hal kecil aja"*, *"jangan ikut-ikut dulu"*, *"lo beban kerjaan"*.

d. *Reporting* menghasilkan laporan forensik digital yang memuat seluruh proses investigasi, temuan utama, serta hasil verifikasi integritas data menggunakan algoritma hash SHA-256. Laporan ini disusun agar dapat digunakan sebagai dokumen pendukung dalam konteks akademik maupun hukum [21].

2.4 Alat dan Lingkungan Penelitian

Perangkat keras yang digunakan dalam penelitian ini adalah laptop dengan prosesor Intel Core i7, RAM 32 GB, dan sistem operasi Windows 11. Perangkat lunak yang digunakan meliputi Autopsy, SQLite Viewer, Android Debug Bridge (ADB), dan Microsoft Excel. Ringkasan alat penelitian dapat dilihat pada Tabel 2 yang merupakan penjelasan alat penelitian yang terdiri dari nama alat dan fungsi dari alat yang telah digunakan. Seluruh proses akuisisi dan analisis dilakukan pada sistem terisolasi (*isolated environment*) untuk menjaga keamanan dan integritas bukti digital selama proses investigasi.

Tabel 2. Alat Penelitian

No	Alat	Fungsi
1	ADB	Akuisisi data logis WhatsApp
2	Autopsy	Analisis artefak digital
3	SQLite Viewer	Pemeriksaan basis data
4	Excel	Klasifikasi & rekap data

2.5 Validasi dan Evaluasi

Validasi dilakukan dengan membandingkan hasil analisis terhadap karakteristik dan indikator temuan pada penelitian-penelitian sejenis. Verifikasi integritas data dilakukan menggunakan nilai hash sebagai dasar pembuktian keaslian bukti digital. Selain itu, evaluasi keandalan hasil dilakukan melalui proses peninjauan sejawat (*peer review*) untuk memastikan konsistensi metodologi dan ketepatan interpretasi hasil analisis.

3. HASIL DAN PEMBAHASAN

Hasil penelitian dan pembahasan berdasarkan penerapan metode forensik digital menggunakan kerangka NIST dalam mengidentifikasi *cyberbullying* pada grup WhatsApp. Seluruh tahapan investigasi, yaitu *collection, examination, analysis,* dan *reporting*, dilaksanakan secara sistematis sesuai dengan metodologi penelitian.

3.1 Hasil Akuisisi Data (*Collection*)

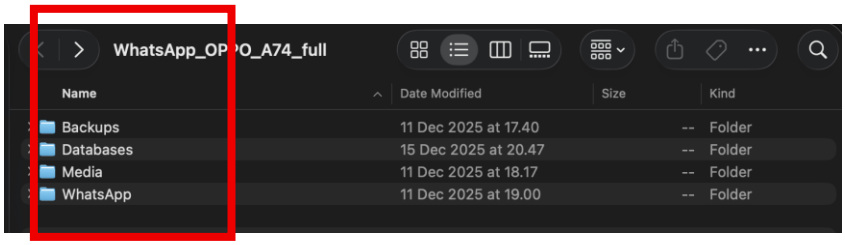
Tahap *collection* dilakukan terhadap satu perangkat *smartphone* Android yang berisi percakapan grup WhatsApp hasil simulasi. Proses akuisisi data menggunakan metode *logical acquisition* melalui *Android Debug Bridge* (ADB). Proses ini diperoleh beberapa artefak digital utama, yaitu file msgstore.db.crypt14 yang berisi isi percakapan WhatsApp, file wa.db yang memuat informasi kontak dan metadata akun, serta direktori media WhatsApp yang berisi lampiran gambar dan pesan suara.

Data harus dipastkan keaslian dan integritas. Setiap file hasil akuisisi diverifikasi menggunakan nilai *hash* SHA-256. Hasil perhitungan *hash* menunjukkan nilai yang konsisten sebelum dan sesudah proses ekstraksi, sehingga dapat disimpulkan bahwa data tidak mengalami perubahan selama proses akuisisi. Temuan ini menunjukkan bahwa metode *logical acquisition* yang diterapkan telah memenuhi prinsip *forensic soundness*. Artefak yang didapat dapat dilihat pada Tabel 3.

Tabel 3. Artefak Data WhatsApp

Artefak	Lokasi	Keterangan
msgstore.db.crypt14	/WhatsApp/Databases	Isi pesan
wa.db	/WhatsApp/Databases	Data kontak
Media	/WhatsApp/Media	Gambar & audio

Tabel 3 menjelaskan artefak yang telah didapat yaitu nama artefak lokasi artefak dan isi dari artefak yang telah ditemukan. Detail artefak dapat dilihat pada Gambar 3 yang menjelaskan hasil file yang telah didapat dari proses akuisisi data whatsapp.



Gambar 3. Hasil File Akuisisi Data Whatsapp

3.2 Pemeriksaan dan Ekstraksi Artefak (*Examination*)

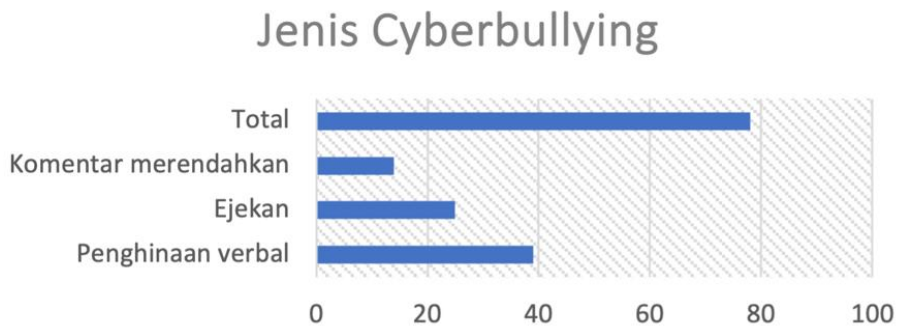
Tahap *examination* dilakukan dengan membuka dan memeriksa struktur basis data WhatsApp menggunakan perangkat lunak forensik. Pemeriksaan difokuskan pada identifikasi tabel-tabel penting yang berkaitan dengan aktivitas komunikasi pengguna, khususnya tabel messages, chat_list, dan contacts.

Hasil pemeriksaan, ditemukan 243 entri pesan dalam grup WhatsApp yang dianalisis. Setiap entri memuat informasi penting berupa isi pesan, waktu pengiriman, serta identitas pengirim. Selain itu, metadata percakapan memungkinkan *investigator* untuk mengamati intensitas komunikasi dan interaksi antaranggota grup. Tahap ini berhasil mengekstraksi artefak digital yang relevan untuk dianalisis lebih lanjut pada tahap berikutnya.

3.3 Analisis Forensik (*Analysis*)

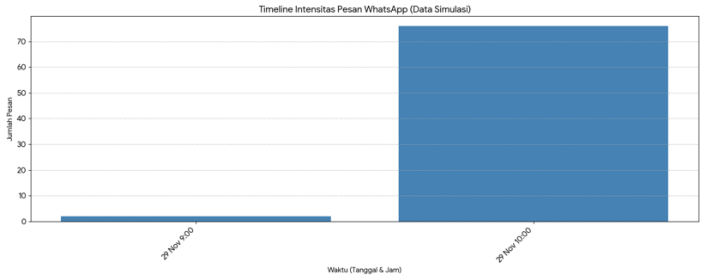
Tahap *analysis* dilakukan untuk mengidentifikasi indikasi *cyberbullying* berdasarkan isi percakapan grup WhatsApp. Analisis dilakukan melalui tiga pendekatan utama, yaitu analisis konten pesan, rekonstruksi kronologi kejadian, dan identifikasi pola perilaku pengguna.

Analisis konten menunjukkan bahwa dari keseluruhan pesan yang diperiksa. Hasil analisis konten menunjukkan bahwa dari total 243 pesan yang diperiksa terdapat 77 pesan yang mengandung unsur *cyberbullying*, seperti penghinaan verbal, ejekan, dan komentar merendahkan terhadap anggota grup tertentu. Rekonstruksi kronologi dilakukan dengan memanfaatkan metadata waktu pada setiap pesan. Hasil analisis menunjukkan bahwa tindakan *cyberbullying* terjadi secara berulang dalam rentang waktu tiga hari berturut-turut, dengan pola intensitas yang meningkat pada jam-jam tertentu. Analisis pola komunikasi mengungkap adanya beberapa akun yang secara konsisten berperan sebagai pelaku utama, dengan frekuensi pengiriman pesan bermuatan negatif yang lebih tinggi dibandingkan anggota grup lainnya. Bentuk *cyberbullying* yang paling dominan adalah perundungan verbal yang dilakukan secara berulang. Jenis-jenis *cyberbullying* yang telah didapat dapat dilihat pada Gambar 4 yang menjelaskan terkait jenis-jenis *cyberbullying* yang dilakukan pada whatsapp yang telah dilakukan. Hasil yang diperoleh 39 penghinaan verbal, 25 ejekan, 14 komentar merendahkan..



Gambar 4 Grafik Jenis *Cyberbullying*

Rekonstruksi kronologi dilakukan dengan memanfaatkan metadata waktu pada setiap pesan. Hasil analisis menunjukkan pola distribusi pesan yang tidak merata, dengan lonjakan intensitas yang signifikan pada jam-jam tertentu sebagaimana ditampilkan pada Gambar 5.



Gambar 5. Timeline intensitas pesan WA (Data Simulasi)

Berdasarkan Gambar 5, terlihat bahwa intensitas perundungan meningkat tajam pada pukul 09.00 hingga 10.00 WIB. Pola ini menunjukkan bahwa pelaku melakukan serangan secara intensif pada waktu istirahat korban, yang memperkuat temuan adanya unsur kesengajaan dalam pola perundungan digital ini.

3.4 Dokumentasi dan Pelaporan (*Reporting*)

Tahap *reporting* menghasilkan dokumen laporan forensik digital yang memuat seluruh proses investigasi dan temuan penelitian. Laporan mencakup deskripsi perangkat yang dianalisis, metode akuisisi data, hasil pemeriksaan dan analisis artefak digital, serta bukti pendukung berupa hasil verifikasi *hash* dan dokumentasi percakapan.

Seluruh hasil laporan disusun secara sistematis agar mudah dipahami dan dapat digunakan sebagai dokumen pendukung dalam konteks akademik maupun hukum. Dokumentasi dilakukan dengan memperhatikan prinsip integritas data dan keterlacakan proses investigasi.

3.5 Pembahasan

Berdasarkan hasil penelitian, penerapan metode NIST terbukti mampu memberikan kerangka kerja yang terstruktur dalam mengidentifikasi dan menganalisis *cyberbullying* pada grup WhatsApp. Setiap tahapan investigasi saling melengkapi dan berkontribusi dalam menjaga validitas serta keandalan hasil analisis.

Meskipun adanya keterbatasan akibat mekanisme enkripsi *end-to-end* pada WhatsApp, metode *logical acquisition* masih memungkinkan diperolehnya artefak digital yang relevan untuk kepentingan investigasi. Selain itu, kombinasi analisis konten, rekonstruksi kronologi, dan identifikasi pola perilaku terbukti efektif dalam mengungkap dinamika perundungan digital dalam grup percakapan.

4. KESIMPULAN

Hasil penelitian dapat disimpulkan bahwa penerapan metode forensik digital berbasis kerangka kerja NIST mampu memberikan alur investigasi yang sistematis dan terstruktur dalam

mengungkap kasus *cyberbullying* pada grup WhatsApp. Melalui metode *logical acquisition*, artefak digital berhasil diperoleh dan dianalisis tanpa mengganggu integritas data, yang dibuktikan melalui verifikasi hash SHA-256. Analisis percakapan mengungkap adanya 77 pesan bermuatan *cyberbullying* dari 243 pesan dengan dominasi perundungan verbal yang terjadi secara berulang dan terarah. Dengan demikian, metode NIST terbukti efektif dalam mendukung proses identifikasi, analisis, dan pelaporan bukti digital *cyberbullying* secara valid dan dapat dipertanggungjawabkan.

Penelitian selanjutnya dapat dilakukan dengan perluasan sumber data ke berbagai grup atau platform pesan instan lain dan kolaborasi dengan lembaga forensik digital resmi dapat meningkatkan validitas hukum hasil penelitian. Pengembangan sistem visualisasi berbasis web juga direkomendasikan untuk membantu investigator dalam memahami pola komunikasi dan kronologi kejadian secara lebih intuitif.

DAFTAR PUSTAKA

[1] E. Bozzola, "The Use of Social Media in Children and Adolescents: Scoping Review on the Potential Risks," *Int J Environ Res Public Health*, vol. 19, no. 16, 2022, doi: 10.3390/ijerph19169960.

[2] C. Evangelio, "Cyberbullying in elementary and middle school students: A systematic review," *Comput Educ*, vol. 176, 2022, doi: 10.1016/j.compedu.2021.104356.

[3] R. R. Hanaputra *et al.*, "Identifikasi Digital Evidence dalam Transaction Fraud pada WhatsApp Desktop berdasarkan NIST SP 800-86: Studi Kasus Bisnis Properti," 2024.

[4] R. Hidayat and N. Anwar, "Forensic Analysis Of Web Phishing And Social Engineering Using The National Institute Of Standards And Technology Method Case Study Of Facebook Account Data Theft," *Journal of Digital Security and Forensics*, vol. 1, no. 1, Jul. 2024, doi: 10.29121/digisecforensics.v1.i1.2024.14.

[5] M. Machrush Aliy Sirojjam Mushlich and R. Wirawan Fernando, "Forensic Analysis Using Autopsy To Get Deleted Whatsapp Data," vol. 13, no. 2, pp. 1–10, 2022, [Online]. Available: http://ejurnal.provisi.ac.id/index.php/JTIKP

[6] R. Majlista and T. Sutabri, "Analisis_Pencarian_Data_Smartphone_Menggunakan_Nis," 2023.

[7] M. Muammar, I. Riadi, and R. Umar, "Pengembangan Alat Forensik Whatsapp Menggunakan Android Debug Bridge Sebagai Metode Akuisisi Data," *JIPI (Jurnal Ilmiah Penelitian dan Pembelajaran Informatika)*, vol. 10, no. 2, pp. 1099–1110, Mar. 2025, doi: 10.29100/jipi.v10i2.5968.

[8] M. F. Mubarok Nahdli, M. K. Biddinika, and I. Riadi, "Forensic Analysis of the WhatsApp Application Using the National Institute of Justice Framework," *International Journal of Advances in Data and Information Systems*, vol. 5, no. 2, Sep. 2024, doi: 10.59395/ijadis.v5i2.1328.

[9] A. M. Muniz Soares, "WhatsApp Web Client Live Forensics Technique," in *International Conference on Information Systems Security and Privacy*, Science and Technology Publications, Lda, 2022, pp. 629–636. doi: 10.5220/0011006400003120.

[10] B. A. H. Murshed, "DEA-RNN: A Hybrid Deep Learning Approach for Cyberbullying Detection in Twitter Social Media Platform," *IEEE Access*, vol. 10, pp. 25857–25871, 2022, doi: 10.1109/ACCESS.2022.3153675.

[11] F. Nasiroturrohmah, R. Rustono, B. Wahyudi, and J. Santoso, "Seloka: Jurnal Pendidikan Bahasa dan Sastra Indonesia Types of Cyberbullying What Happens Between Middle School Students on Social Media Whatsapp," 2024, [Online]. Available: https://journal.unnes.ac.id/sju/index.php/seloka

[12] S. Nishchal, "Forensic Analysis of WhatsApp: A Review of Techniques, Challenges, and Future Directions," *Journal of Forensic Science and Research*, vol. 8, no. 1, pp. 019–024, Jun. 2024, doi: 10.29328/journal.jfsr.1001059.

[13] R. Nurdin and E. Ramadhani, “Investigasi Forensika Digital WhatsApp Scam Dengan Menggunakan Framework D4I,” vol. 11, no. 1, pp. 158–166, 2024, [Online]. Available: http://jurnal.mdp.ac.id

[14] E. Putri Silmina, S. Sunardi, and A. Yudhana, “Comparative Analysis Of Yolo Deep Learning Model For Image-Based Beef Freshness Detection,” *JITK (Jurnal Ilmu Pengetahuan dan Teknologi Komputer)*, vol. 11, no. 1, pp. 250–265, Aug. 2025, doi: 10.33480/jitk.v11i1.6784.

[15] S. Sarmini, S. Sunardi, and A. Fadlil, “Evaluating The Effectiveness of Augmentation and Classifier Algorithms for Fraud Detection: Comparing CGAN and SMOTE with Random Forest and XGBoost,” *Applied Information System and Management (AISM)*, vol. 8, no. 2, pp. 221–230, Oct. 2025, doi: 10.15408/aism.v8i2.46308.

[16] J. R. Polanin, “A Systematic Review and Meta-analysis of Interventions to Decrease Cyberbullying Perpetration and Victimization,” *Prevention Science*, vol. 23, no. 3, pp. 439–454, 2022, doi: 10.1007/s11121-021-01259-y.

[17] I. Riadi and T. Ruslan, “Analisis Forensik Digital Pada Whatsapp Dan Facebook Menggunakan Metode NIST,” 2023.

[18] S. alya Sudjayanti and D. Hamdani, “Digital Forensic Analysis Of APK Files In Phishing Scams On Whatsapp Using The NIST Method,” *Brilliance: Research of Artificial Intelligence*, vol. 4, no. 1, pp. 100–110, May 2024, doi: 10.47709/brilliance.v4i1.3800.

[19] 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.

[20] A. Yudhana, I. Riadi, R. Yudhi Prasongko, A. Dahlan, J. Ahmad Yani Tamanan, and J. Soepomo, “Forensik WhatsApp Menggunakan Metode Digital Forensic Research Workshop (DFRWS),” vol. 7, no. 1, 2022.

[21] D. Yuliana, T. Yuniati, and B. P. Zen, “CyberSecurity dan Forensik Digital,” 2022.