

# Analisis Forensik *Cyberbullying* pada Aplikasi IMO Messenger Menggunakan Metode *Association of Chief Police Officers*

## *Forensics Investigation Analysis of Cyberbullying on IMO Messenger Services Using Association of Chief Police Officers Method*

Imam Riadi<sup>1</sup>, Sunardi<sup>2</sup>, Yana Safitri<sup>3</sup>

<sup>1,2,3</sup> Universitas Ahmad Dahlan

[imam.riadi@is.uad.ac.id](mailto:imam.riadi@is.uad.ac.id)<sup>1</sup>, [sunardi@mti.uad.ac.id](mailto:sunardi@mti.uad.ac.id)<sup>2</sup>, [yana2107048011@webmail.uad.ac.id](mailto:yana2107048011@webmail.uad.ac.id)<sup>3</sup>

### Informasi Artikel:

Diterima: 17 Mei 2023, Direvisi: 02 Juni 2023, Disetujui: 22 Juni 2023

---

#### Abstrak-

**Latar Belakang:** Perkembangan teknologi komputer meningkat sangat pesat. Hal ini memiliki dampak positif dan negatif. Salah satu dampak negatifnya adalah banyak dilakukan tindakan *cyberbullying*. Hal semacam inilah yang kemudian dimanfaatkan oleh sejumlah orang untuk melakukan aksi *bullying* di media sosial salah satunya pada aplikasi IMO Messenger.

**Tujuan:** Tujuan penelitian ini untuk menginvestigasi kejahatan *cyberbullying* melalui bukti-bukti yang akan ditemukan.

**Metode:** Metode yang digunakan pada penelitian ini adalah *Association of Chief Police Officers* (ACPO). Metode ACPO dalam investigasi IMO Messenger memiliki empat tahapan yaitu *Plan, Capture, Analysis, dan Present*. Data digital berupa 16 teks percakapan, 29 user ID, 6 data terhapus, dan grup yang digunakan sebagai parameter dalam proses penelitian. Pengujian dilakukan dengan menggunakan alat MOBILEdit Forensic Express.

**Hasil:** Hasil penelitian ini memperoleh data digital 100% untuk teks percakapan, user ID, dan grup, sedangkan 0% untuk data yang dihapus

**Kesimpulan:** Metode ACPO dapat membantu dalam proses penyelidikan kasus *cyberbullying* pada aplikasi IMO.

**Kata Kunci:** Cyberbullying, Forensik Digital, Forensik Mobile, IMO Messenger.

---

#### Abstract-

**Background:** The development of computer technology has increased very rapidly. This has both positive and negative impacts. One of the negative impacts is that many acts of cyberbullying are carried out. This kind of thing is then used by a number of people to carry out acts of bullying on social media, one of which is the IMO Messenger application.

**Objective:** The purpose of this study is to investigate cyberbullying crimes through the evidence that will be found.

**Methods:** The method used in this study is the Association of Chief Police Officers (ACPO). The ACPO method in the Imo Messenger investigation has four stages, namely Plan, Capture, Analysis, and Present. Digital data in the form of 16 text conversations, 29 user IDs, 6 deleted data, and groups used as parameters in the research process. Testing was carried out using the MOBILEdit Forensic Express tool.

**Result:** The results of this study obtained 100% digital data for text conversations, user IDs and groups, while 0% for deleted data.

**Conclusion:** The ACPO method can assist in the process of investigating cyberbullying cases on IMO applications

**Keywords:** Cyberbullying, Digital Forensics, Mobile Forensics, IMO Messenger.

---

#### Penulis Korespondensi:

Yana Safitri,

Master Program of Informatics, Universitas Ahmad Dahlan, Yogyakarta, Indonesia,

Email: [yana2107048011@webmail.uad.ac.id](mailto:yana2107048011@webmail.uad.ac.id)

---

**How to Cite:** I. Riadi, S. Sunardi, and Y. Safitri, "Analisis Forensik Cyberbullying pada Aplikasi IMO Messenger Menggunakan Metode Association of Chief Police Officers" *Jurnal Bumigora Information Technology (BITe)*, vol. 5, no. 1, pp. 1~8, 2023.

This is an open access article under the CC BY-SA license (<https://creativecommons.org/licenses/by-sa/4.0/>)

## 1. PENDAHULUAN

Akses internet dapat dilakukan kapan saja, oleh siapapun, kapanpun dan dimanapun [1]. Beragamnya informasi yang ditawarkan [2], kebebasan menjalin hubungan pertemanan, dan kebebasan berpendapat di seluruh dunia membuat ekspos media semakin besar karena setiap orang memiliki kepentingannya masing-masing. Selain memiliki dampak negatif, internet juga memiliki dampak positif [3]. Perkembangan internet juga didasari oleh *smartphone* yang semakin canggih saat ini semakin memudahkan masyarakat untuk mengakses informasi dan dengan mudah menggunakan media sosial [4]. Manusia adalah makhluk sosial yang memiliki kebutuhan untuk berkomunikasi dan berinteraksi dengan sesama manusia [5]. Pengguna media sosial yang semakin banyak akan membuka peluang terjadinya kejahatan dunia maya. *Cybercrime* merupakan kejahatan media sosial yang memanfaatkan kecanggihan teknologi internet [6]. *Cybercrime* merupakan kejahatan yang terjadi di dunia maya, dimana salah satu kejahatan dunia maya yang paling banyak terjadi adalah *cyberbullying* yang dilakukan pada remaja [7, 8]. *Bullying* merupakan salah satu tindakan di mana satu atau lebih orang mencoba menyakiti atau mengendalikan orang lain dengan cara kekerasan [9]. Kejahatan di internet atau yang dikenal dengan *cybercrime* antara lain adalah praktek pornografi, penipuan *online*, maraknya kejahatan yang dilakukan oleh *hacker*, dan *cyberbullying* [10]. Hal semacam inilah yang kemudian dimanfaatkan oleh sejumlah orang untuk melakukan aksi *bullying* di media sosial yang banyak merugikan pihak yang di-*bully*. Kasus *bullying* saat ini banyak dilakukan di hampir semua media sosial, salah satunya adalah aplikasi IMO Messenger yang memiliki fitur personal *chat* sebagai sarana untuk melakukan kejahatan. Selain berfungsi sebagai alat untuk berkirim pesan atau *chatting*, pengguna IMO Messenger juga dapat mengetahui dan mengatur banyak akun menggunakan IMO Messenger. Jika perangkat pengguna menggunakan teknologi NFC, maka IMO Messenger juga dapat digunakan sebagai alat untuk mengirim data ke perangkat lain yang lebih kompatibel. Fitur menarik dan jaminan keamanan data yang ditawarkan oleh aplikasi pesan instan menjadi faktor utama yang mempengaruhi jumlah pengguna aplikasi ini [11].

Forensik digital merupakan ilmu yang digunakan untuk pembuktian hukum, dalam kasus ini pembuktian kejahatan komputer secara ilmiah untuk mendapatkan bukti digital yang valid [12]. Bukti digital merupakan hasil pemulihan data dokumen, akun email, kontak, obrolan teks, file media (suara/gambar/video) atau file log [13]. Forensik digital memiliki banyak cabang [14], salah satunya adalah forensik mobile berkaitan dengan pemulihan bukti atau data digital dari perangkat seluler dalam kondisi forensik yang sehat [15]. Dalam dunia forensik digital banyak menggunakan *tools* yang dapat memudahkan investigasi [16]. Mobile forensic merupakan cabang dari forensik digital yang berhubungan dengan ekstraksi barang bukti digital atau data dari perangkat seluler dalam kondisi forensik yang baik [17]. Mobile Forensic adalah cara untuk memulihkan bukti digital dari perangkat seluler menggunakan prosedur forensik. IMO Messenger dan fitur keamanan yang ada memungkinkan penyadapan percakapan IMO Messenger sebagai bukti di pengadilan. Hal ini menunjukkan bahwa dari segi penyelidikan forensik, aplikasi IMO Messenger dapat menyimpan data bukti yang dapat digunakan di pengadilan sebagai barang bukti. Mobile Forensik adalah ilmu yang berasal dari forensik digital atau lebih dikenal dengan forensik komputer [18].

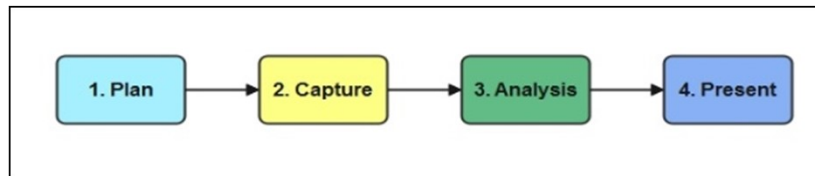
Penelitian sebelumnya yang serupa bertujuan untuk mengetahui nilai kerentanan instan messanging Skype, WA, dan Telegram berbasis web dari hasil komparatif teknologi anti forensiknya masing-masing aplikasi tersebut menggunakan metode ACPO. Penelitian tersebut menggunakan tools FTK Imager dan Fiddler [19]. Penelitian lainnya juga melakukan investigasi bukti digital dalam mengungkap *cybercrime*. Perangkat yang digunakan dalam penelitian adalah Flash Disk SanDisk Cruzer Blade 8GB SDC250-008B B1180724954B. Penelitian dilakukan dengan tiga perlakuan berbeda, yaitu tanpa dilakukan penghapusan atas file-file simulasi diperoleh hasil seluruh file simulasi terdeteksi, menghapus permanen (shift+delete) seluruh file simulasi diperoleh hasil seluruh file simulasi terdeteksi sekaligus dengan file-file yang pernah ada dalam flash disk sebelum dilakukan format ulang, dan menghapus permanen (shift+delete) seluruh file serta membuat *password flash disk* dengan *tools* bawaan Windows 10 BitLocker Drive Encryption tidak terdeteksi file apapun [20]. Pada penelitian yang lain juga melakukan investigasi *cyberbullying* pada WA. Penelitian tersebut dilakukan untuk menemukan barang bukti *cyberbullying* dengan kerangka kerja *Digital Forensics Research Workshop* (DFRWS). Penelitian

melakukan akuisisi untuk mengungkap bukti digital pada pelaku di fitur grup berupa teks menggunakan MOBILEdit Forensic Express [21]. Penelitian lainnya juga melakukan ekstraksi file steganografi menggunakan Framework DFRWS. Penelitian melakukan analisis bukti digital menggunakan metode static forensic dengan menerapkan enam tahapan pada DFRWS serta melakukan ekstraksi berdasarkan skenario kasus yang melibatkan kejahatan digital. Penelitian tersebut menggunakan perangkat Laptop Acer Aspire E1-431,4 GB DDR 3 Memory, 500 GB HDD [22]. Pada penelitian selanjutnya, dilakukan analisis media sosial Facebook Lite dan didapatkan berupa akun yang digunakan, audio, percakapan, dan gambar [23].

Perbedaan penelitian ini dengan penelitian sebelumnya yaitu objek penelitian yang dianalisis yaitu forensik cyberbullying pada aplikasi IMO messenger dan metode yang digunakan pada penelitian ini yaitu association of chief police officers. Tujuan penelitian ini adalah untuk menghasilkan alat bukti digital berupa percakapan pada aplikasi IMO untuk memperkuat pembuktian perkara pidana di pengadilan berupa hasil analisis alat bukti digital. Sehingga dengan adanya penelitian ini dapat bermanfaat untuk analisis forensik cyberbullying.

## 2. METODE PENELITIAN

Metode *Association of Chief Police Officers* (ACPO) merupakan suatu metode penelitian dengan 4 dasar elemen kunci yang terdiri dari identifikasi, mengamankan bukti, analisa dan pemaparan atau presentasi. Skema tahapan-tahapan penelitian metode ACPO ditunjukkan pada Gambar 1.



Gambar 1. Tahapan ACPO.

Berdasarkan Gambar 1. dapat diketahui bahwa ACPO memiliki beberapa tahapan penelitian. Tahapan-tahapan tersebut dijelaskan sebagai berikut:

1. Plan : Tahapan dimana rancangan segala sesuatu yang dilakukan dalam proses penelitian dipersiapkan.
2. Capture: Tahap dimana hasil penelitian disimpan untuk kemudian dilanjutkan dengan tahap analisis menggunakan hasil tersebut.
3. Analisis: Tahap dimana analisis dilakukan dengan menggunakan parameter hasil yang telah diperoleh dari tahap sebelumnya.
4. Present: tahap dimana data hasil analisis pada tahap sebelumnya disajikan sehingga dapat diketahui oleh publik.

Penelitian yang akan dilakukan tentunya membutuhkan alat dan bahan penelitian. Hal ini perlu dipersiapkan agar proses penelitian dilakukan tanpa hambatan. Alat dan bahan yang dibutuhkan dalam penelitian bisa dilihat pada Tabel 1.

Tabel 1. Bahan penelitian.

Alat dan Bahan	Deskripsi
Samsung Galaxy Core 2	Android Oreo, Sebagai Objek Penelitian
Laptop Acer Aspire E14	Core i3, RAM 4 GB
IMO Messenger	Perangkat lunak
Kabel USB	Smartphone Konektor
MOBILEdit Forensic Express	Alat Forensik
Super SU	Rooting

Tabel 1. Menyebutkan alat dan bahan yang digunakan antara lain smartphone Samsung Galaxy Core 2, laptop Acer Aspire E 14 core i3 dan konektor USB. *Software* pendukung penelitian forensik ini adalah aplikasi IMO *Messenger* dan menggunakan tool MOBILEdit Forensic Express. Smartphone yang digunakan harus di-root terlebih dahulu untuk memudahkan mendapatkan data dari perangkat Android.

Penelitian ini menggunakan skenario yang telah disiapkan oleh peneliti. Skenario kasus adalah kasus *cyberbullying* yang terjadi antara satu pelaku dan satu korban. Dalam kasus ini, pelaku berada dalam skenario antara dua orang yang sedang melakukan percakapan yang mengarah pada *cyberbullying* terhadap korban dengan menggunakan aplikasi IMO Messenger. Skenario dibuat menggunakan smartphone Samsung Galaxy Core 2 sebagai *smartphone* korban. Kondisi dalam skenario adalah korban dan pelaku adalah teman sekolah. Mula-mula korban menanyakan bagaimana keadaannya, kemudian pelaku menjawab dengan merujuk pada *cyberbullying* dengan membicarakan keburukan fisik korban. Korban merasa tersinggung dengan perkataan pelaku dalam percakapan tersebut, kemudian korban melapor kepada pihak berwajib. Kasus ini menggunakan satu alat sebagai alat bukti dalam kasus kejahatan.



Gambar 2. Skenario penelitian.

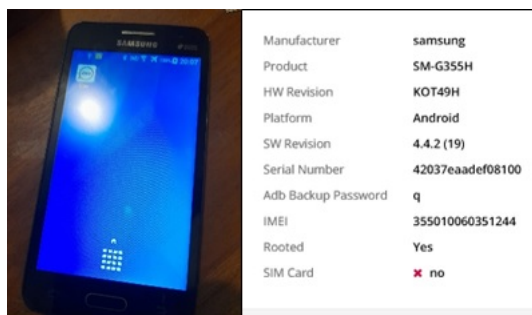
Gambar 2. menjelaskan bahwa penyidik mendapatkan barang bukti atau bukti dalam percakapan *chat*. Diketahui korban sempat melakukan percakapan melalui grup chat IMO Messenger. Penyidik mengamankan barang bukti digital berupa *smartphone* milik korban. Barang bukti berupa *smartphone* yang diperoleh kemudian dilakukan penelitian dengan menggunakan alat MOBILEdit Forensic Express. Hasil proses akuisisi digunakan sebagai dasar untuk menentukan hasil penelitian.

### 3. HASIL DAN PEMBAHASAN

Hasil penelitian dengan menggunakan metode ACPO memiliki 4 tahapan yaitu *Plan, Capture, Analysis, dan Present*.

#### 3.1. Plan

Tahapan ini pertama-tama dilakukan dengan rencana yang tersusun secara detail berkaitan dengan langkah-langkah yang akan dilakukan dalam proses penelitian antara lain membuat skenario penelitian dan menyiapkan bahan dan alat penelitian. Penelitian ini berhasil mengidentifikasi *smartphone* Samsung Galaxy Core 2 dengan berbagai spesifikasi seperti Android Oreo sebagai sistem operasinya. Spesifikasi rinci ditunjukkan pada Gambar 3.



Gambar 3. Spesifikasi bukti.

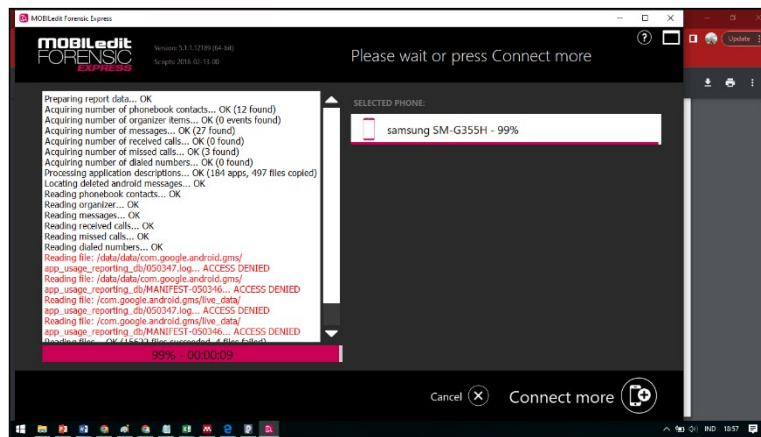
Parameter penelitian diambil dari data digital aplikasi IMO Messenger berupa Pesan *Teks, user ID, Data yang dihapus, dan Grup* bisa dilihat pada Tabel 2.

Tabel 2. Data digital IMO

Tipe Data	Jumlah Data
Pesan Teks	16
User ID	29
Data Hapus	6
Grup	1

### 3.2. Capture

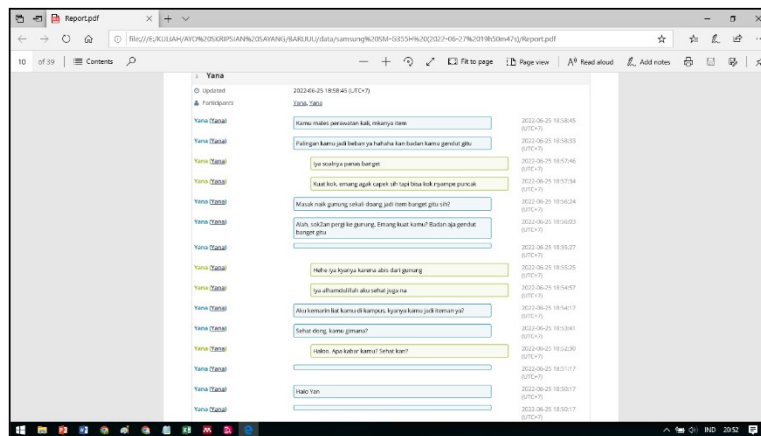
Tahap *Capture* merupakan tahap penyimpanan atau pendokumentasian semua data digital yang diperoleh dari proses akuisisi, kemudian data tersebut dikelompokkan sesuai jenis data masing-masing. Data digital tersebut merupakan hasil dari *physical memory capture* menggunakan MOBILEdit Forensic Express bisa dilihat pada Gambar 4.



Gambar 4. Capture dengan MOBILEdit Forensics.

### 3.3. Analysis

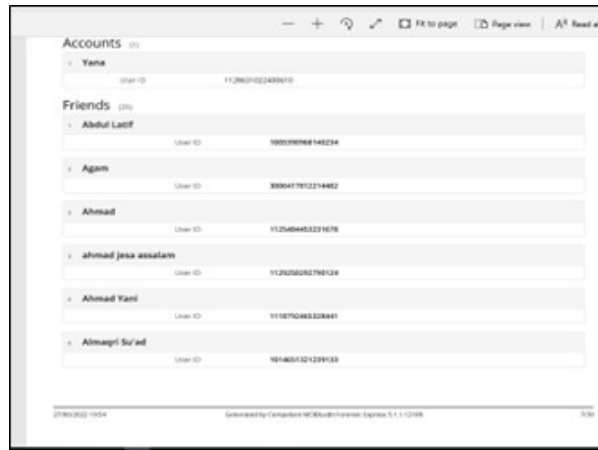
Tahapan ini merupakan proses analisis ekstrak file MOBILEdit Forensic Express seperti pada Gambar 5.



Gambar 5. Hasil Ekstrak MOBILEdit Forensic Express Text Message Data.

Gambar 5. MOBILEdit Forensic Express berhasil mengekstrak data pesan teks dari aplikasi IMO *Messenger*. Tahap analisis tidak hanya mampu memperoleh teks pesan tetapi juga data digital berupa User ID pada aplikasi IMO *Messenger* yang bisa dilihat pada Gambar 6.

Hasil yang diperoleh dari proses ekstrak kemudian dianalisis untuk mendapatkan data digital dari aplikasi IMO *Messenger*. Data digital berupa chat yang ditemukan pada proses analisis telah membuktikan bahwa MOBILEdit Forensic Express mampu memperoleh data digital dari aplikasi IMO *Messenger*.



Gambar 6. Data digital user ID di MOBILEedit Forensics Express.

### 3.4. Present

Penelitian ini menentukan nilai kerentanan teknologi anti forensik aplikasi IMO *Messenger* dengan menggunakan perhitungan indeks berdasarkan jumlah data yang diperoleh. Rumus perhitungan nilai kerentanan teknologi anti forensik aplikasi IMO *Messenger* menggunakan persamaan *unweighted index* seperti yang dapat ditunjukkan pada persamaan (1).

$$Pon = \frac{\sum pn}{\sum po} \times 100\% \quad (1)$$

Dimana:

$Pon$  : persentase skor kerentanan aplikasi anti forensik aplikasi pesan instan.

$\sum pn$  : jumlah data digital yang berhasil diperoleh.

$\sum po$  : total data digital aplikasi instant messenger.

Tabel 3. Hasil akuisisi.

Tipe Data	Jumlah Data Awal	Jumlah Perolehan Data	Tingkat Keberhasilan (%)
Pesan Teks	16	16	100
User ID	29	29	100
Data Hapus	6	0	0
Grup	1	1	100

Tabel 3. merupakan hasil akuisisi data digital aplikasi IMO *Messenger*, hasil akuisisi data digital menjadi dasar penentuan nilai anti kerentanan teknologi forensik dari aplikasi. Tabel 3. merupakan keseluruhan data digital dari aplikasi IMO Messenger, berdasarkan data digital terlihat bahwa keberhasilan 100% untuk Pesan Teks, User ID, dan Grup, sedangkan Data Hapus diperoleh sebesar 0%. Merujuk pada [23] dapat menampilkan berupa akun id, Image, Audio, dan Video pada saat menggunakan tool MOBILEedit Forensic, sedangkan pada penelitian ini memunculkan jumlah data yang diperoleh menggunakan tool MOBILEedit Forensic Express.

## 4. KESIMPULAN

Berdasarkan hasil analisis dan percobaan pada penelitian yang telah dilakukan membuktikan bahwa metode ACPO dapat mempermudah proses investigasi mulai dari pengangkatan barang bukti sampai dengan tahap pelaporan barang bukti. Berdasarkan hasil penelitian Analisis Forensik *Cyberbullying* pada Aplikasi IMO *Messenger* Menggunakan Metode ACPO, diperoleh bukti digital 100% berupa percakapan teks, user ID, dan grup, sedangkan data yang dihapus diperoleh di 0%. Hasil penelitian ini diharapkan menjadi acuan bagi pengembang dan pengguna aplikasi IMO *Messenger* untuk lebih memperhatikan keamanan data aplikasi. Penelitian selanjutnya diharapkan dapat menggunakan *tools* yang lebih banyak untuk dapat membandingkan hasil yang didapatkan, karena pada penelitian ini hanya menggunakan satu *tools* forensik.



**DAFTAR PUSTAKA**

- [1] J. Li, Y. Wu, and T. Hesketh, “Computers in Human Behavior Internet use and cyberbullying : Impacts on psychosocial and psychosomatic wellbeing among Chinese adolescents,” *Computers in Human Behavior*, vol. 138, no. February 2022, p. 107461, 2023.
- [2] M. Sari, I. Sembiring, and H. D. Purnomo, “Analisis Kualitas Layanan Jaringan Internet di Daerah Perbatasan Analysis of Frontier ’ s Internet Network Quality,” vol. 4, no. 2, pp. 205–216, 2022.
- [3] B. Fakiha, “Effectiveness of Forensic Firewall in Protection of Devices from Cyberattacks,” vol. 12, no. 1, pp. 77–82, 2022.
- [4] P. M. Nirmala Dharmapatni and N. L. P. Merawati, “Penerapan Algoritma Support Vector Machine Dalam Sentimen Analisis Terkait Kenaikan Tarif BPJS Kesehatan,” *Jurnal Bumigora Information Technology (BITe)*, vol. 2, no. 2, pp. 105–112, 2020.
- [5] S. R. Ardiningtias, “Forensik Digital Kasus Penyebaran Pornografi pada Aplikasi Facebook Messenger Berbasis Android Menggunakan Kerangka Kerja National Institute of Justice,” vol. 7, no. 3, pp. 322–328, 2021.
- [6] I. Riadi, A. Yudhana, S. Informasi, U. A. Dahlan, T. Elektro, F. T. Industri, U. A. Dahlan, T. Informatika, F. T. Industri, and U. A. Dahlan, “Forensik Mobile pada Layanan Media Sosial LinkedIn,” vol. 6, no. 1, pp. 9–20, 2021.
- [7] R. N. Dasmen, F. Kurniawan, T. Komputer, U. B. Darma, S. Inggris, U. B. Darma, and D. Forensik, “Digital Forensik Deleted Cyber Crime Evidence pada Pesan Instan Media Sosial,” vol. 20, no. 4, pp. 527–539, 2021.
- [8] O. C. Hang and A. S. Media, “Cyberbullying Lexicon for Social Media,” 2019.
- [9] M. Yao, C. Chelmiss, and D. S. Zois, “Cyberbullying ends here: Towards robust detection of cyberbullying in social media,” *The Web Conference 2019 - Proceedings of the World Wide Web Conference, WWW 2019*, pp. 3427–3433, 2019.
- [10] M. A. Al-Garadi, M. R. Hussain, N. Khan, G. Murtaza, H. F. Nweke, I. Ali, G. Mujtaba, H. Chiroma, H. A. Khattak, and A. Gani, “Predicting Cyberbullying on Social Media in the Big Data Era Using Machine Learning Algorithms: Review of Literature and Open Challenges,” *IEEE Access*, vol. 7, pp. 70 701–70 718, 2019.
- [11] K. Gibson, “Bridging the digital divide: Reflections on using WhatsApp instant messenger interviews in youth research,” *Qualitative Research in Psychology*, vol. 19, no. 3, pp. 611–631, 2022.
- [12] J. Son, Y. Woong, D. Bin, and K. Kim, “Forensic Science International : Digital Investigation Forensic analysis of instant messengers : Decrypt Signal , Wickr , and Threema,” *Forensic Science International: Digital Investigation*, vol. 40, p. 301347, 2022.
- [13] G. Fanani, I. Riadi, and A. Yudhana, “Analisis Forensik Aplikasi Michat Menggunakan Metode Digital Forensics Research Workshop,” *JURNAL MEDIA INFORMATIKA BUDIDARMA*, vol. 6, no. 2, p. 1263, apr 2022.
- [14] R. A. Ramadhan and D. Mualfah, “Implementasi Metode National Institute of Justice (NIJ) Pada Fitur TRIM SOLID STATE DRIVE (SSD) Dengan Objek Eksperimental Sistem Operasi Windows, Linux dan Macintosh,” *IT Journal Research and Development*, vol. 5, no. 2, pp. 183–192, 2020.
- [15] H. H. Lwin, W. P. Aung, and K. K. Lin, “Comparative Analysis of Android Mobile Forensics Tools,” *2020 IEEE Conference on Computer Applications, ICCA 2020*, pp. 1–6, 2020.

- [16] I. Riadi, “Analisis Forensik Smartphone Android Menggunakan Metode NIST dan Tool MOBILedit Forensic Express,” vol. 5, no. 1, pp. 89–94, 2020.
- [17] G. Humphries, R. Nordvik, H. Manifavas, P. Cobley, and M. Sorell, “Forensic Science International : Digital Investigation Law enforcement educational challenges for mobile forensics,” *Forensic Science International: Digital Investigation*, vol. 38, p. 301129, 2021.
- [18] T. Hermawan and L. Roselina, “Android Forensic Tools Analysis for Unsend Chat on Social Media,” pp. 233–238, 2021.
- [19] S. R. A. Muhammad Abdul Aziz, Wicaksono Yuli Sulisty, “Komparatif Anti Forensik Aplikasi Instant Messaging Berbasis Web Menggunakan Metode Association of Chief Police Officers ( ACPO ),” vol. 1, no. 1, pp. 8–15, 2021.
- [20] M. Riskiyadi, “Investigasi Forensik Terhadap Bukti Digital Dalam Mengungkap Cybercrime,” *Cyber Security dan Forensik Digital*, vol. 3, no. 2, pp. 12–21, 2020.
- [21] R. Sistem, S. S. Informasi, U. A. Dahlan, S. T. Elektro, U. A. Dahlan, P. Studi, T. Informatika, and U. A. Dahlan, “Investigasi Cyberbullying pada WhatsApp Menggunakan Digital Forensics,” vol. 1, no. 10, pp. 730–735, 2021.
- [22] S. Sunardi and I. Riadi, “Penerapan Metode Static Forensics untuk Ekstraksi File Steganografi,” no. June, 2020.
- [23] R. A. Bintang, R. Umar, and A. Yudhana, “Analisis Media Sosial Facebook Lite dengan tools Forensik menggunakan Metode NIST,” *Techno (Jurnal Fakultas Teknik, Universitas Muhammadiyah Purwokerto)*, vol. 21, no. 2, p. 125, 2020.