Jurnal Teknologi Terpadu

https://journal.nurulfikri.ac.id/index.php/jtt
ISSN : 2477-0043 ISSN ONLINE : 2460-7908

ANALISIS DAN PERBANDINGAN *TOOLS* FORENSIK MENGGUNAKAN METODE NIST DALAM PENANGANAN KASUS KEJAHATAN SIBER

Achmad Iqbal Yuladi[1], Rini Indrayani[2]

[1] Teknik Komputer, Universitas Amikom Yogyakarta
[2] Rekayasa Perangkat Lunak, Universitas Muhammadiyah Palopo
Sleman, Daerah Istimewa Yogyakarta, Indonesia 55281
achmad.11@students.amikom.ac.id , riniindrayani@umpalopo.ac.id

Abstract

Cybercrime cases in Indonesia have increased yearly; during the COVID-19 pandemic as it is now, people rely on the internet to carry out daily activities such as teaching and learning activities, buying and selling online, working from home, etc. Therefore, cybercrime cases in Indonesia have increased. One of the most common examples is Cyberbullying cases on various social media networks with mobile platforms, one of which is WhatsApp Messenger. This study will analyze and compare the results of the MOBILedit Forensic Express and Magnet Axiom tools using the National Institute of Standards and Technology (NIST) method. This method can facilitate the investigation process in the case scenarios in this research. Researchers will also compare the results of the two tools used in this forensic process. The results of this study using the National Institute of Standards and Technology (NIST) method on the WhatsApp apps showed the Magnet Axiom tools were slightly superior with an accuracy of 82,8% compared to MOBILedit Forensics Express 72,7% in the condition that the object was not rooted.

Keywords: *Cyberbullying, Cybercrime, Digital Forensic, Forensic Tools, NIST.*

Abstrak

Kasus Kejahatan siber di Indonesia setiap tahunnya mengalami peningkatan, pada masa pandemi *COVID* -19 seperti sekarang, masyarakat mengandalkan internet untuk melakukan kegiatan sehari-hari seperti kegiatan belajar mengajar, jual-beli *online*, kerja dari rumah, dan lain sebagainya. Oleh karena itu kasus kejahatan siber di Indonesia mengalami peningkatan, salah satu contoh yang paling sering terjadi yaitu kasus *Cyberbullying* di berbagai jejaring *social media* dengan *platform mobile*, salah satunya WhatsApp *Messanger*. Penelitian ini akan menganalisis dan membandingkan hasil dari *tools* MOBILedit Forensic Express dan Magnet Axiom dengan menggunakan metode *National Institute of Standards and Technology* (NIST). Metode tersebut dapat memudahkan proses investigasi pada skenario kasus yang ada pada penelitian ini. Peneliti juga akan membandingkan hasil yang diperoleh oleh kedua *tools* yang digunakan pada proses forensik ini. Hasil dari penelitian ini pada aplikasi WhatsApp *Messanger* menunjukkan *tools* Magnet Axiom sedikit lebih unggul dengan akurasi 81,8% dibandingkan MOBILedit Forensics Express 72,7% dalam kondisi objek *Un-rooted*.

Kata kunci: *Cyberbullying*, Forensik Digital, Kejahatan Siber, NIST, *Tools* Forensik.

1. PENDAHULUAN

Perkembangan era teknologi yang cepat dan dengan adanya pandemi *COVID* -19 ini mengharuskan kegiatan sehari-hari dilakukan secara digital. Hal tersebut akan membuat kemungkinan terjadinya kejahatan digital atau kejahatan *cybercrime* meningkat. *Cybercrime* adalah segala aktivitas ilegal yang digunakan oleh pelaku kejahatan dengan memanfaatkan teknologi sistem informasi jaringan komputer. Salah satunya *Cyberbullying* atau tindakan merendahkan derajat orang lain dengan memanfaatkan teknologi *smartphone* [1]. Kejahatan *cyberbullying* dapat dilakukan menggunakan *platform instant messenger* WhatsApp. Menurut Hootsuite (We are Social) pada tahun 2022 pengguna aplikasi pesan singkat Whatsapp messanger di Indonesia sebanyak 88,7% dari jumlah populasi orang di Indonesia[2]. Tindakan kejahatan *cyberbullying* tersebut biasanya meninggalkan jejak digital pelaku pada *smartphone* yang digunakan oleh pelaku untuk melakukan tindakan tersebut[3]. Jejak digital ini dapat digunakan sebagai barang bukti tindak kejahatan siber yang menjadi bagian dari tindak pidana dan dapat menjadi barang bukti untuk dibawa ke pihak berwenang [4][5]. Namun sering kali para pelaku tindak kejahatan siber berusaha menghilangkan jejak digitalnya untuk menutupi kejahatan yang

Diterima 14 Desember 2022, Direvisi 14 Juni 2023, Diterima untuk publikasi 20 Juli 2023

dilakukannya. Oleh karena itu diperlukan *Mobile Forensic* untuk mengembalikan atau menemukan jejak digital yang sudah dihapus oleh pelaku[6][7]. *Mobile forensic* dilakukan dengan menganalisis barang bukti *smartphone* dari pelaku tindak kejahatan siber. Barang bukti tersebut merupakan informasi yang valid dan dapat mendukung penegak hukum dalam mengambil keputusan[8].

Terdapat beberapa kerangka kerja atau *framework* untuk melakukan *digital forensic* maupun *mobile forensic* salah satunya yaitu *National Institute Standards and Technology (NIST)*. Metode NIST terdiri dari 4 tahapan, *Collection, Examination, Analysis,* dan *Reporting*[9]. NIST memiliki panduan kerja baik itu kebijakan dan standar untuk menjamin setiap orang yang melakukan *digital forensic* akan menggunakan alur kerja yang sama akan menjadikan pekerjaan mereka dapat didokumentasikan sehingga hasilnya bisa diulang dan juga bisa dipertahankan[10].

Beberapa penelitian terkait *Mobile forensic* dengan memanfaatkan beberapa *tools* dan berbagai jenis skenario media sosial telah dilakukan. Salah satu penelitian terkait yaitu penelitian mengenai penggunaan *Mobile forensic* pada analisis bukti digital tindak kejahatan memanfaatkan media *social* Facebook[4]. Penelitian tersebut menggunakan *tool* Oxigen Forensic untuk mendapatkan barang bukti dari *smartphone* yang digunakan pelaku. Hasil penelitian tersebut menunjukkan bahwa barang bukti yang berhasil didapatkan menggunakan Oxigen Forensic adalah barang bukti berupa percakapan, gambar, dan audio. Sementara barang bukti berupa video tidak berhasil dikembalikan.

Penelitian lain terkait penggunaan metode NIST memanfaatkan *tool* MOBILedit Forensic Express memanfaatkan *platform* Telegram[9]. Penelitian tersebut melakukan upaya pengangkatan barang bukti digital menggunakan skenario penggelapan dana. Hasil penelitian tersebut menunjukkan bahwa dengan menggunakan *tool* MOBILedit Forensic Express, barang bukti digital yang didapatkan mencapai persentase sebanyak 75% berupa profil pengguna, kontak, email, *chat*, dan gambar.

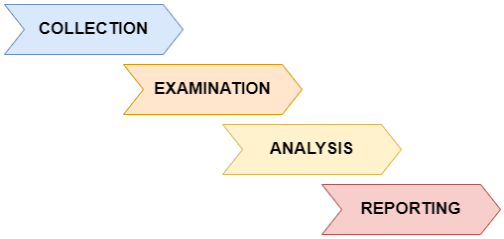
Terdapat banyak *tools* yang dapat digunakan untuk melakukan *Mobile forensic* pada *smartphone*, namun penelitian ini menggunakan *tools* MOBILedit Forensic Express dan Magnet Axiom. Kemudian kedua *tools* tersebut akan dibandingkan untuk mendapatkan rekomendasi *tools* mana yang lebih baik untuk penanganan kasus *Cyberbullying* sesuai skenario yang telah ditentukan. [11].

Menurut hasil riset *Polling* Indonesia bersama dengan Asosiasi Penyelenggara Jasa Internet Indonesia (APJII) mengatakan ada sekitar 49 % dari 5.900 *netizen* yang pernah menjadi sasaran *cyberbullying.* Dari 49 % tersebut terdapat 3,6% orang yang melaporkannya[12].

Berdasarkan latar belakang tersebut, dengan semakin banyaknya kejahatan siber, salah satunya pada bagian *Cyberbullying* maka penelitian ini dilakukan untuk melakukan analisis kinerja dari dua aplikasi atau *tools mobile forensic* dengan memanfaatkan metode atau kerangka kerja *National Institute of Standard and Technology* (NIST). Hasil analisa *log chat* pada *smartphone* dan aplikasi WhatsApp yang digunakan untuk melakukan kejahatan *cyberbullying* tersebut dapat membantu merekomendasikan *tools* mana yang lebih efektif dan dapat menjadi alternatif referensi dalam proses pengungkapan barang bukti digital pada kejahatan siber[13].

2. METODE PENELITIAN

Penelitian ini akan menggunakan metode atau *framework* dari NIST untuk mendapatkan bukti digital. Metode ini digunakan untuk mendapatkan alur atau langkah-langkah secara sistematis dan jelas. Adapun alur dari NIST ini ditunjukkan oleh Gambar 1[14].



Gambar 1. Metode NIST

a. *Collection*, merupakan tahap peneliti mengumpulkan barang bukti fisik dan digital serta menjaga kondisi objek agar sama dengan kondisi saat ditemukan, misalnya jika ditemukan dalam kondisi masih beroperasi (*on*) maka kondisi objek tetap dalam keadaan beroperasi saat proses akuisisi data. Kemudian barang bukti digital yang didapatkan dikenakan prosedur pengawasan agar tidak terjadi perubahan.

b. *Examination*, pada tahap ini peneliti melakukan pencarian data secara sistematis dari bukti digital yang berhubungan dengan skenario kasus pada penelitian ini. Hasil dari tahap ini adalah data-data sesuai variabel yang sudah ditentukan sebelumnya.

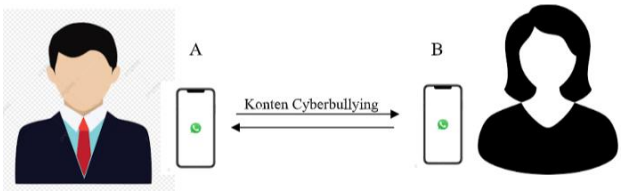
c. *Analysis*, pada tahap ini peneliti melakukan analisis terhadap bukti digital yang telah ditemukan, dan dapat menggambarkan kesimpulan yang didapat untuk dijadikan barang bukti kasus *Cyberbullying*.

d. *Reporting* merupakan tahap di mana peneliti akan melakukan dokumentasi seluruh hasil yang didapatkan dari proses yang telah dilakukan.

Penelitian ini menggunakan barang bukti yang disesuaikan dengan skenario dan tidak diambil dari tindak kejahatan yang sebenarnya. Barang bukti digital yang digunakan disesuaikan dengan skenario kasus yang relevan secara umum mengenai tindak kejahatan kriminal melalui media digital.

Penelitian ini menggunakan skenario kasus yang didapatkan dengan melakukan simulasi kasus kejahatan *cyberbullying*

dan kemudian data simulasi tersebut akan dikenakan proses *forensic* menggunakan beberapa *tools* dan kemudian hasilnya akan dibandingkan. Penelitian ini diawali dengan mempersiapkan skenario kasus dimulai dari melakukan percakapan melalui aplikasi WhatsApp antara akun Pelaku dan akun korban melalui kejahatan *cyberbullying*. Ilustrasi skenario ditunjukkan pada Gambar 2.



Gambar 2. Ilustrasi Skenario Percakapan

Penentuan akurasi *tools* dapat ditunjang oleh beberapa parameter yang menjadi variabel penelitian, maka peneliti menentukan fokus pada beberapa variabel yang menjadi bahan perbandingan untuk hasil dari penelitian ini[15]. Adapun variabelnya dapat dilihat pada Tabel 1.

Tabel 1. Variabel Skenario Akurasi

No	Variabel skenario hasil
1	Mengirim pesan teks
2	Mengirim pesan suara
3	Mengirim pesan gambar
4	Mengirim pesan video
5	Foto *profile*
6	Histori panggilan
7	Daftar Kontak
8	Nomor kontak
9	*Database file*
10	WhatsApp *Logs*
11	Menarik / menghapus pesan

3. HASIL DAN PEMBAHASAN

3.1. *Collection*

Tahap *collection* adalah tahap di mana peneliti mengumpulkan barang bukti dari *smartphone* yang dijadikan objek penelitian dan melakukan dokumentasi. Peneliti menggunakan *smartphone* Samsung Galaxy J2 sebagai properti untuk melakukan skenario *cyber bullying* melalui aplikasi *instant messanger* WhatsApp. *Smartphone* tersebut dalam kondisi normal atau tidak dalam kondisi *root*. Kondisi dan keterangan *smartphone* ditunjukkan pada Gambar 3 dan Tabel 2.

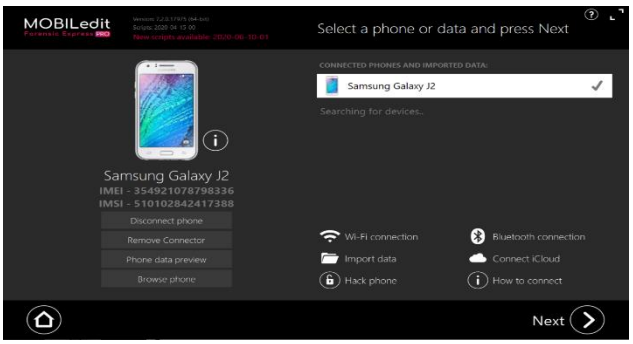
Gambar 3. Barang Bukti Fisik

Tabel 2. Informasi Objek

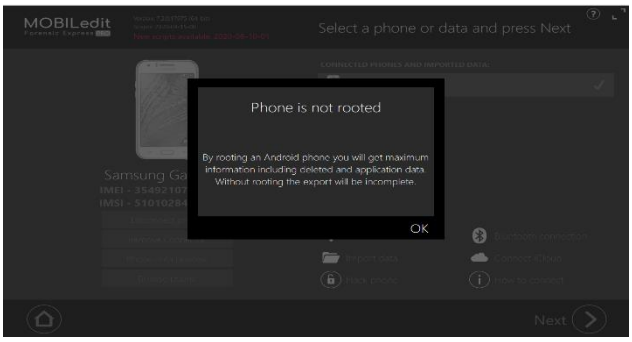
Informasi Perangkat	Spesifikasi
Samsung Galaxy	J2 2015
Nomor model	SM-J200G
Nomor versi	LMY47XJ200GDDU*****
Versi android	5.1.1
Processor	Quad-core 1.3 GHz Cortex-A7
RAM	1GB
ROM	8GB
Imei	3549210***** / 01

3.2. *Examination*

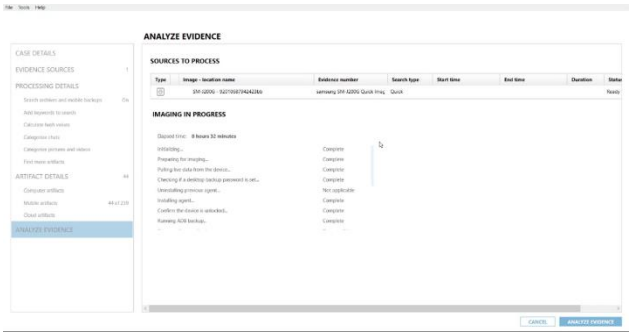
Tahap *Examination* adalah tahap di mana peneliti melakukan pemeriksaan menggunakan *tools* MOBILedit Forensic Express dan Magnet Axiom dimana *tools* ini dapat melakukan ekstraksi data dan *imaging* data dari *smartphone* karena mendukung berbagai bentuk *image*. *Tools* ini memungkinkan pengguna untuk bisa memilih data apa saja yang diperlukan untuk menunjang kebutuhan analisis pada kasus yang sedang dikerjakan, sehingga tidak perlu melakukan *backup* keseluruhan ponsel. Hal ini dapat mempersingkat waktu untuk melakukan forensik pada *smartphone* tersebut. Proses *examination* menggunakan aplikasi MobilEdit ditunjukkan pada Gambar 4 dan Gambar 5. Sedangkan proses *examination* menggunakan aplikasi Magnet Axiom ditunjukkan pada Gambar 6.



Gambar 4. *Examination* Menggunakan Mobiledit Forensic Express



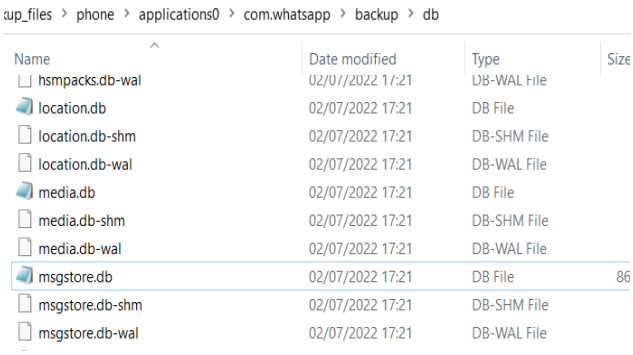
Gambar 5. Objek dalam Keadaan *Un-rooted* pada MOBILedit



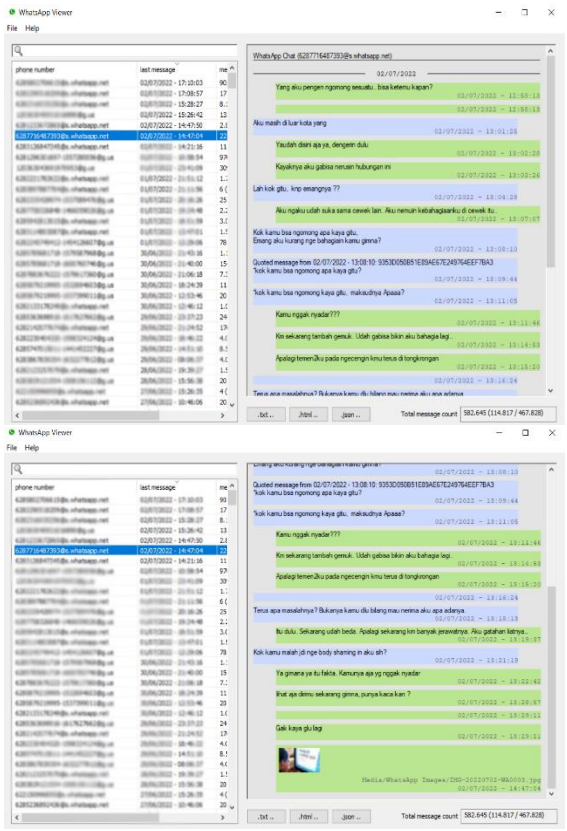
Gambar 6. *Examination* Menggunakan Magnet Axiom

3.3. *Analysis*

Tahap *analysis* adalah tahap di mana peneliti melakukan proses ekstraksi pada *file database*s msgstore.db yang sudah tidak dalam keadaan *encrypted*. Letak folder dan *file database*-nya ditunjukkan pada Gambar 7, sedangkan *database* percakapan Whatsapp yang diakses menggunakan Whatsapp *Viewer* ditunjukkan pada Gambar 8.



Gambar 7. *File Database* Percakapan Whatsapp



Gambar 8. *Database* Percakapan Dibuka Menggunakan Whtasapp *Viewer*

3.4. *Reporting*

Tahap *reporting* adalah tahap di mana hasil dari proses pemeriksaan dan analisis dimuat dalam laporan hasil investigasi. Hasil analisis dimuat dalam Tabel 3 dan Tabel 4.

Tabel 3. Perbandingan Hasil Temuan Artefak

Jumlah Artefak MobilEedit Forensic Express	Jumlah Artefak Magnet Axiom
File database (21)	*File database* (21)
File gambar (3203)	*File* gambar (3203)
File video (52)	*File* video (52)
File voice note (105)	*File voice note* (106)
Foto *Profile* (0)	Foto profil (968)
Data kontak (6492)	Data kontak (6493)
Data percakapan (1386)	Data percakapan (1396)
Data *logs* (6)	Data *logs* (6)

Tabel 4. Perbandingan Hasil Akhir

No	Variabel skenario hasil	MobilEedit Forensic Express	Magnet Axiom
1	Mengirim pesan teks	Ada	Ada
2	Mengirim pesan suara	Ada	Ada
3	Mengirim pesan gambar	Ada	Ada
4	Mengirim pesan video	Ada	Ada
5	Foto *profile*	Tidak ada	Ada
6	Histori panggilan	Tidak ada	Tidak ada
7	Daftar Kontak	Ada	Ada
8	Nomor kontak	Ada	Ada
9	*Database file*	Ada	Ada
10	WhatsApp *Log*	Ada	Ada
11	Menarik/menghapus pesan	Tidak ada	Tidak ada

Berdasarkan tabel perbandingan hasil artefak, maka dapat ditentukan kinerja dari kedua *tools* tersebut menggunakan rumus :

$$Par = \frac{\sum ar0}{\sum arT} x\ 100\%$$

Keterangan :

Par adalah angka indeks akurasi alat *forensic*,

ar0 adalah jumlah variabel yang ditemukan,

arT adalah jumlah keseluruhan variabel yang ada dalam skenario. Menggunakan rumus tersebut, maka dapat dihitung hasil skor dari kedua *tools*:

MOBILedit Forensic Express yaitu $Par = \frac{8}{11} x\ 100\% = 72{,}7\%$

Magnet Axiom yaitu $Par = \frac{9}{11} x\ 100\% = 81{,}8\%$

Hasil perhitungan tersebut menunjukkan bahwa akurasi kinerja MOBILedit Forensic Express sebesar 72,7% dan akurasi kinerja Magnet Axiom sebesar 81,8% berdasarkan variabel yang telah ditentukan

4. KESIMPULAN

Hasil penelitian ini menunjukkan bahwa prosedur *forensic* digital menggunakan metode *National Institute of Standards and Technology* (NIST) dengan *tools* MOBILedit Forensics Express dan Magnet Axiom berhasil melakukan ekstraksi barang bukti digital dari objek *smartphone* dengan baik. Kinerja kedua *tools* tersebut diukur dari tingkat keberhasilan dalam melakukan *recovery* bukti digital. Tingkat keberhasilan Magnet Axiom lebih unggul dengan akurasi 81,8% dibandingkan MOBILedit Forensics Express dengan akurasi sebesar 72,7% berdasarkan perhitungan variabel-variabel yang sudah ditentukan pada penelitian ini. Berdasarkan hasil forensik yang dilakukan pada skenario percakapan yang dilakukan, kedua *tools* tersebut tidak berhasil mengembalikan pesan yang telah dihapus, hal ini terjadi karena keadaan objek dalam kondisi *Un-rooted*. Berdasarkan isi pesan pada percakapan pelaku dan korban, ditemukan bukti tindak *Cyberbullying* dengan jenis *body shaming* atau ejekan terhadap kondisi fisik korban.

DAFTAR PUSTAKA

[1] A. Siwi, F. Utami, and N. Baiti, "Pengaruh Media Sosial Terhadap Perilaku Cyber Bullying Pada Kalangan RSiwi, A., Utami, F., & Baiti, N. (2018). Pengaruh Media Sosial Terhadap Perilaku Cyber Bullying Pada Kalangan Remaja. 18(2), 257–262.emaja," vol. 18, no. 2, pp. 257–262, 2018, [Online].Available: http://ejournal.bsi.ac.id/ejurnal/index.php/cakrawala%0APengaruh.

[2] A. D. Riyanto, "Hootsuite (We are Social)_ Indonesian Digital Report 2022," 2022. https://andi.link/hootsuite-we-are-social indonesian-digital-report-2022/.

[3] Pratomo. Yudha, "49 Persen Netizen di Indonesia Pernah Mengalami 'Bullying' di Medsos," *Kompas.Com*. 2019, [Online]. Available: https://amp.kompas.com/tekno/read/2019/05/16/08290047/49-persen-netizen-di-indonesia-pernah-mengalami-bullying-di-medsos.

[4] A. Yudhana, I. Riadi, and I. Anshori, "Analisis Bukti Digital Facebook Messenger Menggunakan Metode Nist," *It J. Res. Dev.*, vol. 3, no. 1, pp. 13–21, 2018, doi: 10.25299/itjrd.2018.vol3(1).1658.

[5] Z. S. Daulay dan R. Indrayani, "Analisis Keamanan Browser Dalam Bersosial Media Menggunakan Metode Institute Of Justice (NIJ)," *Djtechno: Journal of Information Techhnology Research*, vol. 3, no. 2, hlm. 167, Des 2022, doi: 10.46576/djtechno.v3i2.2598

[6] I. Riadi, R. Umar, and I. M. Nasrulloh, "Analisis Forensik Digital Pada Frozen Solid State Drive Dengan Metode National Institute of Justice (Nij)," *Elinvo (Electronics, Informatics, Vocat. Educ.*, vol. 3, no. 1, pp. 70–82, 2018, doi: 10.21831/elinvo.v3i1.19308.

[7] A. Leonardo dan R. Indrayani, "The Comparison Performance of Digital Forensic Tools Using Additional Root Access Options," *Jurnal Ilmiah Teknik Elektro Komputer dan Informatika*, vol. 7, no. 3, hlm. 512, Jan 2022, doi:

10.26555/jiteki.v7i3.22381.

[8] H. Nurhairani and I. Riadi, "Analysis Mobile Forensics on Twitter Application using the National Institute of Justice (NIJ) Method," *Int. J. Comput. Appl.*, vol. 177, no. 27, pp. 35–42, 2019, doi: 10.5120/ijca2019919749.

[9] N. Nasirudin, S. Sunardi, and I. Riadi, "Analisis Forensik *Smartphone* Android Menggunakan Metode NIST dan Tool MOBILedit Forensic Express," *J. Inform. Univ. Pamulang*, vol. 5, no. 1, p. 89, 2020, doi: 10.32493/informatika.v5i1.4578.

[10] A. Yudhana, I. Riadi, and I. Anshori, "Identification of Digital Evidence Facebook Messenger on Mobile Phone With National Institute of Standards Technology (Nist) Method," *Kursor*, vol. 9, no. 3, 2019, doi: 10.28961/kursor.v9i3.152.

[11] I. Anshori, K. E. Setya Putri, and U. Ghoni, "Analisis Barang Bukti Digital Aplikasi Facebook Messenger Pada *Smartphone* Android Menggunakan Metode NIJ," *IT J. Res. Dev.*, vol. 5, no. 2, pp. 118–134, 2020, doi: 10.25299/itjrd.2021.vol5(2).4664.

[12] R. A. Bintang, R. Umar, and A. Yudhana, "Analisis Media Sosial Facebook Lite dengan *tools* Forensik menggunakan Metode NIST," *Techno (Jurnal Fak. Tek. Univ. Muhammadiyah Purwokerto)*, vol. 21, no. 2, p. 125, 2020, doi: 10.30595/techno.v21i2.8494.

[13] Imam Riadi, Sunardi, and P. Widiandana, "Investigating *Cyberbullying* on WhatsApp Using Digital Forensics Research Workshop," *J. RESTI (Rekayasa Sist. dan Teknol. Informasi)*, vol. 4, no. 4, pp. 730–735, 2020, doi: 10.29207/resti.v4i4.2161.

[14] I. Riadi, R. Umar, and A. Firdonsyah, "Forensic *tools* performance analysis on android-based blackberry messenger using NIST measurements," *Int. J. Electr. Comput. Eng.*, vol. 8, no. 5, pp. 3991–4003, 2018, doi: 10.11591/ijece.v8i5.pp3991-4003.

[15] N. Saputri dan R. Indrayani, "ANALISIS DATA FORENSIK INVESTIGASI KASUS PEREDARAN NARKOBA PADA SMARTPHONE BERBASIS ANDROID," *Djtechno: Journal of Information Techhnology Research*, vol. 3, no. 2, hlm. 156, Des 2022, doi: 10.46576/djtechno.v3i2.2597.