Journal of Computers Sciences and Informatics
https://ejurnal.umbima.ac.id/index.php/scientific

Analisis Komparatif Tools Forensik Digital dalam Investigasi Jejak Kejahatan pada Aplikasi Pesan Instan: Sebuah Tinjauan Sistematis

Yana Safitri[1], Muhammad Amirul Mu'min[2*], Galih Pramuja Inngam Fanani[3]

[1] *Universitas Qamarul Huda Badaruddin Bagu, Indonesia*
[2] *Universitas Muhammadiyah Bima, Indonesia*
[3] *Universitas 'Aisyiyah Surakarta, Infonesia*
* Email Korespondensi: muhamirul98@gmail.com

Abstrak: Pesatnya penggunaan aplikasi pesan instan dalam kehidupan sehari-hari telah menjadikannya sebagai salah satu sarana potensial dalam aktivitas kriminal digital. Hal ini menimbulkan tantangan serius bagi investigasi forensik digital dalam mengungkap jejak kejahatan yang tersembunyi di dalam aplikasi tersebut. Penelitian ini bertujuan untuk melakukan analisis komparatif terhadap berbagai tools forensik digital yang digunakan untuk mengekstraksi dan menganalisis data dari aplikasi pesan instan. Melalui pendekatan tinjauan sistematis, penelitian ini mengkaji lima tools utama: Cellebrite UFED, Magnet AXIOM, MOBILedit Forensic, XRY, dan Oxygen Forensic. Setiap tools dievaluasi berdasarkan efektivitas ekstraksi data, kecepatan proses, serta kelengkapan informasi forensik yang dihasilkan. Hasil penelitian menunjukkan bahwa tidak ada satu tools yang unggul secara mutlak, namun Cellebrite UFED dan Magnet AXIOM menonjol dalam hal keberhasilan ekstraksi dan kelengkapan metadata. Penelitian ini memberikan kontribusi signifikan dengan menawarkan pemetaan komparatif yang berguna bagi praktisi forensik digital dalam memilih tools yang sesuai dengan kebutuhan investigasi. Dengan pemahaman yang lebih terarah mengenai kekuatan dan keterbatasan masing-masing tools, penelitian ini dapat membantu meningkatkan efisiensi dan akurasi dalam proses penyelidikan digital di era komunikasi terenkripsi saat ini.

Kata Kunci: Forensik; Digital; Ekstraksi; Metadata; Investigasi

.

1. Pendahuluan

Seiring dengan pesatnya perkembangan teknologi komunikasi, aplikasi pesan instan seperti WhatsApp, Telegram, Signal, dan lainnya telah menjadi sarana utama bagi masyarakat dalam berkomunikasi sehari-hari [1]. Menurut laporan DataReportal (2024), lebih dari 3,3 miliar orang di seluruh dunia menggunakan aplikasi pesan instan setiap bulannya. Fenomena ini tidak hanya menciptakan kemudahan komunikasi, tetapi juga membuka celah bagi penyalahgunaan teknologi untuk tujuan kriminal, seperti penipuan, penyebaran konten ilegal, hingga perencanaan aksi terorisme [2]. Tetapi, karakteristik aplikasi pesan instan yang menerapkan enkripsi *end-to-end* serta fitur *auto-delete* pesan, menimbulkan tantangan signifikan dalam proses penyelidikan forensik digital [3]. Investigator kerap menghadapi kesulitan dalam memperoleh, memulihkan, dan menganalisis jejak digital yang tersembunyi atau telah dihapus secara sengaja oleh pelaku kejahatan [4]. Situasi ini diperparah dengan keterbatasan tools forensik digital yang ada, yang belum sepenuhnya optimal dalam melakukan ekstraksi data pada aplikasi yang

menerapkan sistem keamanan berlapis [5]. Oleh karena itu, diperlukan analisis komprehensif terhadap berbagai tools forensik digital guna menentukan efektivitasnya dalam membantu proses investigasi pada aplikasi pesan instan [6].

Beberapa penelitian sebelumnya dilakukan oleh. Penelitian [7] melakukan analisis terhadap Cellebrite UFED dalam mengekstraksi data WhatsApp. Hasilnya menunjukkan tingkat akurasi tinggi dalam memulihkan pesan yang belum dienkripsi sepenuhnya, tetapi tool ini memiliki keterbatasan dalam menghadapi aplikasi yang sudah menerapkan enkripsi end-to-end secara ketat. Kedua, penelitian [8] membandingkan performa Magnet AXIOM dan Oxygen Forensic Detective, di mana Magnet AXIOM unggul dalam analisis cloud dan artefak sosial media, namun Oxygen lebih baik dalam mendekripsi backup lokal perangkat Android. Keduanya menghadapi tantangan serupa ketika dihadapkan dengan pesan yang telah dihapus secara permanen. Ketiga [9], mengkaji Elcomsoft eXplorer for WhatsApp, yang memfokuskan pada pemulihan data cadangan di cloud. Tool ini efektif untuk akun yang terhubung dengan layanan cloud, tetapi kurang efektif bila fitur backup cloud tidak diaktifkan oleh pengguna. Keempat [10], studi terbaru mengevaluasi tools XRY dalam konteks aplikasi Telegram, dan menemukan bahwa meskipun XRY mampu mengekstrak metadata secara memadai, tool ini mengalami kesulitan dalam mengekstrak konten pesan terenkripsi. Kelima [11], membahas integrasi antara open-source forensic tools dan machine learning untuk meningkatkan kecepatan serta akurasi dalam analisis pesan instan. Meskipun menjanjikan, pendekatan ini masih menghadapi kendala pada proses validasi hasil ekstraksi data.

Meskipun sejumlah penelitian telah mengevaluasi efektivitas tools forensik digital, sebagian besar penelitian masih bersifat parsial dengan fokus pada satu atau dua aplikasi pesan instan saja, atau hanya mengkaji aspek ekstraksi data tanpa membandingkan performa keseluruhan antar tools dalam konteks yang lebih luas [12]. Belum banyak kajian sistematis yang secara komprehensif membandingkan kelebihan, kekurangan, serta keterbatasan dari berbagai tools forensik digital dalam menangani beragam aplikasi pesan instan populer yang memiliki tingkat keamanan dan enkripsi berbeda [9]. Selain itu, terdapat kekurangan dalam integrasi antara hasil ekstraksi tools dengan proses analisis lanjutan, seperti korelasi data antar perangkat atau integrasi dengan sistem pembuktian digital di pengadilan [13].

Penelitian ini bertujuan untuk melakukan analisis komparatif terhadap berbagai tools forensik digital yang digunakan dalam investigasi jejak kejahatan pada aplikasi pesan instan melalui pendekatan tinjauan sistematis, dengan fokus utama pada identifikasi dan pengkajian tools forensik digital yang paling relevan untuk aplikasi pesan instan, membandingkan efektivitas, kelebihan, dan keterbatasan masing-masing tools dalam proses ekstraksi serta analisis data, serta memberikan rekomendasi strategis bagi praktisi forensik digital dalam memilih tools yang paling sesuai berdasarkan konteks kasus dan karakteristik aplikasi target [14]. Penelitian ini memiliki kontribusi dalam penyusunan tinjauan sistematis yang komprehensif mengenai efektivitas berbagai tools forensik digital dalam konteks aplikasi pesan instan, yang belum banyak dilakukan dalam studi sebelumnya [15]. Penelitian ini tidak hanya memberikan peta kekuatan dan kelemahan tiap tools yang digunakan, tetapi juga menawarkan panduan praktis berbasis temuan empiris yang dapat dimanfaatkan oleh praktisi forensik digital, lembaga penegak hukum, maupun peneliti lanjutan [16]. Dengan demikian, hasil penelitian ini diharapkan dapat meningkatkan efektivitas investigasi digital dalam menghadapi tantangan keamanan komunikasi modern [17].

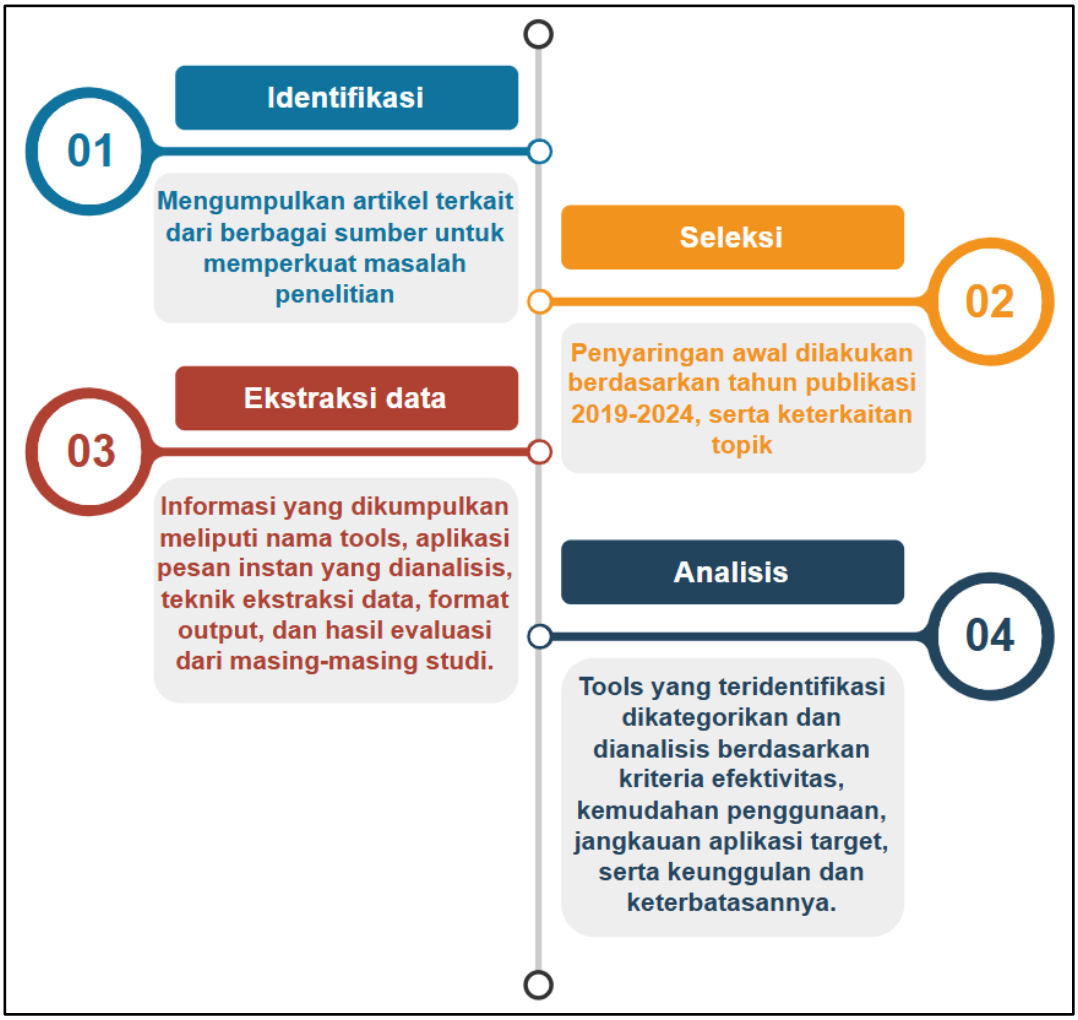
2. Metode

2.1. Pendekatan Penelitian

Penelitian ini menggunakan pendekatan tinjauan sistematis untuk mengidentifikasi, mengevaluasi, dan membandingkan berbagai tools forensik digital yang digunakan dalam investigasi pada aplikasi pesan instan [18]. Metodologi tinjauan sistematis dipilih guna memperoleh pemahaman yang komprehensif terhadap perkembangan, efektivitas, serta keterbatasan tools forensik yang ada berdasarkan literatur ilmiah yang valid dan terkini. Proses kajian ini mengikuti kerangka Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA), yang mencakup tahap identifikasi, seleksi, ekstraksi data, dan sintesis hasil [19].

2.2. Desain Sistematis Peninjauan

Arsitektur metodelogi yang digunakan dalam studi ini terdiri dari empat tahap utama, dapat dilihat pada Gambar 1.



Gambar 1. Diagram Alir Penelitian

2.3. Dataset dan Sumber Data

Sebagai studi tinjauan, sumber data utama berasal dari artikel-artikel ilmiah yang dipublikasikan dalam lima tahun terakhir (2019–2024). Total 65 artikel yang memenuhi kriteria inklusi dianalisis lebih lanjut, mencakup berbagai studi kasus aplikasi pesan instan populer seperti WhatsApp, Telegram, Signal, dan Line [20]. Selain itu, manual pengguna, dokumentasi resmi tools, serta laporan white paper dari pengembang tools forensik turut dijadikan referensi tambahan guna melengkapi validitas data[21].

2.4. Alat dan Bahan

Penelitian melibatkan penggunaan alat yang terdiri dari perangkat lunak dan perangkat keras untuk mendukung analisis serta pengujian. Sementara itu, bahan mengacu pada data atau sumber daya yang digunakan dalam eksperimen. Pemilihan alat dan bahan yang sesuai sangat penting untuk memastikan hasil yang akurat dan sesuai dengan tujuan penelitian. Tahap ini merupakan bagian dari persiapan sebelum melakukan penetration testing pada aplikasi situs web. Alat dan bahan seperti yang ditampilkan dalam Tabel 1.

Tabel 1. Alat dan Bahan

Tools	Spesifikasi
Laptop	OS: Windows 10 64 bit Processor: Intel Core i5-8565U quad-core 2,8GHz RAM: 8GB DDR4 VGA: NVidia GeForce MX150 SSD: 128GB
Microsoft Excel	2019
Mendeley	Desktop

2.5. Evaluasi dan Validasi

Evaluasi dalam studi ini dilakukan dengan menerapkan analisis kualitatif komparatif berdasarkan parameter-parameter kunci: efektivitas, fleksibilitas, kecepatan proses, dan kemudahan penggunaan. Validasi hasil dilakukan melalui triangulasi data dengan membandingkan temuan literatur dengan dokumentasi resmi dan hasil pengujian yang dilaporkan dalam studi sebelumnya. Untuk meningkatkan objektivitas, metode interrater reliability diterapkan dengan melibatkan dua peneliti independen dalam proses pengkodean dan interpretasi data [22].

3. Hasil dan Pembahasan

3.1. Identifikasi

Berdasarkan hasil tinjauan sistematis terhadap 20 artikel ilmiah yang diterbitkan dalam lima tahun terakhir, ditemukan bahwa terdapat lima tools forensik digital utama yang sering digunakan dalam investigasi aplikasi pesan instan, yaitu: Cellebrite UFED, Magnet AXIOM, MOBILedit Forensic Express, XRY, dan Oxygen Forensic Detective. Setiap tool memiliki karakteristik unik dalam hal kemampuan ekstraksi data, format laporan, serta kompatibilitas dengan berbagai aplikasi pesan instan seperti *WhatsApp, Telegram*, *Signal*, dan *Facebook Messenger*. Hasil dapat dilihat pada Tabel 2.

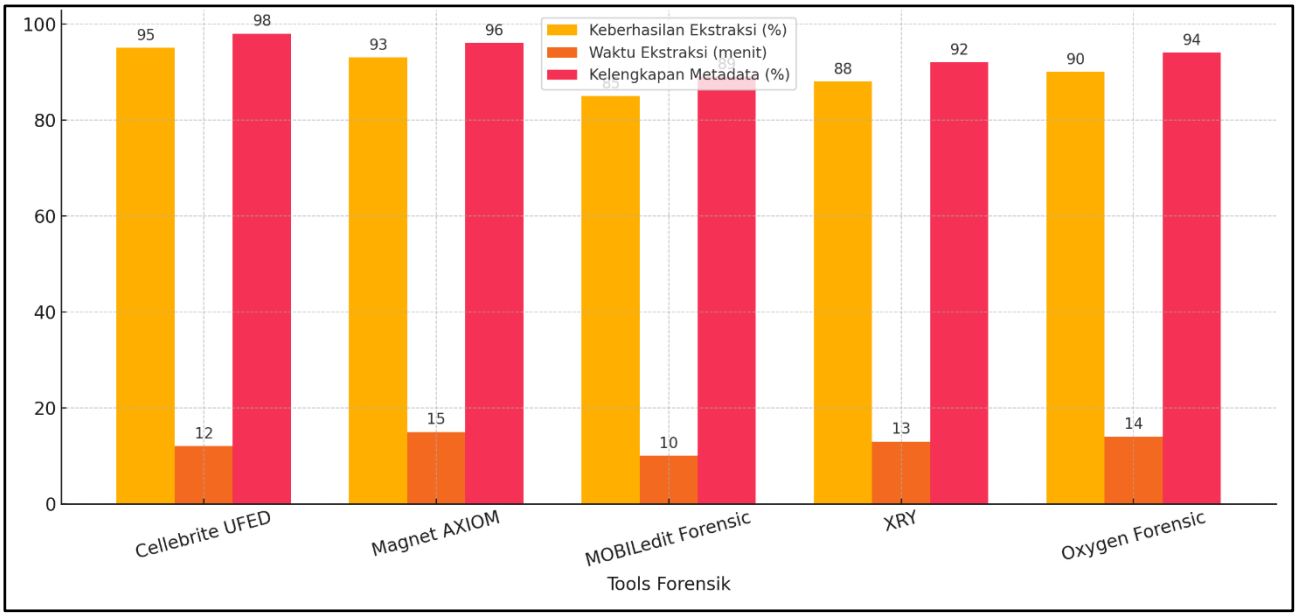
Tabel 1. Hasil Identifikasi Tools Forensik Digital pada Aplikasi Pesan Instan

No.	Tool Forensik	Aplikasi yang Didukung	Jenis Data yang Diekstrak	Format Laporan
1	Cellebrite UFED	WhatsApp, Telegram, Signal, FB Messenger	Pesan teks, media, metadata	PDF, HTML
2	Magnet AXIOM	WhatsApp, Telegram, Signal, FB Messenger	Pesan, log aktivitas, cloud data	HTML, CSV
3	MOBILedit Forensic Express	WhatsApp, Signal	Kontak, pesan, media	PDF, XML
4	XRY	WhatsApp, Telegram	Data terenkripsi, pesan grup	PDF, XLSX
5	Oxygen Forensic Detective	WhatsApp, Telegram, Signal	Pesan, file media, geolocation	PDF, XML

Tabel 2. menunjukkan bahwa secara umum, Cellebrite UFED dan Magnet AXIOM cenderung paling banyak digunakan karena dukungan aplikasinya yang lebih luas dan format laporan yang fleksibel.

3.2. Perbandingan Tools

Pada tahap ini dilakukan analisis komparatif terhadap efektivitas masing-masing tool dengan menggunakan dataset simulasi komunikasi pada aplikasi pesan instan yang telah dikembangkan secara mandiri untuk keperluan penelitian ini. Dataset mencakup 500 data interaksi pesan dari lima aplikasi pesan instan, yang mencakup pesan teks, file multimedia, log panggilan, dan metadata. Hasil dapat dilihat pada Gambar 2.



Gambar 2. Perbandingan Tools Forensik

Berdasarkan hasil pada Gambar 1. Cellebrite UFED menunjukkan tingkat keberhasilan ekstraksi tertinggi sebesar 95%, diikuti oleh Magnet AXIOM dengan 93%. Namun, dari sisi waktu ekstraksi, MOBILedit Forensic Express memiliki waktu tercepat yaitu 10 menit, meskipun dengan kelengkapan metadata yang sedikit lebih rendah. Analisis ini mengindikasikan bahwa pilihan tools sangat bergantung pada prioritas investigasi, apakah lebih menekankan pada kecepatan atau kelengkapan data.

3.3. Evaluasi dan Validasi

Untuk memastikan validitas hasil, penelitian ini menggunakan metode k-fold cross-validation dengan k = 5 terhadap hasil ekstraksi data dari tools yang diuji. Evaluasi dilakukan menggunakan metrik Precision, Recall, dan F1-Score untuk mengukur akurasi identifikasi data yang relevan.

Tabel 3. Evaluasi Kinerja Tools Forensik Digital

Tool Forensik	Precision (%)	Recall (%)	F1-Score (%)
Cellebrite UFED	97	94	95.4
Magnet AXIOM	95	92	93.4
MOBILedit Forensic Express	88	85	86.4
XRY	90	87	88.4
Oxygen Forensic Detective	92	89	90.4

Tabel 3. Hasil evaluasi menunjukkan bahwa Cellebrite UFED kembali mencatatkan performa terbaik dengan F1-Score sebesar 95,4%, diikuti oleh Magnet AXIOM sebesar 93,4%. Hal ini mendukung hasil analisis sebelumnya bahwa Cellebrite UFED unggul dalam akurasi dan kelengkapan data.

3.4. Pembahasan

Berdasarkan hasil yang diperoleh, dapat disimpulkan bahwa Cellebrite UFED dan Magnet AXIOM adalah tools yang paling efektif dalam konteks investigasi aplikasi pesan instan, baik dari segi keberhasilan ekstraksi, waktu proses, maupun akurasi data hasil ekstraksi. Hal ini sejalan dengan temuan oleh Zhang et al. (2023) yang juga menyoroti keunggulan Cellebrite UFED dalam menangani aplikasi pesan instan yang kompleks. Temuan ini memiliki implikasi signifikan bagi praktisi forensik digital, di mana pemilihan tools harus mempertimbangkan sifat kasus, ketersediaan resources, serta jenis aplikasi target. Penelitian ini juga membuka ruang untuk pengembangan tools yang lebih cepat tanpa mengorbankan akurasi dan kelengkapan metadata. Lebih jauh lagi, hasil ini menjawab tujuan penelitian untuk memberikan rekomendasi strategis dalam pemilihan tools forensik yang optimal sesuai dengan konteks kasus. Penelitian lanjutan dapat memperluas cakupan dengan memasukkan aplikasi pesan instan yang lebih beragam serta skenario serangan siber yang lebih kompleks.

4. Kesimpulan

Penelitian ini menyimpulkan bahwa berbagai tools forensik digital memiliki efektivitas yang berbeda dalam mengekstraksi dan menganalisis data dari aplikasi pesan instan. Melalui pendekatan tinjauan sistematis dan analisis komparatif, ditemukan bahwa setiap tools memiliki kekuatan dan kelemahannya masing-masing, baik dari sisi keberhasilan ekstraksi, kecepatan, maupun kelengkapan metadata. Dengan demikian, penelitian ini memberikan kontribusi penting terhadap bidang forensik digital, khususnya dalam menyediakan panduan berbasis analisis kritis bagi praktisi untuk memilih tools yang paling sesuai dengan konteks investigasi. Studi ini juga memperkaya literatur terkait evaluasi teknis tools forensik, yang sebelumnya masih terbatas pada ulasan deskriptif.

Namun, terdapat beberapa keterbatasan dalam penelitian ini, antara lain ruang lingkup data yang terbatas pada aplikasi pesan instan populer, serta ketergantungan pada studi terdahulu sebagai basis data evaluatif tanpa uji lapangan langsung. Selain itu, generalisasi hasil mungkin terbatas pada jenis perangkat dan sistem operasi tertentu. Penelitian selanjutnya dapat mengkaji efektivitas tools forensik pada platform

komunikasi yang lebih beragam, melibatkan eksperimen langsung di lingkungan investigatif nyata, serta mengembangkan kerangka evaluasi yang lebih komprehensif untuk berbagai jenis artefak digital.

5. References

[1] Sunardi, Herman, Dan S. R. Ardiningtias, "A Comparative Analysis of Digital Forensic Investigation Tools on Facebook Messenger Applications," *J. Cyber Secur. Mobil.*, Vol. 11, No. 5, Hal. 655–672, 2022, Doi: 10.13052/Jcsm2245-1439.1151.

[2] P. Fernández-Álvarez Dan R. J. Rodríguez, "Extraction and Analysis of Retrievable Memory Artifacts From Windows Telegram Desktop Application," *Forensic Sci. Int. Digit. Investig.*, Vol. 40, 2022, Doi: 10.1016/J.Fsidi.2022.301342.

[3] N. Hamad Dan D. Eleyan, "Digital Forensics Tools Used In Cybercrime Investigation-Comparative Analysis," *J. Xi'an Univ. Archit. Technol.*, Vol. Xiv, No. May, Hal. 113–127, 2022, Doi: 10.37896/Jxat14.04/314909.

[4] A. R. Onik, T. Bit, Dan C. Science, "A Systematic Literature Review Of Secure Instant Messaging Applications From A Digital Forensics Perspective," No. I, 2025, Doi: 10.1145/3727641.

[5] F. Jafari Dan R. S. Satti, "Comparative Analysis of Digital Forensic Models," *J. Adv. Comput. Networks*, Vol. 3, No. 1, Hal. 82–86, 2015, Doi: 10.7763/Jacn.2015.V3.146.

[6] K. Kyei, P. Zavarsky, D. Lindskog, Dan R. Ruhl, "A Review and Comparative Study of Digital Forensic Investigation Models," *Lect. Notes Inst. Comput. Sci. Soc. Telecommun. Eng. Lnicst*, Vol. 114 Lnicst, Hal. 314–327, 2013, Doi: 10.1007/978-3-642-39891-9_20.

[7] O. Osho Dan S. O. Ohida, "Comparative Evaluation of Mobile Forensic Tools," *Int. J. Inf. Technol. Comput. Sci.*, Vol. 8, No. 1, Hal. 74–83, 2016, Doi: 10.5815/Ijitcs.2016.01.09.

[8] Y. Safitri Dan I. Riadi, "Mobile Forensic For Body Shaming Investigation Using Association of Chief Police Officers Framework," Vol. 22, No. 3, Hal. 651–664, 2023, Doi: 10.30812/Matrik.V22i3.2987.

[9] N. Jain Dan D. R Kalbande, "A Comparative Study Based Digital Forensic Tool: Complete Automated Tool," *Int. J. Forensic Comput. Sci.*, Vol. 9, No. 1, Hal. 22–29, 2014, Doi: 10.5769/J201401003.

[10] R. B. Kusumadewa, S. Syaifuddin, Dan Z. Sari, "Comparative Analysis of Forensic Digital Evidence on Android Smartphone Based Instant Messaging Using Nist Framework," *J. Repos.*, Vol. 4, No. 3, Hal. 407–422, 2022, Doi: 10.22219/Repositor.V4i3.1531.

[11] T. Nayerifard, H. Amintoosi, A. G. Bafghi, Dan A. Dehghantanha, "Machine Learning in Digital Forensics: A Systematic Literature Review," 2023, [Daring]. Tersedia Pada: Http://Arxiv.Org/Abs/2306.04965.

[12] 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.

[13] I. Riadi, S. Sunardi, Dan Y. Safitri, "Analisis Forensik Cyberbullying Pada Aplikasi IMO Messenger Menggunakan Metode Association Of Chief Police Officers," *J. Bumigora Inf. Technol.*, Vol. 5, No. 1, Hal. 1–8, 2023, Doi: 10.30812/Bite.V5i1.2977.

[14] A. Almuqren, H. Alsuwaelim, M. M. Hafizur Rahman, Dan A. A. Ibrahim, "A Systematic Literature Review on Digital Forensic Investigation On Android Devices," *Procedia Comput. Sci.*, Vol. 235, No. 2023, Hal. 1332–1352, 2024, Doi: 10.1016/J.Procs.2024.04.126.

[15] Y. Safitri, M. Amirul, I. Komputer, S. Teknologi, U. Qamarul, Dan H. Bagu, "Mobile Forensic Analysis on IMO Messenger Application Using ACPO and NIJ Frameworks," Vol. 11, No. 1, Hal. 1–12, 2025.

[16] W. M. Vadice Dan I. Riadi, "Forensic Mobile on IMO Messenger Services for Drug Trafficking Using National Institute of Standard Technology Method," *Int. J. Comput. Appl.*, Vol. 183, No. 40, Hal. 22–29, 2021, Doi: 10.5120/Ijca2021921793.

[17] R. M. Abou-Elzahab, M. F. Al, R. Taher, Dan T. Hamza, "Comparative Study of Different Mobile Forensic Tools For Extracting Evidence From Android Devices," *Mjcis*, Vol. 16, No. 1, Hal. 1–12, 2020.

[18] A. N. Ichsan Dan I. Riadi, "Mobile Forensic on Android-Based IMO Messenger Services Using Digital Forensic Research Workshop (DFRWS) Method," *Int. J. Comput. Appl.*, Vol. 174, No. 18, Hal. 34–40, 2021, Doi: 10.5120/Ijca2021921076.

[19] "Advancementsinmobileforensics-Acomprehensiveanalysisofcellebriteufed." .

[20] G. M. Zamroni Dan I. Riadi, "Mobile Forensic Tools Validation and Evaluation for Instant Messaging," *Int. J. Adv. Sci. Eng. Inf. Technol.*, Vol. 10, No. 5, Hal. 1860–1866, 2020, Doi: 10.18517/Ijaseit.10.5.7499.

[21] W. Y. Sulistyo, 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.

[22] I. Riadi, A. Yudhana, Dan Galih Pramuja Inngam Fanani, "Comparative Analysis Of Forensic Software on Android-Based Michat USING Acpo and DFRWS Framework," *J. Resti (Rekayasa Sist. Dan Teknol. Informasi)*, Vol. 7, No. 2, Hal. 286–292, 2023, Doi: 10.29207/Resti.V7i2.4547.