Jurnal Bumigora Information Technology (BITe)
Vol. 5, No. 1, Juni 2023, Hal. 1∼8
E-SSN: 2685-4066, DOI: 10.30812/bite/v5i1.2977

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[1], **Sunardi**[2], **Yana Safitri**[3]
[1,2,3] Universitas Ahmad Dahlan
imam.riadi@is.uad.ac.id[1], sunardi@mti.uad.ac.id[2], yana2107048011@webmail.uad.ac.id[3]

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

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.

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 mngetahui 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].

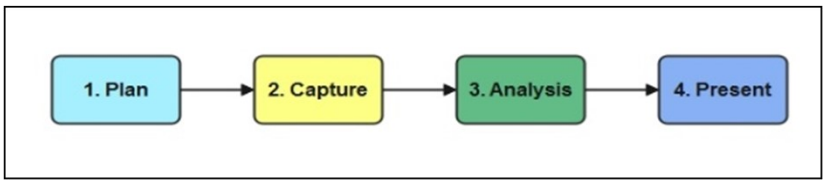
Penelitian sebelumnya yang serupa bertujuan untuk mengetahui nilai kerentanan instan messanging Skype, WA, dan Telegram berbasis web dari hasil komparatif teknologi anti forensiknya masing-masing aplikasi tersebut menggunakan metode ACPO. Penelitian tersebut menggunakan tools FTK Imager dan Fiddler [19]. 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.

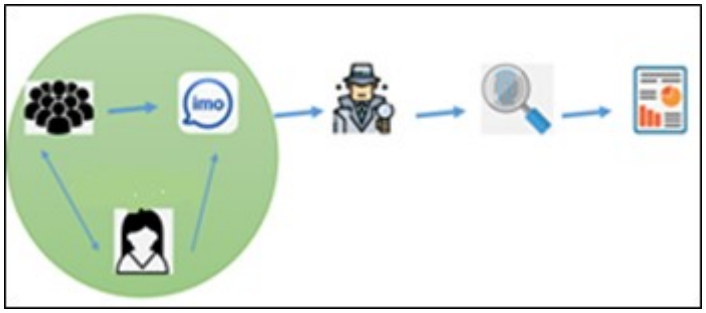
Penelitian yang akan dilakukan tentunya membutuhkan alat dan bahan penelitian. Hal ini perlu dipersiapkan agar proses penelitian dilakukan tanpa hambatan. Alat dan bahan yang dibutuhkan dalam penelitian bisa dilihat pada Tabel 1.

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.

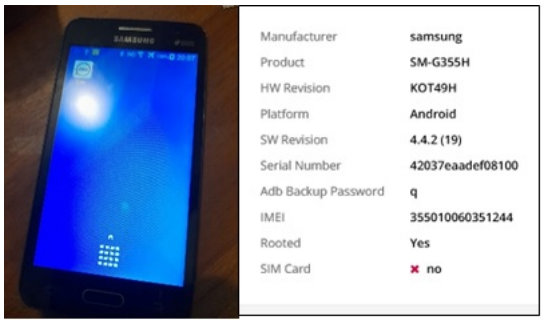
Gambar 2. menjelaskan bahwa penyidik mendapatkan barang bukti atau bukti dalam percakapan c*hat*. Diketahui korban sempat melakukan percakapan melalui grup chat IMO *Messenger*. Penyidik mengamankan barang bukti digital berupa *smartphone* milik korban. Barang bukti berupa *smartphone* yang diperoleh 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.

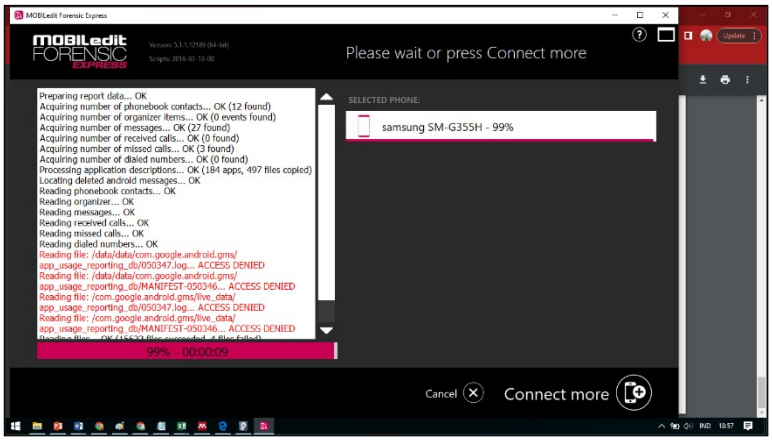
Parameter penelitian diambil dari data digital aplikasi IMO *Messenger* berupa Pesan *Teks*, *user* ID, Data yang dihapus, dan Grup bisa dilihat pada Tabel 2.

Tabel 2. Data digital IMO

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

3.2. *Capture*

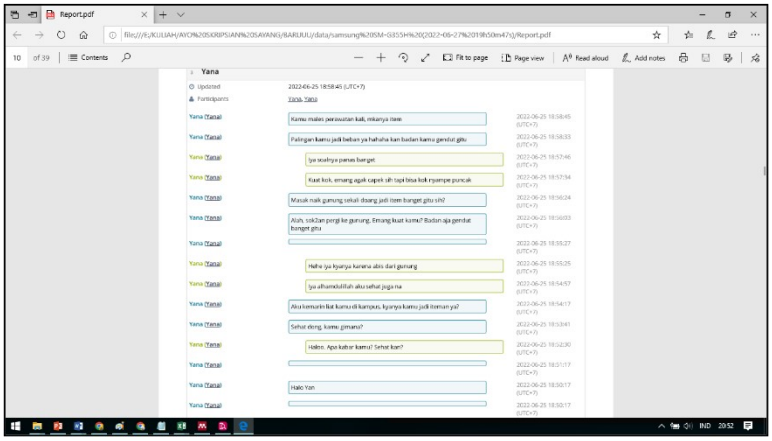
Tahap *Capture* merupakan tahap penyimpanan atau pendokumentasian semua data digital yang diperoleh dari proses akuisisi, kemudian data tersebut dikelompokkan sesuai jenis data masing-masing. Data digital tersebut merupakan hasil dari *physical memory capture* menggunakan MOBILEdit Forensic Express bisa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

$$Pon = \frac{\sum pn}{\sum po} \times 100\% \tag{1}$$

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 MOBILEdit 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 o f 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. Chelmis, 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 Sulistyo, "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.

Matrik: Jurnal Manajemen, Teknik Informatika, dan Rekayasa Komputer
Vol. 22, No. 3, July 2023, pp. 651∼664
ISSN: 2476-9843, accredited by Kemenristekdikti, Decree No: 200/M/KPT/2020
DOI: 10.30812/matrik.v22i3.2987

Mobile Forensic for Body Shaming Investigation Using Association of Chief Police Officers Framework

Yana Safitri, Imam Riadi, Sunardi
Universitas Ahmad Dahlan, Yogyakarta, Indonesia

Article Info

Article history:

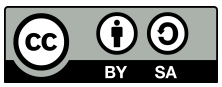
Received May 21, 2023
Revised Juny 26, 2023
Accepted July 15, 2023

Keywords:

Body Shaming
Digital Forensic
Mobile Forensic
IMO Messenger

ABSTRACT

Body shaming is the act of making fun of or embarrassing someone because of their appearance, including the shape or form of their body. Body shaming can occur directly or indirectly. MOBILEdit Forensic Express and Forensic ToolKit (FTK) Imager are used to perform testing of evidence gathered through Chat, User ID, Data Deletion, and Groups based on digital data obtained on IMO Messenger tokens on Android smartphones. This study aimed to collect evidence of conversations in body shaming cases using the Association of Chiefs of Police (ACPO) framework with MOBILedit Forensic Express and FTK Imager as a tool for testing. Based on the research findings, MOBILedit Forensic Express got an extraction yield of 0.75%. In contrast, using the FTK Imager got an extraction yield of 0.25%. The ACPO framework can be used to investigate cases of body shaming using mobile forensics tools so that the extraction results can be found. The results of this study contributed to forensic mobile knowledge in cases of body shaming or cyberbullying ACPO framework as well as for the investigators.



Corresponding Author:

Yana Safitri, +6287762222550,
Faculty Technology Industry, Master Program of Informatics,
Universitas Ahmad Dahlan, Yogyakarta, Indonesia,
Email: yana2107048011@webmail.uad.ac.id

How to Cite:
Y. Safitri, I. Riadi, and S. Sunardi, "Mobile Forensic for Body Shaming Investigation Using Association of Chief Police Officers Framework", MATRIK : Jurnal Manajemen, Teknik Informatika dan Rekayasa Komputer, vol. 22, no. 3, pp. 651-664, Jul. 2023.

1. INTRODUCTION

The advancement of Internet technology is rapid. The total number of internet users in cyberspace has surpassed 3.8 billion [1]. People may access the internet from anywhere, including on smartphones. Smartphones have now become a daily must for everyone [2]. Smartphone use has become a lifestyle need in Indonesia, which has a total population of 274.9 million in 2021 [3, 4]. Mobile phones now include an operating system that allows them to perform various duties similar to a personal computer, including internet connectivity. An Android smartphone is a hybrid device that functions as both a telephone and a computer but in a more portable form [5]. Smartphones, which have a variety of functionalities, can be exploited as cybercrime instruments [6]. The advancement of information and communication technology affects every aspect of life. Currently, mobile phones have numerous advantages and intriguing characteristics, the most prominent of which is the use of communication and life in cyberspace or online, namely social media [7]. There are numerous consequences to using social media, including cyberbullying [8]. In terms of cyberbullying cases, Indonesia ranks third in the globe. Children account for up to 91% of all cyberbullying reports [9]. Every year, the number of criminal cases on the internet grows. The internet has altered people's social lives, schooling, and even community activities [10]. Human activities today are mostly concerned with data, information, and communication, which are directly or indirectly tied to computer technology equipment. People benefit greatly from social media, but it also has significant drawbacks, such as disseminating inaccurate information, fake news, and addiction [11]. The effect of technology makes communication easier for people. In addition to having a good influence, information technology and telecommunications improvements have a negative consequence, specifically the increase in crimes involving online applications. The crime will undoubtedly leave evidence, such as a crime report, in court [12].

Digital forensics is a branch of science that applies investigative and analytical techniques to computer media or digital storage media in order to find, acquire, examine, and save evidence of criminal cases in order for them to be legally justifiedforensic analysis of worldwide Internet connections from several networks [13, 14]. Digital forensics refers to efforts to gather digital evidence relating to past crime cases [15], like in the case of IMO Messenger. IMO Messenger is an instant messaging application for iOS and Android devices. This application has almost the same capabilities as what WhatsApp offers. Instant messaging is a real-time communication channel that uses text, graphics, voice, or video [16]. Social media content can be of tremendous use to detectives during a criminal investigation [17]. To investigate short message-based cybercrimes like body shaming cases, detectives must analyze victims' and suspects' devices to locate digital evidence. Instant messengers have implemented end-to-end encryption technology to prevent privacy violations such as widespread spying by intelligence agencies [18]. Smartphones and social media are currently being widely abused to perpetrate crimes (cybercrime) such as human trafficking, cyberbullying, fraud, spreading hoaxes, and other crimes. Body shaming is a form of cyberbullying. The belief that your own body is the most ideal among your pals is one of the traits of body shaming. Unconsciously, you compare yourself to others who are slimmer or heavier than you. The Association of Chief Police Officers (ACPO) framework is used in this study to adapt the digital forensic investigation framework [19]. According to the guidance, it aids in dealing with high-tech crime claims and ensuring that all evidence is collected in a timely and acceptable manner. According to a senior police official. The results of the two forensic apps were compared using the MOBILEdit Forensic Express application and the FTK imager. It is intended that by using these techniques, a forensic investigator will be able to locate necessary artifacts [20]. The purpose of research, the method or framework, and the tools utilized separate this research from earlier research. It is envisaged that the research would yield digital evidence that will strengthen the proof of criminal cases in court in the form of digital evidence analysis results.

Riski Yudhi Prasongko et al. [21] researched the Use of the ACPO (Association of Chief Police Officers) Method on Forensic WhatsApp. The study employs 13 factors, and the results demonstrate that Belkasoft Evidence Center detects digital authenticity 81.92% of the time, while HashMyFiles detects it 79.95% of the time. Ilham Algi Plianda et al. [22] researched Analysis and Performance Comparison of Digital Forensic Tools on Android Smartphones using Whatsapp Instant Messaging, notably the MOBILEdit and Oxygen Forensic tools. In order to identify the best recommendations, the two tools are compared in terms of performance. This study demonstrates the advantages of the MOBILEdit tool over Oxygen Forensic in the context of the specific case. Many factors can affect the performance of each tool, including the type of device, the specifications of the device utilized, the version of the tools, and the research topic. As a result, the MOBILEdit Forensic tool is recommended in this study for digital schemes involving WhatsApp IM items and Android-based smartphone devices. Research conducted by Imam Riadi et al. [23] in the title Mobile Forensic of Vaccine Hoaxes on Signal Messenger using DFRWS Framework, MOBILedit Forensic Evidence, and Magnet AXIOM passed the repeatability and reproducibility validation tests in the following research. The AXIOM magnet did not obtain the digital signal messenger evidence from the offender's smartphone. The MOBILedit Forensic tool, on the other hand, was able to obtain Signal Messenger contact information and information with a performance value of 22.22%. MOBILedit Forensics and Magnet AXIOM do not receive digital evidence from Signal Messenger, such as chats, pictures, GIFs, pdf documents, videos, voice call history, and video call history. Research conducted by Galih Fanani et al. [24] in the title Michat Application Forensics Using the

Digital Forensics Research Workshop Method, Further investigation was conducted using Michat objects and the DFRWS approach with MOBILedit Forensic Express Pro tools, DB Browser For SQLite, and Oxygen Forensic Detective. A comparison was conducted to evaluate the capabilities of three forensic programs with varying processing levels in acquiring evidence: MOBILedit Forensic Express Pro (66.7%), DB Browser For SQLite (33.3%), and Oxygen Forensic Detective (83%). In litigation, digital evidence can be used as confirming evidence.

Unlike previous research, the forensic process was carried out using the DFRWS Framework [23, 24]. While the objects in previous research were WhatsApp [21, 22], Signal Messenger [23], and Michat [24]. This research is limited to text messaging (chats), user ID, erasing data, and groups and focuses on the IMO Messenger with the ACPO Framework. The primary goals of this study are to 1) perform digital forensic simulations using the ACPO framework and two tools, MOBILEdit Forensic Express and FTK Imager. 2) Search for digital evidence of body shaming incidents on the IMO Messenger app. This study focuses on digital evidence derived from instant messages.

This article is structured as follows: Part 1. Introduction, which includes a distinction from previous studies, section 2. Research Methods, which discusses the ACPO Framework for obtaining the expected research results, section 3. Results and analysis, which describes the research analysis results using the ACPO framework on IMO Messenger, use the MOBILEdit Forensic Express and FTK Imager tools, section 4. The conclusion summarizes the research findings and provides recommendations for further research.

2. RESEARCH METHOD

This study simulates digital forensic investigation. A simulation of digital forensic research focuses on investigating and finding the contents of digital devices and related computer crimes. Body shaming cases were the subject of case study-style digital forensic research simulations. Stages of forensic investigation utilize the ACPO framework in digital forensic simulation research. This study aims to forensic examine the Android smartphone software IMO Messenger. MOBILedit Forensic and FTK Imager are the forensic software programs used in this study. Figure 1 shows the steps of the research.

Figure 1. Research Flowchart

Following is a description of each stage of the research process. First is the literature review phase, which starts with gathering prior study data from different sources as a reference. Google Scholar, ResearchGate, and Science Direct were used to conduct literature searches on these websites. The terms Cybercrime, ACPO Framework, Mobile Forensics, Internet Messaging, Digital Forensics, and Body Shaming were used in the search process. Information for literature reviews is gathered from works published in reputable national and international publications. Articles from the past five years are those that are used. Investigations into Android-based devices can use earlier work in the fields of mobile forensics and the ACPO framework. The introduction and research methods section contains the literature review used as a study source.

The next case is a simulation step. Case simulation is developed at this stage. The study was started by carrying out a case simulation according to the previously designed case scenario shown in Figure 3. An Android device was used to carry out the

case simulation, namely the victim's smartphone. Based on this research case study, the perpetrator was arrested with an Android smartphone which was used as evidence. Smartphones will be checked to see if there is any relevant digital evidence. A laptop with MOBILedit Forensic and FTK Imager tools was used for the investigation.

The third stage is forensic analysis. At this stage, the ACPO framework is used to assess the simulation data. Our research concentrates on text messages, user ids, deleted data, and groups to help with the search for digital evidence. The following are some of the variables sought in this study. The MOBILEdit Forensic and FTK Imager tools are used to identify research variables in the forensic analysis process. Analysis of forensic results is the last step, and the investigator examines the forensic findings.

2.1. Framework

The ACPO framework is used in this study to search for digital evidence in the form of text messages, user IDs, deleted data, and groups in four stages: Plan, Capture, Analyze, and Present. The ACPO framework was used to conduct this research. Figure 2 illustrates the four processes that must be completed to achieve good research results.

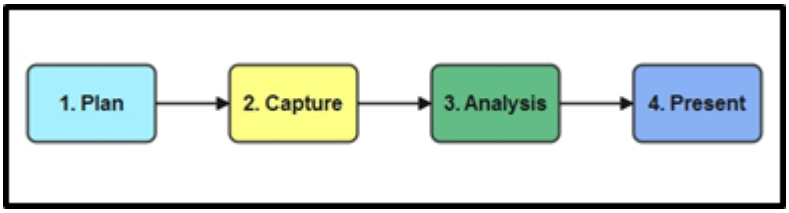


Figure 2. ACPO Flow

Figure 2 depicts the flow of the ACPO method, which consists of four stages:

1. Plan

The planning phase starts with determining the hardware and software required for the research process in order to get research results. The planning process begins with determining the tools and research materials; research tools might be hardware or software, and their respective applications have been identified.

2. Capture

This is the step in which all of the study results are recorded, stored, captured, and collected. Process capture on the results of the research process can make use of existing software as well as assistance hardware. The research will uncover data that can be used as evidence that there is no wrongdoing.

3. Analysis

This is the step in which all of the study results are recorded, stored, captured, and collected. Process capture on the results of the research process can make use of existing software as well as assistance hardware. The research will uncover data that can be used as evidence that there is no wrongdoing.

2.2. Present

At this stage, an explanation of all actions carried out during the study is carried out and discussed in full the outcomes of the research and provides input or ideas linked to the study's conclusions.

2.3. Research Tools

Tools are now needed for this project in order to collect artifacts from the IMO Messenger program. There are two types of research tools: forensic software and hardware. The research materials utilized in this experiment are described in detail in Table 1.

Table 1. Research Tools

Hardware and Software	Function
PC	A method used to transmit digital data from a smartphone to a storage device so that it can be analyzed
USB	Used to provide access from a smartphone and connect it to a computer
Smartphone	Used to store digital evidence data
KingRoot	Used to root the smartphone
MOBILedit Forensic Express	Used for the IMO Messenger application in the smartphone physical imaging process or data backup
FTK Imager	Used to carry out testing of digital evidence without changing the data or metadata of the original evidence

2.4. Case Simulation

Simulation is utilized to collect the data required for the study's sample. Conversations in an instant messaging group are used to carry out the simulation. One of the group members became a victim of bullying. At this point, the researcher does mobile forensics, which uses ID numbers to look for criminals and serves as the foundation for retrieving an analysis report from a database. The method employed in this study involves retrieving conversational data from the victim's Imo database, which will then be further analyzed utilizing the MOBILEdit Forensic Express application as a tool to look for evidence in the form of chat and perpetrator id. a brief explanation of the mobile forensic workflow applied to the Figure 3; the scenario of a criminal investigation on the IMO instant messaging platform. The process of finding evidence will next be examined using the tools MOBILEdit Forensic Express and FTK Imager, which will offer data in the form of previously recorded conversations in the database.

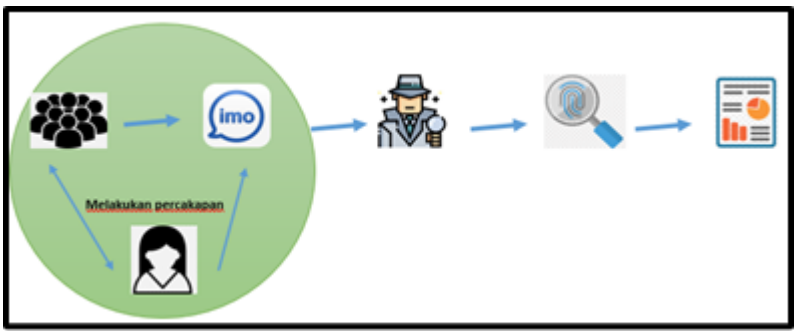


Figure 3. Case Simulation

In Figure 3, a case simulation was performed using a fictional group of teenage friends who regularly communicate on the IMO Messenger program in a group chat. However, one of them received a summons that referred to "you are really fat right now" and other forms of body shaming, which caused the victim to complain and report it to the police. The investigator uses the victim's smartphone to perform an inquiry, and they receive the report's findings. The investigator constructed a scenario for this investigation. The scenario is a cyberbullying instance involving multiple attackers and one victim. In this case, the victim and the perpetrators had a chat that resulted in cyberbullying against the victim via the IMO Messenger application. As the victim's smartphone, a Samsung Galaxy Core 2 was used in this scenario.

3. RESULT AND ANALYSIS

This section will review how to use the Association of Chief Police Officers framework in IMO Messenger forensics.

3.1. Plan

This flow begins with preparing a plan outlining the stages to be taken in the research process, including creating scenarios and preparing research tools and materials. In this stage, a search, data collection, and documentation of evidence is carried out in the form of the victim's smartphone, according to the predetermined scenario. The evidence is alive, and the security feature is not active. At this stage, documentation related to the evidence is carried out. Documentation of evidence can be seen in Figure 4.

Figure 4. Protecting Evidence

The next step is to turn on Airplane mode to separate the evidence from the internet connection. Avoiding damaging evidence on the smartphone is the goal of Airplane Mode, then switch on the smartphone's Development Options feature. To prevent the smartphone from going into sleep mode if it is not used for a time, the Stay Awake and USB Debugging options must also be enabled. Sleep mode serves to stop smartphone devices from activating the security system during the forensic procedure. Figure 5 depicts the evidence isolation stage.

Figure 5. Development Option

Table 1 depicts the investigation of the instruments and materials utilized in forensic analysis.

Table 2. Tools and Material

Tool Name	Description
USB Cable	Connector smartphone to Laptop
Smartphone	Evidence
FTK Imager	Software
MOBILedit Forensic Express	Software
Laptop	Acquisition Process

Table 2 shows the instruments utilized, which comprise an Acer Aspire E 14 core i3 laptop, a Samsung Galaxy Core 2 smartphone, and a USB connector. The IMO Messenger program, MOBILEdit Forensic Express, and FTK Imager tools are used to support this forensic research. The smartphone must first be rooted to extract data from an Android device.

The Imo application messenger, which is attached to the physical evidence, will evaluate the digital evidence utilizing the following investigation techniques on the evidence:

1. A smartphone running the Android operating system was purchased from the incident scene.
2. Isolation or signal coverage is turned off, and airplane mode is engaged.
3. By connecting to a laptop or PC with the ACER brand, MOBILEdit Forensic is used to back up smartphone evidence.
4. The MOBILEdit Forensic tool Express and FTK Imager are used for extraction and analysis.

3.2. Capture

Capture is the process of storing or documenting all digital data obtained during the acquisition phase. The data is then classified according to its type. Because all forensics techniques utilized were able to gather, text chat and user Ids were the best results for confirming digital evidence data. Chat messages and user Ids are the most crucial and key data points for cyberbullying cases.

Figure 6. MOBILedit Forensic Express Capture Result

Figure 6 shows the output of a comprehensive report generated by the MOBILEdit Forensics Express tool. Then various reporting files in these outcomes will be employed as digital data. MOBILEdit Forensics Express is capable of logical as well as physical acquisition. MOBILEdit Forensics Express is capable of extracting data from smartphone devices. MOBILEdit Forensic Express can recognize a cell phone's International Mobile Equipment Identity (IMEI) and a registered SIM card's IMSI and Integrated Circuit Card Identifier (ICCID). MOBILEdit successfully obtained contact information, text messages, and group data.

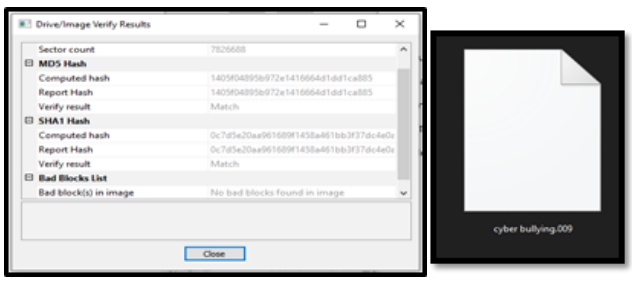


Figure 7. Capture Results and Imaging Results Using FTK Imager

Figure 7 depicts the SHA1 Hash value findings, where this value is utilized as a reference to match the hash value in the original file when imaging is performed. FTK Imager produced an imaging result file. FTK Imager is a tool for previewing and producing photographs for use in digital evidence testing. FTK Imagers may also create flawless duplicates (forensic images) of original evidence without altering the data or metadata.

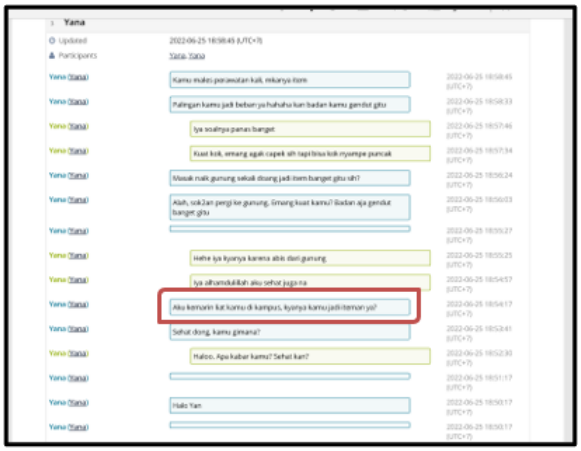


Figure 8. MOBILedit Forensic Express and Extracts Result

Figure 8 displays evidence gathered through chat. There are signs of cyberbullying in the chat since it comprises nasty sentences in the form of blasphemy toward the victim.

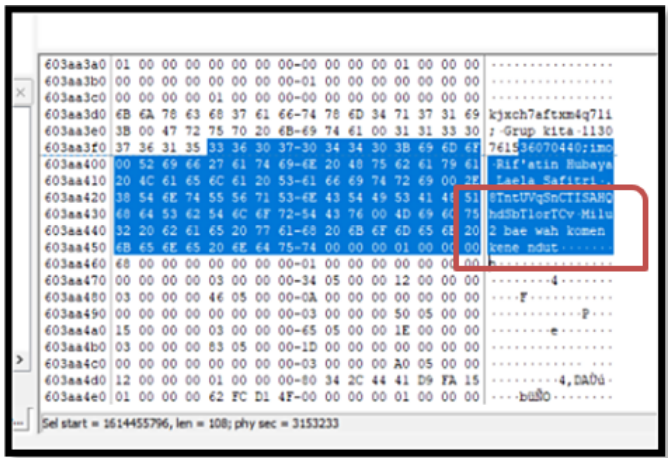


Figure 9. FTK Imager Data Extract Results

Figure 9 shows the outcome of the imaging results file recovered with the FTK Imager, which is the discussion between the criminal and the victim. However, because the conversations generated by data extraction are still scrambled, they must be found manually.

The extraction of text message data from the IMO Messenger application utilizing MOBILEdit Forensic Express and FTK Imager was successful. The outcomes of the extraction process were then evaluated. The digital data discovered in the analysis procedure in the form of text messages demonstrates that MOBILEdit Forensics Express and FTK Imager can gather digital data from the IMO Messenger program.

3.3. Analysis

The following Table 2 contains IMO Messenger data that was used in the study. This stage involves the examination and processing of the data obtained through the examination process, followed by an investigation to obtain or discover proof of the required items, namely the Imo database kept on the smartphone device storage without affecting the integrity of the data.

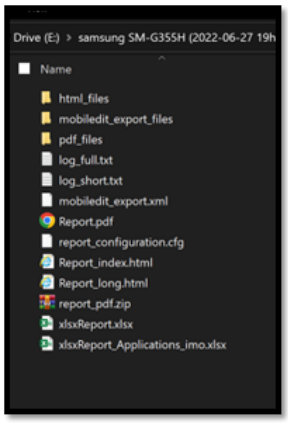


Figure 10. Full Report of MOBILedit Forensic Express

Figure 10 is the result of an extraction performed using the MOBILEdit Forensic Express tool found the report results which is a report on the results of digital evidence found in physical evidence.

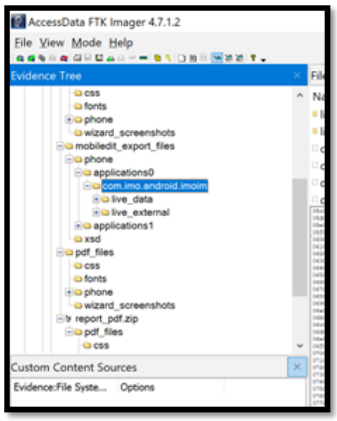


Figure 11. File Structure Tool of FTK Imager

The file structure that was extracted using the FTK Imager program is shown in Figure 11. The com.imo file found in the evidence is displayed by the FTK Imager program as the necessary database.

3.4. Present

This flow shows the evidence that was successfully acquired after the previous stages. The mobile forensic process and the ACPO flow on the Android platform were discovered to be capable of obtaining digital artifacts linked to the required evidence. These artifacts include conversations, User IDs, Data Delete, and Groups. In this study, the researchers focus exclusively on studying recorded and stored conversations in the database. Based on the testing findings, the index number formula determines each forensic tool's performance. The equation shows how the index number was calculated using an unweighted index.

$$P_{ar} = \frac{\sum ar0}{\sum arT} \times 100 \tag{1}$$

Explanation:
P_{ar} = Forensic tool accuracy index number.
$ar0$ = number of detected variables.
arT = Total number of variables used [23].

Table 3 shows the analysis results based on the conclusions collected through digital evidence.

Table 3. Digital Evidence

Data Type	MOBILedit Forensic Express	FTK Imager
Text Messaging	✓	✓
User ID	✓	-
Deleting Data	-	-
Group	✓	-
Percentage %	0.75	0.25

Since it can only locate three of the four digital evidence parameters sought by the MOBIL edit Forensic Express tool's equation, its performance value is only 0.75%. The FTK Imager, nevertheless, has a performance value of 0.25% since it can only locate one of the four characteristics of digital evidence. The following formula can be used to obtain the performance value needed to gauge each forensic tool's potential.

$$\text{MOBILedit Forensic Express: } P_{ar} = \frac{3}{4} \times 100\% = 0.75\% \tag{2}$$

$$\text{FTK Imager: } P_{ar} = \frac{1}{4} \times 100\% = 0.25\% \tag{3}$$

The evidence extraction is in Table 3 illustrates that the MOBILEdit Forensic and FTK Imager tools can discover the digital chat evidence you are looking forthe total findings of the evidence forensic process for the Samsung Galaxy Core 2 android smartphone. The evidence discovered at the scene of the occurrence includes both digital and physical evidence. The victim's smartphone was discovered as physical evidence. Furthermore, an investigative process is carried out on the victim's smartphone to acquire digital evidence. Table 3 is the outcome of obtaining digital evidence using percentages. The overall findings of the forensic process for the evidence of the Samsung Galaxy Core 2 android smartphone after the stages were completed following the ACPO method step technique utilized for research. A comparison of research results obtained in other studies using the ACPO framework can be seen in Table 4.

Table 4. Comparison with previous research

Title	Object	Artifact	Tools	Results
Forensic Whatsapp Investigation Analysis on Bluestack Simulator Device Using Live Forensic Method with ACPO Standard.	Whatsapp	msgstore.db.crypt12	Bluestack, FTK Imager, Whatsapp Viewer, and SQLite	The approach can be followed to perform WhatsApp analysis on the Android Bluestack simulator. Communication information about the Whatsapp application was collected from the Whatsapp database file msgstore.db.crypt12 as a result of the method.
Forensic Analysis of the TikTok Application on Android Smartphones Using the Association of Chief Police Officers Framework.	TikTok	Contact, Messages, Video, Hashtag	Magnet Axiom	The findings of the research process on the forensic analysis of the TikTok application, which runs on rooted Android smartphones, have several conclusions, including digital evidence obtained in the form of accounts, contacts, messages, videos, and hashtags related to defamation cases. A framework is used in the forensic procedure. ACPO's work and Magnet Axiom tools can be used to extract digital evidence from the TikTok app installed on the Samsung Galaxy Tab A SM-P355 smartphone.
Forensic Analysis of Dana Applications Using the ACPO Framework.	Dana	Profile Picture and Screenshot Transaction	Belkasoft Evidence Center & MOBILedit Forensic Express Pro	The results of the forensic analysis results obtained with two forensic tools, Belkasoft Evidence Center, failed to find artifacts that can be used as digital evidence. In contrast, the tool MobilEdit Express Pro forensics only managed to find artifacts in the form of photographs of users and screenshots of transactions made.
This study	IMO Messenger	Text Messaging, User ID, Deleting data, Group	MOBILedit Forensic Express and FTK Imager	The result found 0.75% data using MOBILEdit Forensic and 0.25% data using FTK Imager.

In Table 4, research conducted by Kurniadin Abd. Latif et al. [25] titled Forensic Whatsapp Investigation Analysis on Bluestack Simulator Device Using Live Forensic Method with ACPO Standard. Based on research, WhatsApp with the tools Bluestack, FTK Imager, Whatsapp Viewer, and SQLite. The findings of this investigation demonstrate that forensic analysis on Android devices using the Bluestacks simulator can be carried out following ACPO guidelines. Fitri Anggraini et al. [26] conducted research on the title Forensic Analysis of the TikTok Application on Android Smartphones Using the Association of Chief Police Officers Framework with the tool Magnet Axiom. The Magnet Axiom forensics software and the ACPO forensics framework are combined in this study. Together, they generated 77% of the proof through data messages, videos, and hashtags, in cases where these data were previously specified as initial data posted throughout the simulation procedure. Ermin et al. [27] researched Forensic Analysis of Dana Applications Using the ACPO Framework. Based on the research, the forensic analysis results were obtained using two forensic tools, Belkasoft Evidence Center and MobilEdit Express Pro Forensic Tools, and both failed to find artifacts that could be used as digital evidence. Compared with previous research, this research uses MOBILEdit Forensic and FTK Imager tools to search for digital evidence. Previous research did not use many tools to obtain information about the object to be tested.

4. CONCLUSION

According to the research findings of the Application of the Association of Chief Police Officers Framework for Body Shaming analysis Using the MOBILEdit Forensic Express tools, it has a 0.75% extraction percentage, and FTK Imager has a 0.25% extraction percentage. The findings of this study can be used as a resource for future studies; it is believed that the usage of forensic tools will become more diverse with the latest editions, allowing for the collection of additional digital artifacts from the IMO Messenger application. MOBILEdit Forensic gets more digital evidence, while FTK Imager only gets text messages and has to be searched manually. For future research, the researcher suggests studying mobile forensic techniques and frameworks and using other forensic instruments with recent updates to expect them to produce more precise results when collecting digital evidence.

5. ACKNOWLEDGEMENTS

Thank you to the Ahmad Dahlan University MTI Study Program for facilitating the Research Laboratory to complete the research.

6. DECLARATIONS

AUTHOR CONTIBUTION

This study was compiled by three authors divided into their respective tasks. Yana Safitri compiles and designs work, collects, analyzes, and interprets data. Imam Riadi and Sunardi as supervisors for articles to be published.

FUNDING STATEMENT

This study received no specific financing from any funding agency in the public, commercial, or non-profit sectors.

COMPETING INTEREST

I am unrepresented by conflicting financial, public, or institutional interests.

REFERENCES

[1] I. Riadi, A. Yudhana, and M. A. Barra, "Forensik Mobile pada Layanan Media Sosial LinkedIn," *JISKA: Jurnal Informatika Sunak Kalijaga*, vol. 6, no. 1, pp. 9–20, 2021.

[2] B. Fakiha, "Effectiveness of Forensic Firewall in Protection of Devices from Cyberattacks," *International Journal of Safety and Security Engineering*, vol. 12, no. 1, pp. 77–82, 2022.

[3] A. Alanda, D. Satria, H. A. Mooduto, and B. Kurniawan, "Mobile Application Security Penetration Testing Based on OWASP," *IOP Conference Series: Materials Science and Engineering*, vol. 846, no. 1, pp. 1–13, 2020.

[4] N. Setyaningsih, "Metode NIJ Untuk Analisis Forensik Layanan Dropbox Pada Smartphone Android," *JURNAL CYBERAEREA*, vol. 2, no. 6, pp. 1–10, 2022.

[5] I. Riadi, "Analisis Forensik Smartphone Android Menggunakan Metode NIST dan Tool MOBILedit Forensic Express," *Jurnal Informatika Universitas Pamulang*, vol. 5, no. 1, pp. 89–94, 2020.

[6] R. Y. Patil and S. R. Devane, "Network Forensic Investigation Protocol to Identify True Origin of Cyber Crime," *Journal of King Saud University - Computer and Information Sciences*, vol. 34, no. 5, pp. 2031–2044, 2022.

[7] 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.

[8] I. Riadi and S. Sunardi, "Investigasi Cyberbullying pada WhatsApp Menggunakan Digital Forensics," *Jurnal Resti (Rekayasa Sistem dan Teknologi Informasi)*, vol. 1, no. 10, pp. 730–735, 2021.

[9] G. M. Abaido, "Cyberbullying on social media platforms among university students in the United Arab Emirates," *International Journal of Adolescence and Youth*, vol. 25, no. 1, pp. 407–420, 2020.

[10] S. R. Ardiningtias, "Forensik Digital Kasus Penyebaran Pornografi pada Aplikasi Facebook Messenger Berbasis Android Menggunakan Kerangka Kerja National Institute of Justice," *JEPIN: Jurnal Edukasi & Penelitian Informatika*, vol. 7, no. 3, pp. 322–328, 2021.

[11] O. C. Hang and A. S. Media, "Cyberbullying Lexicon for Social Media," *ICRIIS: International Conference on Research and Innovation in Information System*, 2019.

[12] I. Anshori, K. Eka, S. Putri, and U. Ghoni, "Analisis Barang Bukti Digital Aplikasi Facebook Messenger Pada Smartphone Android Menggunakan Metode NIJ," *ITJRD: IT Journal Research & Development*, vol. 5, no. 2, pp. 118–134, 2021.

[13] S. Sotnik, T. Shakurova, and V. Lyashenko, "Development Features Web-Applications," vol. 7, no. 1, pp. 79–85, 2023. [Online]. Available: https://openarchive.nure.ua/handle/document/21600

[14] S. Sunardi and I. Riadi, "Penerapan Metode Static Forensics untuk Ekstraksi File Steganografi," *RESTI: Rekayasa Sistem dan Teknologi Informasi*, no. June, 2020.

[15] A. K. Priyanka and S. S. Smruthi, "WebApplication Vulnerabilities:Exploitation and Prevention," *Proceedings of the 2nd International Conference on Inventive Research in Computing Applications, ICIRCA 2020*, pp. 729–734, 2020.

[16] 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," *Jurnal Teknologi Infomasi*, vol. 20, no. 4, pp. 527–539, 2021.

[17] M. El-tayeb, A. Taha, and Z. Taha, "Video Reconstruction for Firefox Browser Forensics," *Ingénierie des Systèmes d ' Information*, vol. 26, no. 4, pp. 337–344, 2021.

[18] 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.

[19] I. Riadi, R. Umar, and M. A. Aziz, "Forensik Web Layanan Instant Messaging Menggunakan Metode Association Of Chief," *Mobile and Forensics (MF)*, vol. 1, no. 1, pp. 29–38, 2019.

[20] T. Hermawan and L. Roselina, "Android Forensic Tools Analysis for Unsend Chat on Social Media," *2020 3rd International Seminar on Research of Information Technology and Intelligent Systems (ISRITI)*, pp. 233–238, 2020.

[21] R. Y. Prasongko, A. Yudhana, and I. Riadi, "Analisis Penggunaan Metode ACPO (Association of Chief Police Officer) pada Forensik WhatsApp," *Jurnal Sains Komputer & Informatika (J-SAKTI*, vol. 6, no. 2, pp. 1112–1120, 2022.

[22] I. A. Plianda and R. Indrayani, "Analisa dan Perbandingan Performa Tools Forensik Digital pada Smartphone Android menggunakan Instant Messaging Whatsapp," *Jurnal Media Informatika Budidarma*, vol. 6, no. 1, p. 500, 2022.

[23] I. Riadi, H. Herman, and N. H. Siregar, "Mobile Forensic of Vaccine Hoaxes on Signal Messenger using DFRWS Framework," *MATRIK : Jurnal Manajemen, Teknik Informatika dan Rekayasa Komputer*, vol. 21, no. 3, pp. 489–502, 2022.

[24] G. Fanani, I. Riadi, and A. Yudhana, "Analisis Forensik Aplikasi Michat Menggunakan Metode Digital Forensics Research Workshop," *RESTI*, vol. 6, no. April, pp. 1263–1271, 2022.

[25] K. A. Latif, R. Hammad, T. T. Sujaka, K. Marzuki, and A. S. Anas, "Forensic Whatsapp Investigation Analysis on Bluestack Simulator Device Using Live Forensic Method With ACPO Standard," *International Journal of Information System & Technology Akreditasi*, vol. 5, no. 3, pp. 331–338, 2021.

[26] F. Anggraini, H. Herman, and A. Yudhana, "Analisis Forensik Aplikasi TikTok Pada Smartphone Android Menggunakan Framework Association of Chief Police Officers," *JURIKOM (Jurnal Riset Komputer)*, vol. 9, no. 4, p. 1117, 2022.

[27] M. R. Setyawan and F. Tella, "Forensic Analysis Of Dana Applications Using The ACPO Framework," *JURASIK: Jurnal Riset Sistem Informasi dan Teknik Informatika*, vol. 8, pp. 1–8, 2023.

[This page intentionally left blank.]

Analisis Bukti pada Aplikasi IMO Messenger Berbasis Android: Perbandingan Metode ACPO dan NIJ dalam *Framework* Forensik Digital

Yana Safitri, Imam Riadi, Sunardi

Abstrak Kebutuhan akan alat forensik digital yang efektif untuk membantu lembaga penegak hukum dalam menyelidiki kegiatan kriminal semakin meningkat karena pesatnya pertumbuhan platform komunikasi digital. Penelitian ini membandingkan *framework* forensik yang digunakan pada aplikasi IMO Messenger berbasis Android, khususnya berfokus pada kerangka *Association of Chiefs of Police* (ACPO) dan *National Institute of Justice* (NIJ). Alat yang digunakan untuk pemeriksaan adalah MOBILEedit Forensic Express dan Autopsy. Tujuan dari penelitian ini adalah mengumpulkan barang bukti pada kasus *body shaming* menggunakan *framework* ACPO dan NIJ dengan alat pengujian MOBILedit Forensic Express Pro dan Autopsy. Berdasarkan hasil pencarian, MOBILedit Forensic Express Pro mencapai tingkat ekstraksi 100%. Sebaliknya, menggunakan Autopsy menghasilkan efisiensi ekstraksi sebesar 3,33%. Framework NIJ dinilai terbaik karena mendukung proses investigasi dengan langkah paling komprehensif dalam menyelidiki kasus *body shaming* dengan menggunakan alat forensik *mobile*, sehingga memberikan hasil yang dapat diekstraksi. Barang bukti telah diidentifikasi sebagai bentuk bukti digital terbaik yang dapat digunakan untuk mendukung tuntutan hukum yang sah. Temuan penelitian ini berkontribusi untuk memajukan pengetahuan forensik seluler dalam kasus-kasus mempermalukan fisik atau cyberbullying dalam kerangka ACPO dan NIJ, sehingga menguntungkan para penyelidik.

Kata kunci ACPO, *Cyberbullying*, Forensik Digital, Forensik *Mobile*, NIJ

• Yana Safitri ✉
Program Magister Informatika, Fakultas Teknologi Industri, Universitas Ahmad Dahlan, Yogyakarta
e-mail: yana2107048011@webmail.uad.ac.id

• Imam Riadi
Department of Information System, Faculty of Applied Science and Technology, Ahmad Dahlan Yogyakarta
e-mail: imam.riadi@is.uad.ac.id

• Sunardi
Program Studi Teknik Elektro, Fakultas Teknologi Industri, Universitas Ahmad Dahlan, Yogyakarta
e-mail: sunardi@mti.uad.ac.id

1.1. PENDAHULUAN

Kemajuan teknologi yang pesat ditandai dengan maraknya smartphone yang menggunakan sistem operasi Android yang hadir dengan berbagai fitur canggih (Riadi dkk., 2023). Pertumbuhan ponsel pintar Android menghadirkan peluang menarik sekaligus tantangan yang menantang (Nurhairani & Riadi, 2019). Berkat kemajuan teknologi terkini, hampir semua orang, dari berbagai latar belakang, berinteraksi online secara tidak sengaja. Berkat aplikasi ponsel pintar, penjahat dunia maya kini memiliki lebih banyak cara untuk melakukan kejahatan (Al-Garadi dkk., 2019). Salah satu komponen kejahatan digital adalah analisis jejak perilaku kriminal untuk digunakan sebagai alat bukti (Widiandana dkk., 2020). Selain lebih kompak dan portabel dibandingkan komputer, smartphone Android merupakan perangkat hybrid yang dapat digunakan sebagai ponsel (Dweikat dkk., 2021). Banyak alat yang digunakan di bidang forensik digital untuk membantu penyelidikan. Ada banyak peluang dan masalah menarik yang terkait dengan pengembangan forensik ponsel pintar Android (Ichsan & Riadi, 2021).

Aplikasi pesan instan berbasis Android seperti IMO Messenger telah menjadi komponen penting dalam komunikasi kita sehari-hari (Al-Rawashdeh dkk., 2020). Meskipun aplikasi ini menawarkan sarana praktis untuk bertukar informasi, pentingnya aplikasi ini dalam menghasilkan bukti digital semakin meningkat, terutama dalam hal forensik digital (Atlam dkk., 2020). Seiring kemajuan era digital, platform pesan instan seperti IMO Messenger menjadi semakin penting untuk komunikasi (Zhu dkk., 2021). Lebih dari sebelumnya, komunikasi antar manusia menjadi lebih mudah, begitu pula pertukaran ide dan acara sosial penting (Alanda dkk., 2020). Untuk tujuan khusus, banyak konten yang meragukan dan menipu dibuat dan disebarluaskan. Program seperti ini memang mempunyai manfaat, namun juga membawa bahaya penyalahgunaan, misalnya *cyberbullying*, yang dapat merugikan korbannya (Adamu dkk., 2021). Kejahatan dunia maya saat ini menjadi perhatian terbesar pada aplikasi pesan instan (Hou dkk., 2020). Untuk mencegah kejahatan dunia maya dengan pesan singkat, penyidik perlu melakukan pemeriksaan forensik terhadap perangkat tersangka dan korban guna memulihkan barang bukti digital (Yao dkk., 2019). Kejahatan dunia

maya (*cybercrime*) merupakan aktivitas melawan hukum yang memanfaatkan terobosan teknologi internet dan komputer (Riadi dkk., 2022). Kejahatan dunia maya mencakup kejahatan terhadap manusia, kejahatan terhadap properti, kejahatan terhadap organisasi, dan kejahatan terhadap masyarakat (Sukamto dkk., 2022). *Cyberbullying* merupakan salah satu dampak negatif yang dihadapi remaja saat ini (Turanovic & Siennick, 2022).

Investigasi terhadap percakapan IMO Messenger harus melihat artefak layanan pesan jika bukti kriminal ditemukan (Sunardi dkk., 2022). Penanganan forensik khususnya forensik *mobile* diperlukan untuk membantu penyelesaian kasus pidana (Ferguson dkk., 2020). Teknologi forensik *mobile* diperlukan untuk memulihkan artefak, mendekripsi data, dan menganalisisnya guna mendukung penyelidik dalam penyelidikan kejahatan perangkat seluler. Teknik forensik *mobile* dapat diterapkan pada analisis kejahatan menggunakan perangkat Android (Khanafseh dkk., 2019). Kontinuitas bukti, akurasi dalam proses ekstraksi data, dan pemahaman mendalam tentang berbagai platform seluler dan sistem operasi adalah area fokus utama forensik seluler (Al-Sabaawi & Foo, 2019). Selain itu, karena hal ini dapat mempersulit penyelidikan forensik, kemajuan teknologi seperti enkripsi data dan keamanan perangkat harus diperhitungkan (Patil & Devane, 2022).

Pengumpulan dan analisis bukti digital sangat penting dalam konteks forensik digital untuk mendukung kasus pidana, perdata, dan lainnya. Untuk menemukan jejak digital yang relevan, forensik digital memerlukan prosedur pengumpulan data digital yang cermat dari perangkat dan jaringan dan memeriksanya dengan cermat (ALThebaity dkk., 2020). Forensik digital kini semakin penting dalam memahami dan merespons kejahatan digital, pelanggaran keamanan, atau aktivitas yang melibatkan penggunaan teknologi sejak munculnya perangkat seluler, komputasi awan, dan teknologi kontemporer lainnya. (Goldstraw-White, 2022). Oleh karena itu, menjaga keadilan dan keamanan di dunia digital yang berubah dengan cepat memerlukan pemahaman menyeluruh tentang dasar-dasar forensik digital dan cara penerapannya.(Salih & Dabagh, 2023).

Teknik atau kerangka kerja yang digunakan di bidang forensik digital untuk mengumpulkan, memeriksa, dan menyajikan bukti digital sangat penting untuk hasil penyelidikan (Kolla, 2022). Teknik-

teknik yang dikeluarkan oleh *National Institute of Justice* (NIJ) dan *Association of Chief Police Officers* (ACPO) merupakan dua teknik yang terkenal dan sering diterapkan dalam penegakan hukum, khususnya di bidang forensik digital (Feucht, 2021). Kedua pendekatan tersebut menawarkan arahan dan protokol untuk melaksanakan pemeriksaan forensik dengan tujuan mencapai ketepatan analitis dan kontinuitas bukti.

Penting untuk membandingkan pendekatan NIJ dan ACPO untuk memahami kelebihan, kekurangan, dan kegunaannya di dunia nyata (Horsman, 2020). Hal ini penting karena keberhasilan dan kualitas temuan forensik digital dapat dipengaruhi oleh pilihan metodologi yang dibuat (Kebande & Venter, 2019). Pemahaman menyeluruh terhadap kedua pendekatan juga dapat membantu peneliti, organisasi penegak hukum, dan praktisi forensik digital meningkatkan kemanjuran dan efisiensi pengelolaan kasus digital (Pribadi dkk., 2023).

Membandingkan teknik ACPO dan NIJ dalam konteks penggunaannya dalam forensik digital akan menjadi tujuan utama penelitian ini (Choi dkk., 2019). Untuk menyelidiki kejahatan digital yang semakin rumit, penelitian ini diharapkan dapat membantu membangun metode forensik digital yang lebih baik dan efektif dengan menilai dan memahami kelebihan dan kekurangan masing-masing metode (Yaacoub dkk., 2022)

1.2 FORENSIK

Forensik, atau ilmu forensik, adalah cabang ilmu yang berkaitan dengan pengumpulan, analisis, dan interpretasi bukti fisik yang ditemukan di tempat kejadian untuk membantu penyelidikan dan penyelesaian kasus kriminal atau perdata. Ilmu forensik menggabungkan berbagai disiplin ilmu, seperti kimia, biologi, fisika, ilmu komputer, dan sebagainya, untuk menyelidiki bukti-bukti yang dapat digunakan dalam pengadilan (Khairunnisa & Zulfan, 2023). Tujuan utama ilmu forensik adalah untuk membantu penyelidikan kasus dengan mengidentifikasi bukti fisik, menghubungkan bukti tersebut dengan pelaku kejahatan atau peristiwa yang terjadi, dan menyediakan informasi yang akurat dan objektif kepada pengadilan.

Contoh-contoh aplikasi ilmu forensik meliputi analisis DNA untuk mengidentifikasi pelaku kejahatan, penentuan penyebab kematian dalam otopsi, analisis sidik jari, analisis serologi, penggunaan rekaman CCTV, dan banyak lagi (Khairunisa & Priyana, 2022).

Ilmu forensik sangat penting dalam sistem peradilan pidana dan perdata, karena membantu dalam membuktikan atau membantah tuduhan, serta mengidentifikasi pelaku dan korban dalam kasus-kasus hukum (Aurelia dkk., 2023).

Ilmu forensik adalah kegiatan yang bertujuan untuk melakukan penyidikan dan menentukan fakta-fakta yang berkaitan dengan kegiatan pidana dan urusan hukum lainnya. Ilmu forensik merupakan salah satu cabang ilmu yang mencakup pendeteksian dan penyelidikan data yang terdapat pada perangkat digital (komputer, telepon genggam/*smartphone*, tablet, media penyimpanan, dan lain-lain). Forensik digital dapat dibagi menjadi investigasi yang berhubungan dengan komputer (*host, server*), jaringan, aplikasi (termasuk *database*) dan perangkat (*digital devices*), masing-masing investigasi memiliki kedalamannya masing- masing (Ramadhan & Mualfah, 2020). Forensik digital dapat dianggap sebagai metode ilmiah untuk mengembangkan sistem untuk mengidentifikasi, mencari, memulihkan, dan menganalisis bukti dari komputer, media penyimpanan komputer, dan perangkat elektronik lainnya, dan menyajikan hasil kesimpulan tersebut dalam eksperimen. Forensik digital juga dapat didefinisikan sebagai pengumpulan dan analisis data dari berbagai sumber komputer termasuk sistem komputer, jaringan komputer, jalur komunikasi dan berbagai media penyimpanan, yang dapat dikirim ke pengadilan (Dewi dkk., 2022).

1.2.1 FORENSIK DIGITAL

Forensik digital dapat dibagi menjadi investigasi yang berhubungan dengan komputer (*host, server*), jaringan, aplikasi (termasuk *database*) dan perangkat (*digital devices*), masing-masing investigasi memiliki kedalamannya masing- masing (Ramadhan & Mualfah, 2020). Forensik digital dapat dianggap sebagai metode ilmiah untuk mengembangkan sistem untuk mengidentifikasi, mencari, memulihkan, dan menganalisis bukti dari komputer, media

penyimpanan komputer, dan perangkat elektronik lainnya, dan menyajikan hasil kesimpulan tersebut dalam eksperimen. Forensik digital juga dapat didefinisikan sebagai pengumpulan dan analisis data dari berbagai sumber komputer termasuk sistem komputer, jaringan komputer, jalur komunikasi dan berbagai media penyimpanan, yang dapat dikirim ke pengadilan (Dewi dkk., 2022).

1.2.2 FORENSIK *MOBILE*

Forensik *mobile* sering digunakan dalam berbagai konteks, termasuk dalam penyelidikan kasus kriminal seperti pencurian, kejahatan siber, penipuan, dan bahkan terorisme. Kehadiran perangkat seluler yang berisi informasi pribadi yang sangat penting membuat forensik *mobile* menjadi alat yang berharga dalam membantu penyelidikan dan peradilan (Bintang dkk., 2020).

Forensik *mobile*, dikenal sebagai forensik seluler atau ponsel forensik, adalah cabang ilmu forensik yang fokus pada pengumpulan, analisis, dan interpretasi bukti yang terkait dengan perangkat seluler seperti *smartphones*, tablet, dan perangkat portabel lainnya. Tujuan utama forensik *mobile* adalah untuk mengungkap informasi yang relevan dari perangkat seluler untuk membantu penyelidikan kasus kriminal, perdata, atau kasus lain yang melibatkan penggunaan perangkat seluler (Fanani dkk., 2022). Kegiatan dalam forensik *mobile* dapat mencakup:

1) Pengumpulan Bukti, mencakup pengambilan salinan data dari perangkat seluler melalui koneksi fisik maupun nirkabel untuk memastikan integritas data seluler tersebut tetap terjaga.
2) Analisis Data, melibatkan pemeriksaan data yang diambil dari perangkat seluler, termasuk pesan teks, panggilan telepon, *email*, foto, video, lokasi GPS, riwayat perambanan *web*, dan banyak lagi. Analisis ini bertujuan untuk menemukan bukti yang relevan dengan penyelidikan.
3) Pemulihan Data, data pada perangkat seluler dapat terhapus atau tersembunyi. Dalam forensik *mobile*, teknik pemulihan data

digunakan untuk mengembalikan data yang mungkin dihapus atau tersembunyi.

4) Pemeriksaan Aplikasi, seluler forensik juga melibatkan pemeriksaan aplikasi yang terinstal di perangkat, termasuk jejaring sosial, aplikasi pesan, dan aplikasi lain yang mungkin berisi informasi penting.
5) Analisis Forensik Jaringan Nirkabel, penyelidikan dalam forensik *mobile* juga dapat mencakup analisis jaringan nirkabel yang terkait dengan perangkat seluler, seperti aktivitas jaringan, panggilan seluler, dan lainnya (Ruslan dkk., 2022).

1.2.3 *CYBERBULLYING*

Cyberbullying merujuk pada semua bentuk kekerasan yang dialami oleh anak atau remaja yang dilakukan oleh teman sebaya melalui dunia maya atau internet. Intimidasi maya terjadi ketika anak atau remaja menjadi sasaran ejekan, penghinaan, intimidasi, atau penghinaan oleh anak atau remaja lain melalui media internet, teknologi digital, atau telepon seluler (Nurhairani & Riadi, 2019). Intimidasi dunia maya dianggap sah jika baik pelaku maupun korban berusia di bawah 18 tahun dan secara hukum belum dianggap dewasa. Jika salah satu atau kedua pihak yang terlibat sudah berusia di atas 18 tahun maka kasus tersebut dikategorikan sebagai kejahatan dunia maya atau sering disebut pembuntutan dunia maya (atau *cyber harassment*) (Hou dkk., 2020).

Bentuk dan metode intimidasi dunia maya sangat bervariasi yang dapat mencakup ancaman melalui *email*, memposting foto yang merendahkan korban, membuat situs *web* untuk menyebarkan fitnah dan ejekan terhadap korban, hingga mengakses akun media sosial orang lain untuk mengancam korban dan menciptakan masalah. Motivasi pelaku juga beragam, termasuk kemarahan, balas dendam, frustrasi, pencarian perhatian, atau bahkan sekadar hiburan dalam waktu luang (Riadi dkk., 2021). Jenis-jenis *cyberbullying* di media sosial antara lain:

1) Hinaan terhadap penampilan fisik atau *body shaming*, seperti merendahkan tubuh seseorang, misalnya menyebut wanita gemuk sehingga mereka merasa malu untuk menunjukkan tubuh. Yang menjadi perhatian adalah ketika korban *body shaming* melakukan usaha yang tidak sehat untuk mencapai standar "kecantikan" atau "ketampanan" yang dianggap ideal. Selain masalah berat badan, hinaan terhadap warna kulit yang gelap juga sering terdengar di media sosial.
2) Ras. Tidak ada yang dapat memilih warna kulit saat lahir. Namun, sayangnya, dalam beberapa waktu terakhir banyak individu yang mencela ras orang lain. Bahkan, konflik rasial sering muncul karena prasangka-prasangka tertentu. Sebagai contoh, ada anggapan bahwa suatu ras sering terlibat dalam tindakan kriminal, atau ada ras yang dianggap serakah, dan sejenisnya. Padahal, sifat-sifat semacam itu ada di berbagai individu dan tidak terbatas pada satu ras saja. Kejadian semacam ini terjadi di beberapa negara, dan berbagai upaya telah dilakukan untuk melawan rasisme. Salah satu caranya adalah dengan meningkatkan inklusivitas di antara ras.
3) Menghina Hobi. Di media sosial, ada individu yang tanpa alasan yang jelas melakukan tindakan meremehkan terhadap hobi orang lain. Tindakan meremehkan terhadap hobi ini dapat menghambat potensi seseorang karena setiap individu memiliki minat yang berbeda-beda. Setiap individu memiliki bakat dan kemampuan yang berbeda. Jangan sampai semangat dan bakat dalam suatu bidang terhambat oleh rasa takut karena ejekan orang lain. Ingatlah perkataan Steve Jobs, pendiri Apple, “Jangan biarkan suara-suara berisik dari opini orang lain menghalangi suaramu sendiri” (Adamu dkk., 2021).

1.2.4 ACPO

Association of Chief Police Officers (ACPO) mempunyai beberapa tahapan penelitian seperti pada Gambar 1.1 dengan penjelasan berikut:

Gambar 1.1 Tahapan ACPO

1) Tahap rencana (*plan*) melibatkan perencanaan terperinci mengenai semua langkah yang akan dilakukan selama proses penelitian. Pada tahap ini, rancangan tentang semua kegiatan yang akan dilakukan dalam proses penelitian telah disusun sebelumnya.
2) Tahap menangkap (*capture*) merupakan saat dimana hasil penelitian disimpan untuk digunakan dalam tahap analisis selanjutnya. Dalam tahap ini, data hasil penelitian disimpan untuk keperluan analisis yang akan dilakukan pada tahap selanjutnya.
3) Tahap analisis (*analysis*) dilakukan untuk menganalisis hasil dengan menggunakan parameter yang telah diperoleh dari tahap sebelumnya.
4) Tahap presentasi (*present*) adalah saat dimana data hasil analisis dari tahap sebelumnya disajikan agar dapat diakses oleh pihak berwenang (Anggraini dkk., 2022).

1.2.5 NIJ

Metode *National Institute of Justice* (NIJ) pada forensik digital adalah suatu pendekatan yang digunakan untuk mengumpulkan, menganalisis, dan menginterpretasi bukti digital dalam penyelidikan kejahatan atau insiden keamanan. NIJ adalah sebuah lembaga di Amerika Serikat yang berfokus pada penelitian dan pengembangan dalam bidang keadilan pidana.

Metode NIJ dalam forensik digital biasanya mencakup beberapa tahapan yang meliputi:

1) *Identification*: Langkah pertama dalam proses forensik digital adalah tahap indentifikasi yang merupakan tahap pemilihan barang bukti dan pemilihan data data untuk mendukung proses penyidikan. Tahapan ini bertujuan untuk mengidentifikasi kemungkinan bukti yang relevan dan menentukan pendekatan analisis yang tepat.
2) *Collection*: Setelah bukti digital dikumpulkan, analis forensik akan melakukan pengumpulan bukti dari perangkat atau sistem yang terlibat dalam investigasi. Bukti ini bisa berupa data elektronik seperti *file*, catatan *log*, *email*, dan sebagainya. Pengumpulan harus dilakukan dengan hati-hati dan sesuai dengan prosedur yang telah ditetapkan untuk memastikan integritas bukti.
3) *Examination*: Tahap ini merupakan tahap pemeriksaan data yang dikumpulkan secara forensik, baik secara otomatis maupun manual.
4) *Analysis*: Tahap analisis forensik melibatkan penggunaan berbagai teknik dan alat untuk mengidentifikasi, mengambil, dan menganalisis data yang relevan dari bukti digital. Ini bisa mencakup pemulihan data yang dihapus, identifikasi jejak digital, rekonstruksi aktivitas, dan validasi bukti.
5) *Reporting*: Hasil dari analisis forensik digital biasanya disampaikan dalam bentuk laporan resmi. Laporan ini harus jelas, terperinci, dan berisi semua temuan serta kesimpulan yang relevan. Laporan ini bisa digunakan sebagai bukti dalam proses hukum

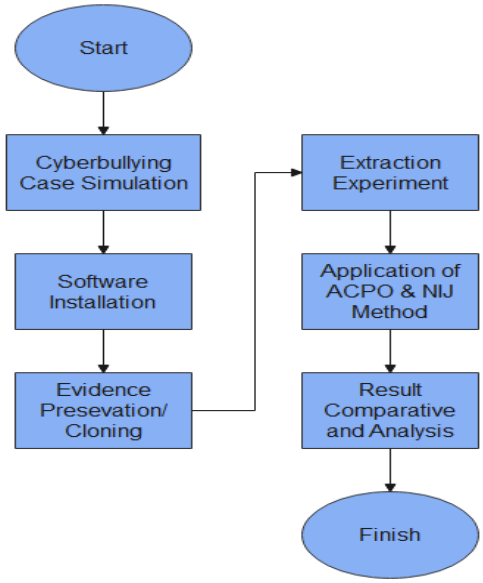
Metode NIJ pada forensik digital menekankan pentingnya pemakaian prinsip-prinsip ilmiah dan standar yang tinggi dalam melakukan investigasi digital. Hal ini membantu memastikan bahwa hasil analisis forensik dapat diandalkan dan dapat digunakan secara efektif dalam proses hukum.

1.3 METODOLOGI PENELITIAN

Metodologi penelitian analisis menggunakan kerangka NIJ dan ACPO untuk mereplikasi studi kasus dan mengevaluasi aplikasi *smartphone* IMO Messenger. Simulasi ini bertujuan untuk membandingkan dua kerangka dan alat forensik yang tersedia untuk

aplikasi seluler IMO Messenger. Menemukan *file* komunikasi dan media yang telah digunakan secara ilegal dan mengubahnya menjadi bukti adalah tujuannya.

1) Topik penelitian yang akan diteliti lebih lanjut dipilih berdasarkan masalah penelitian. Pada titik ini, penyelidik menggunakan berbagai metode untuk mengumpulkan rincian tentang lokasi dan kronologi insiden.
2) Tinjauan literatur harus mengumpulkan semua informasi yang sudah dapat diakses mengenai subjek dan objek penelitian, serta membangun landasan untuk penelitian lebih lanjut dan perspektif segar bagi setiap peneliti. Hal ini memastikan bahwa karya tersebut akan dapat dikutip di masa mendatang.
3) Studi Kasus melakukan pemeriksaan forensik pada aplikasi IMO Messenger Android menggunakan MOBILedit Forensic Express Pro dan Autopsy. *Flowchart* ditunjukkan pada Gambar 1.2 studi kasus.



Gambar 1.2 *Flowchart* investigasi

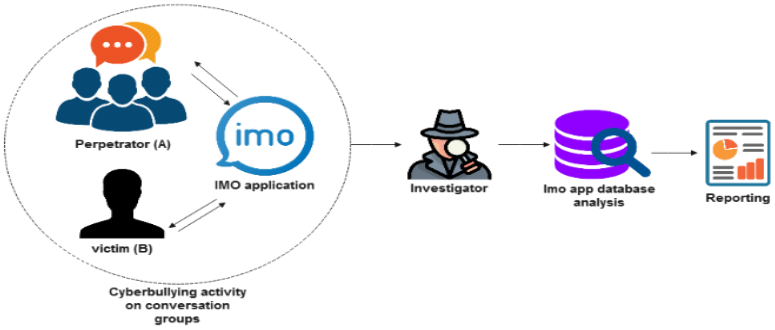
Gambar 1.2 menunjukkan *flowchart* dijelaskan sebagai berikut:

1) Membuat simulasi *cyberbullying*: Aplikasi IMO digunakan untuk menghasilkan simulasi *cyberbullying* untuk penelitian ini.
2) Seorang penyelidik menginstal perangkat lunak alat forensik di desktop atau laptop yang akan digunakan untuk mengumpulkan dan memeriksa bukti digital.
3) Pelestarian/kloning bukti: Penyidik perlu menjaga keamanan bukti nyata saat ponsel cerdas dalam mode pesawat untuk menjaga keutuhan data asli.
4) Eksperimen Ekstraksi: Penyelidik menggunakan serangkaian metode forensik untuk mengekstrak data dari perangkat ponsel cerdas. Menggunakan MOBILedit Forensic Express Pro, ponsel cerdas dipindai secara fisik, dan Autopsy digunakan untuk menilai bukti digital dari file multimedia.
5) Penerapan Metode ACPO dan NIJ: Peneliti menilai dua strategi untuk membantu penyidik dalam melakukan penyelidikan dalam penelitian ini. Perencanaan, penangkapan, analisis, dan presentasi adalah empat tahapan ACPO. NIJ terdiri dari lima proses: identifikasi, pengumpulan, pemeriksaan, analisis, dan pelaporan.

Evaluasi dan Analisis Hasil: Hasil yang di dapat oleh setiap alat forensik akan dinilai dan diperiksa secara cermat berdasarkan karakteristik program dan bukti digital yang dihasilkannya. Parameter yang digunakan mendukung tujuan penelitian khususnya pemeriksaan layanan IMO Messenger.

1.3.1 SKENARIO PENELITIAN

IMO Messenger adalah alat yang digunakan untuk melakukan skenario kasus *cyberbullying*. Gambar 1.3 menunjukkan skenario kasus *cyberbullying* yang menunjukkan komunikasi antara korban dan pelaku.



Gambar 1.3 Skenario penelitian kasus percakapan *cyberbullying*

Gambar 1.3 menggambarkan simulasi berdasarkan diskusi dari grup *chat* pesan instan. *Bullying* terjadi dan berdampak pada salah satu anggota kelompok. Simulasi ini menyimulasikan contoh *cyberbullying* di mana banyak pelaku berkomunikasi dengan satu korban. *Cyberbullying* dari pelaku dalam kejadian ini yang berpura-pura berbicara dengan korban melalui aplikasi IMO Messenger. Dalam skenario ini, perangkat pelaku yang diamankan adalah *smartphone* Samsung Galaxy Core 2. *Smartphone* dari pelaku *cyberbullying* diamankan untuk kemudian diinvestigasi oleh investigator.

1.3.2 ALAT PENELITIAN

Sejumlah perangkat diperlukan untuk mengambil artefak dari aplikasi IMO Messenger untuk tujuan penyelidikan ini. Alat-alat penelitian tersebut dapat dikelompokkan ke dalam dua kategori utama: perangkat lunak forensik dan peralatan fisik. Beberapa instrumen penelitian yang digunakan dalam eksperimen ini untuk mengumpulkan data dan informasi terkait dari aplikasi IMO Messenger diuraikan dalam Tabel 1.1. Instrumen-instrumen ini sangat penting untuk memastikan pemeriksaan forensik yang komprehensif serta untuk menjamin keakuratan dan kebenaran hasil penyelidikan.

Tabel 1.1. Perangkat lunak dan perangkat keras pendukung

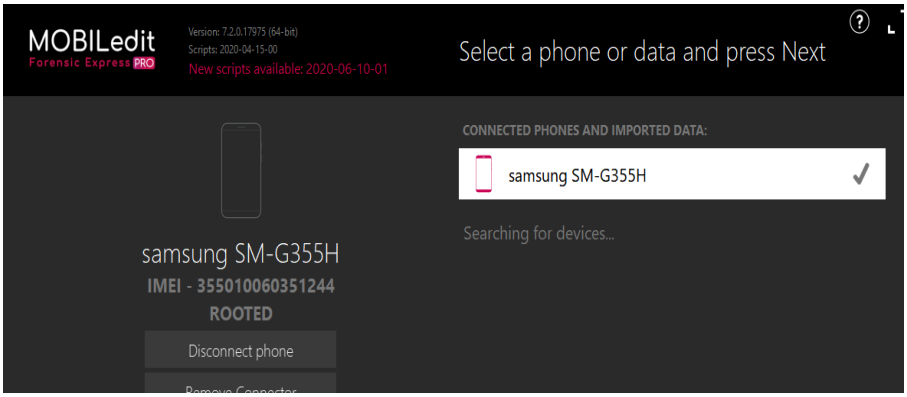
Hardware dan Software	Fungsi
Laptop	Suatu metode transmisi data digital dari *smartphone* ke perangkat penyimpanan agar dapat dianalisis
MOBILedit Forensik Express Pro	Digunakan untuk aplikasi IMO Messenger pada proses pencitraan fisik *smartphone* atau *backup* data
Autopsi	Digunakan untuk analisis file media tambahan pada *file* yang diekstraksi
Konektor USB	Digunakan untuk memberikan akses penuh ke *smartphone* dari komputer
Portable Power Supply	Untuk menjaga baterai *Smartphone* tetap "hidup" dengan konstan
Tas Faraday	Wadah untuk melindungi ponsel dari transmisi data

1.4 HASIL DAN PEMBAHASAN

Prosedur penerapan kerangka NIJ dan ACPO pada forensik IMO Messenger akan dibahas di bagian ini. Prosedur ini menjelaskan secara rinci bagaimana mengumpulkan, memeriksa, dan menguraikan data forensik pada platform IMO Messenger menggunakan ide dan teknik yang ditemukan dalam kerangka ACPO dan NIJ.

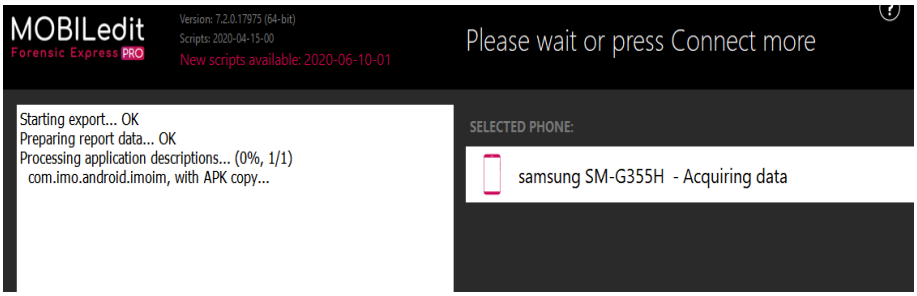
1.4.1 MOBILedit Forensic Express Pro

Data digital dari berbagai *file* pelaporan digunakan dalam hasil ini. MOBILEdit Forensics Express Pro memfasilitasi akuisisi data fisik dan logis. Data dari *smartphone* dapat dipulihkan dengan MOBILEdit Forensics Express Pro. MOBILEdit Forensic Express Pro dapat digunakan untuk menemukan IMEI (*International Mobile Equipment Identity*) ponsel, serta ICCID dan IMSI kartu SIM yang tidak terdaftar. Menggunakan MOBILEdit Forensic Express Pro, informasi kontak, pesan teks, video, foto, dan data lainnya berhasil ditemukan.



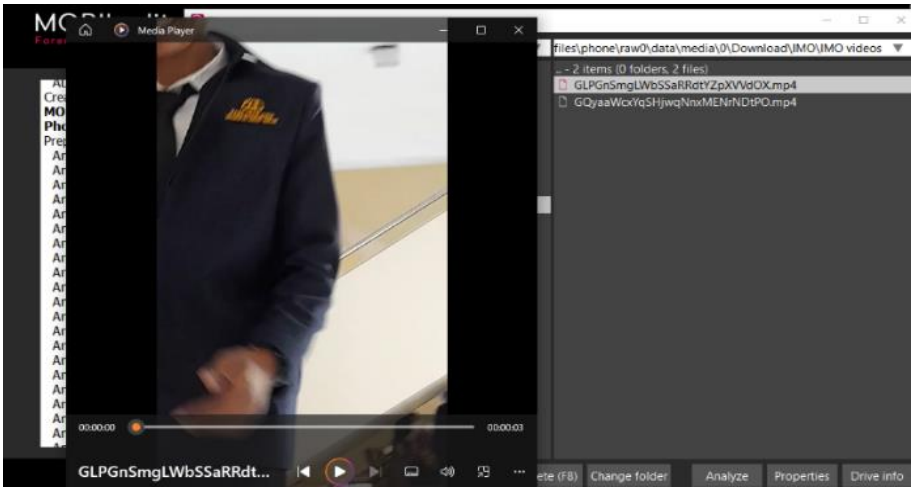
Gambar 1.4 Tahap awal akuisisi penggunaan MOBILEdit Forensic Express Pro

Langkah pertama dalam memanfaatkan alat MOBILEedit Forensic Express Pro untuk mengumpulkan data dari *smartphone* atau bukti nyata digambarkan pada Gambar 1.4. Untuk mulai mengumpulkan data forensik, prosedur ini harus terlebih dahulu melampirkan barang bukti ke PC atau laptop menggunakan kabel USB.



Gambar 1.5 Proses perolehan bukti digital menggunakan MOBILEdit Forensic Express Pro

Gambar 1.5 memudahkan untuk melihat langkah-langkah yang terlibat dalam pengumpulan bukti digital. Bukti digital yang diperoleh berupa *file* laporan PDF. Ada berbagai bukti dalam *file* ini, termasuk artefak video. Artefak video merupakan komponen penting dari bukti digital yang berhasil dikumpulkan, dan metode ini menunjukkan upaya untuk mengumpulkan data terkait dan bukti detail yang dapat digunakan untuk penelitian tambahan.

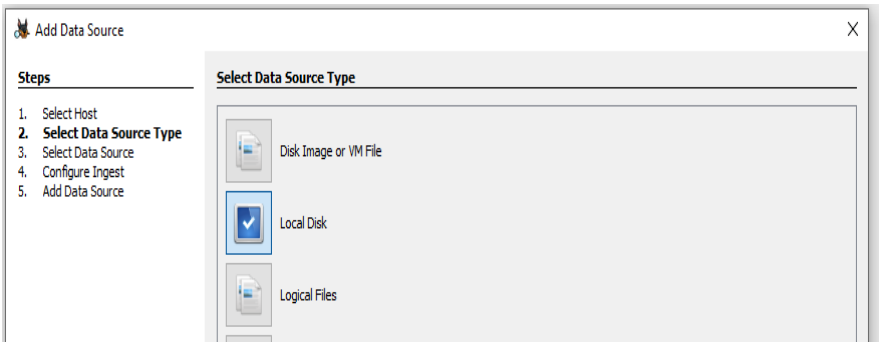


Gambar 1.6 Gambar digital di MOBILEdit forensik exspress Pro

Hasil video artefak yang berhasil ditemukan dengan MOBILEedit Forensic Express Pro ditampilkan pada Gambar 5. Prosedur ini menunjukkan kemampuan untuk menemukan jejak video, yang sangat penting untuk penyelidikan forensik. Secara khusus, penggunaan alat forensik ini memberikan penyelidik representasi visual dari artefak video, yang dapat menjadi bukti penting. Hasil ini mungkin dapat menjelaskan lebih lanjut mengenai karakteristik dan latar dari bukti digital yang diperoleh secara efektif.

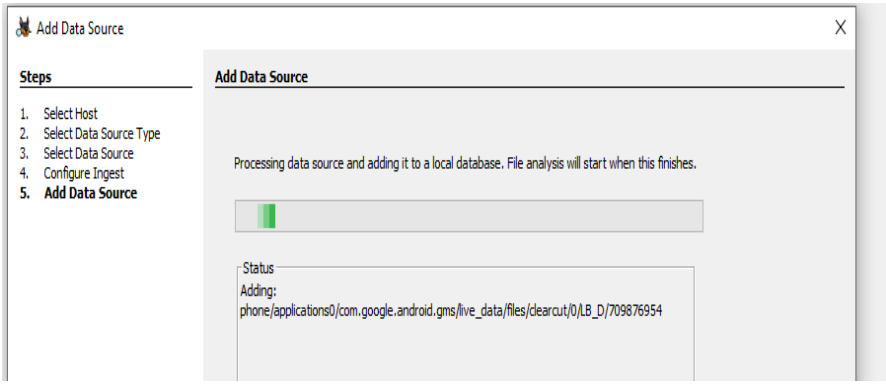
1.4.2 AUTOPSY

Autopsy adalah alat atau *software* forensik digital yang digunakan untuk menganalisis data dari berbagai sumber, seperti *hard drive*, perangkat seluler, dan media penyimpanan lainnya. Autopsy adalah alat yang umum digunakan oleh spesialis forensik digital untuk memeriksa data digital terkait kasus atau kasus kriminal tertentu. Ekstraksi, analisis, dan visualisasi data yang dapat memberikan wawasan tentang tindakan dan jalur digital yang relevan dapat difasilitasi oleh program ini. Hasil proses ekstraksi dari alat Autopsy, ditunjukkan pada Gambar 1.7.



Gambar 1.7 Memilih jenis sumber data menggunakan Autopsi

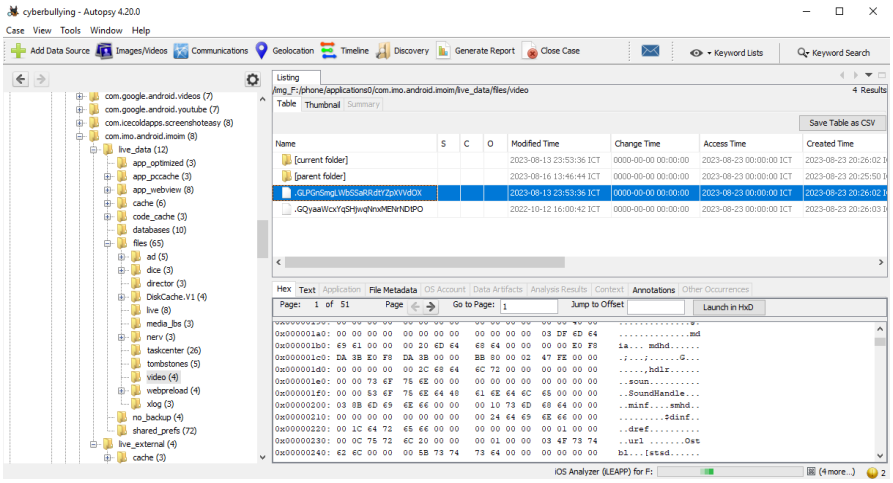
Langkah-langkah dalam memilih jenis data yang akan digunakan dengan Autopsi digambarkan pada Gambar 1.7. Tipe data *disk* lokal digunakan untuk struktur penelitian ini. Menggunakan Autopsi untuk mencari dan menyelidiki data pada *disk* lokal tersebut disediakan oleh prosedur pemilihan ini, yang menyarankan penekanan pada analisis data dari penyimpanan lokal. Penelitian masing-masing prosedur ini penting untuk melakukan analisis forensik pada sumber data tertentu.



Gambar 1.8 Proses pencitraan digital menggunakan Autopsi

Prosedur pemindaian digital otopsi digambarkan pada Gambar 1.8 proses analisis dilakukan selanjutnya, setelah perolehan data berhasil melalui pemindaian. Data yang dipindai akan diperiksa secara menyeluruh sebagai bagian dari penelitian ini untuk mencari

potensi artefak digital, pola, atau informasi lain yang mungkin relevan dengan penyelidikan. Langkah mendasar dalam pendekatan forensik digital yang digunakan untuk memperoleh pemahaman menyeluruh tentang bukti yang sudah ada adalah prosedur pemindaian dan analisis.



Gambar 1.9 Gambar digital pada Autopsy

Temuan penggunaan Autopsy untuk mengidentifikasi artefak gambar yang ditemukan ditampilkan pada Gambar 1.9. Prosedur ini menunjukkan keberhasilan dalam menemukan jejak visual, yang seringkali merupakan komponen penting dalam penyelidikan forensik. Analisis artefak fotografi menggunakan Autopsi dapat memberikan penjelasan tambahan pada bukti digital yang digunakan dalam penyelidikan. Identifikasi artefak foto dapat menghasilkan wawasan yang signifikan mengenai fitur dan konteks data yang diperiksa, sehingga memperkuat teknik investigasi digital yang komprehensif.

Hasil analisis bukti forensik digital dapat dibandingkan dengan informasi dari bukti yang ditemukan pada skenario kasus *cyberbullying*. Karena MOBILEdit Forensic Express Pro dapat mengumpulkan berbagai bukti, termasuk pesan teks, foto, video, ID pengguna, data yang dihapus, dan informasi grup, ini adalah alat terbaik untuk verifikasi. Namun penggunaan aplikasi Autopsi hanya

memungkinkan perolehan rekaman video sebagai bukti digital. Dalam kasus *cyberbullying*, semua video yang dikumpulkan sebagai bukti terbukti menjadi data yang paling penting dan vital. Hasil perbandingan barang bukti digital menurut kemampuan alat forensik disajikan pada Tabel 1.2.

Tabel 1.2 Hasil alat forensik

Framework	Parameter Bukti	Alat Forensik	
		MOBILEdit Forensic Express Pro	Autopsi
ACPO	Pesan teks	✓	-
	Video	✓	✓
	ID Pengguna	✓	-
	Data yang Dihapus	✓	-
	Foto	✓	-
	Grup	✓	-
NIJ	Pesan teks	✓	-
	Video	✓	✓
	ID Pengguna	✓	-
	Data yang Dihapus	✓	-
	Foto	✓	-
	Grup	✓	-
Persentase%		100	33.3

Peneliti menghitung angka indeks berdasarkan hasil eksperimen untuk menentukan nilai setiap alat forensik. rumus (1.1) memberikan penjelasan bagaimana angka indeks dihitung sebagai total skor yang memasukkan unsur-unsur evaluasi terkait. Pendekatan ini memfasilitasi pengetahuan komprehensif tentang kontribusi dan kinerja masing-masing alat forensik dalam kerangka penyelidikan forensik tertentu dengan menawarkan gambaran yang teratur dan dapat diukur tentang efektivitas alat tersebut.

$$Pon = \frac{\sum pn}{\sum po} \; x \; 100\% \qquad (1.1)$$

Note: $\sum pn$ mewakili seluruh jumlah data digital yang diperoleh, $\sum po$ mewakili seluruh data digital dalam aplikasi pesan instan, dan Persamaan Pon mewakili skor persentase kerentanan anti-forensik aplikasi (Aziz dkk., 2021).

MOBILEdit Forensic Exspress: $Pon = \frac{6}{6} \; x \; 100\% = 100\%$

Autopsi: $Pon = \frac{1}{6} \; x \; 100\% = 33.3\%$

Perbedaan antara metode NIJ dan ACPO hanya terletak pada tahapan kerangkanya. Teknik ACPO terdiri dari empat tahap: *Plan, Capture, Analysis,* dan *Present*. Sedangkan NIJ memiliki 5 tahapan yaitu *Identification, Collection, Examination, Analysis*, dan *Reporting*. Metode NIJ lebih komprehensif, mendalam, dan mudah dipahami. Karena MOBILEdit Forensic Express Pro menggunakan rumus (1.1) untuk enentukan indeks untuk setiap alat forensik, MOBILEdit Forensic Express Pro memiliki keunggulan besar dibandingkan instrumen forensik lainnya dalam hal kemampuan untuk menemukan bukti berdasarkan kriteria yang disebutkan. Nilai indeksnya paling tinggi yaitu 100%. 33,3% merupakan nilai indeks Autopsy.

1.5 KESIMPULAN

Kerangka kerja ACPO dan NIJ telah digunakan untuk menganalisis kejadian *cyberbullying* dari aplikasi IMO Messenger. Berikut beberapa hasil analisis dari penyelidikan tersebut. Tahapan terlengkap tertuang dalam kerangka NIJ yang dinilai paling baik karena mendukung proses penyidikan. Verifikasi alat forensik secara keseluruhan menunjukkan bahwa video adalah jenis bukti yang paling umum. MOBILedit Forensic Express Pro adalah alat forensik *mobile* paling mumpuni; ini memiliki tingkat keberhasilan 100%. Autopsy

memiliki tingkat keberhasilan hanya 33,3%. Hasil perbandingan seluruh solusi forensik didasarkan pada penelitian yang menunjukkan seberapa baik kinerja alat forensik MOBILedit Forensic Express Pro dalam tugas ekstraksi data. Tujuan penelitian terpenuhi, memungkinkan peneliti untuk mengungkap dan menganalisis kedua *framework* forensik.

DAFTAR PUSTAKA

Adamu, H., Ahmad, A. A., Hassan, A., & Gambasha, S. B. (2021). Web Browser Forensic Tools: Autopsy, BHE and Net Analysis. *International Journal of Research and Innovation in Applied Science*, *06*(05), 103–107. https://doi.org/10.51584/ijrias.2021.6506

Al-Garadi, M. A., Hussain, M. R., Khan, N., Murtaza, G., Nweke, H. F., Ali, I., Mujtaba, G., Chiroma, H., Khattak, H. A., & Gani, A. (2019). Predicting Cyberbullying on Social Media in the Big Data Era Using Machine Learning Algorithms: Review of Literature and Open Challenges. *IEEE Access*, *7*, 70701–70718. https://doi.org/10.1109/ACCESS.2019.2918354

Al-Rawashdeh, A. M., Al-Sharif, Z. A., Al-Saleh, M. I., & Shatnawi, A. S. (2020). A Post-Mortem Forensic Approach for the Kik Messenger on Android. *2020 11th International Conference on Information and Communication Systems, ICICS 2020*, 79–84. https://doi.org/10.1109/ICICS49469.2020.239559

Al-Sabaawi, A., & Foo, E. (2019). A Comparison Study of Android Mobile Forensics for Retrieving Files System. *Ernest Foo International Journal of Computer Science and Security (IJCSS)*, *13*, 2019–2148.

Alanda, A., Satria, D., Mooduto, H. A., & Kurniawan, B. (2020). Mobile Application Security Penetration Testing Based on OWASP. *IOP Conference Series: Materials Science and Engineering*, *846*(1). https://doi.org/10.1088/1757-899X/846/1/012036

ALThebaity, M., Mishra, S., & Shukla, M. K. (2020). Forensic Analysis of Third-party Mobile Application. *Helix*, *10*(4), 32–38. https://doi.org/10.29042/2020-10-4-32-38

Atlam, H. F., El-Din Hemdan, E., Alenezi, A., Alassafi, M. O., & Wills, G. B. (2020). Internet of Things Forensics: A Review. *Internet of Things (Netherlands)*, *11*, 100220. https://doi.org/10.1016/j.iot.2020.100220

Aurelia, A., Basbeth, F., & Arifandi, F. (2023). Analisa Kedudukan Pemberian Keterangan Ahli Terhadap Proses Ilmu Forensik dan Tinjauannya Menurut Hukum Islam Analysis Position of Expert Information on the Forensic Science Process and According to Islamic Law. *Comserva: Jurnal Penelitian dan Pengabdian Masyarakat*, *03*(01), 411–428. https://doi.org/10.59141/comserva.v3i1.646

Aziz, M. A., Sulistyo, W. Y., & Astari, S. R. (2021). Komparatif Anti Forensik Aplikasi Instant Messaging Berbasis Web Menggunakan Metode Association of Chief Police Officers (ACPO). *Jurnal Riset Teknologi Informasi dan Komputer (JURISTIK)*, *1*(1), 8–15. https://doi.org/10.53863/juristik.v1i01.341

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), 125–130. https://doi.org/10.30595/techno.v21i2.8494

Choi, J., Yu, J., Hyun, S., & Kim, H. (2019). Digital forensic analysis of encrypted database files in instant messaging applications on Windows operating systems: Case study with KakaoTalk, NateOn and QQ messenger. *Digital Investigation*, *28*, S50–S59. https://doi.org/10.1016/j.diin.2019.01.011

Dewi, E. H. K., Suharso, A., & Rozikin, C. (2022). Implementasi Cosine Similarity Dalam Analisis Investigasi Cyberbullying Pada Twitter Dengan Framework Nist. *Cyber Security dan Forensik Digital*, *5*(1), 12–22. https://doi.org/10.14421/csecurity.2022.5.1.3397

Dweikat, M., Eleyan, D., & Eleyan, A. (2021). Digital Forensic Tools Used in Analyzing Cybercrime. *Journal of University of Shanghai for Science and Technology*, *23*(3), 367–379. https://doi.org/10.51201/jusst12621

Fanani, G., Riadi, I., & Yudhana, A. (2022). Analisis Forensik Aplikasi Michat Menggunakan Metode Digital Forensics

Research Workshop. *Jurnal Media Informatika Budidarma*, *6*(2), 1263–1271. https://doi.org/10.30865/mib.v6i2.3946

Ferguson, R. I., Renaud, K., Wilford, S., & Irons, A. (2020). PRECEPT: a framework for ethical digital forensics investigations. *Journal of Intellectual Capital*, *21*(2), 257–290. https://doi.org/10.1108/JIC-05-2019-0097

Feucht, T. (2021). The National Institute of Justice (NIJ). *The Encyclopedia of Research Methods in Criminology and Criminal Justice: Volume II: Parts 5-8*, *II*, 800–803. https://doi.org/10.1002/9781119111931.ch152

Goldstraw-White, J. (2022). *Legal and Policy Framework for Dogital Forensics: A Resource for Practitioners: A Policy and Practice Briefing from the Digital Forensics and Social Media project funded by the Dawes Trust Copyright* (Nomor September).

Horsman, G. (2020). ACPO principles for digital evidence: Time for an update? *Forensic Science International: Reports*, *2*(January), 100076. https://doi.org/10.1016/j.fsir.2020.100076

Hou, J., Li, Y., Yu, J., & Shi, W. (2020). A Survey on Digital Forensics in Internet of Things. *IEEE Internet of Things Journal*, *7*(1), 1–15. https://doi.org/10.1109/JIOT.2019.2940713

Ichsan, A. N., & Riadi, I. (2021). Mobile Forensic on Android-based IMO Messenger Services using Digital Forensic Research Workshop (DFRWS) Method. *International Journal of Computer Applications*, *174*(18), 34–40. https://doi.org/10.5120/ijca2021921076

Kebande, V. R., & Venter, H. S. (2019). A comparative analysis of digital forensic readiness models using CFRaaS as a baseline. *WIREs Forensic Science*, *1*(6), 1–12. https://doi.org/10.1002/wfs2.1350

Khairunisa, T., & Priyana, P. (2022). Kedudukan Alat Bukti Forensik dalam Proses Pembuktian Perkara Pidana Aborsi. *Wajah Hukum*, *6*(1), 1–5. https://doi.org/10.33087/wjh.v6i1.614

Khairunnisa, C., & Zulfan. (2023). Manfaat Ilmu Forensik dalam Hukum Pidana. *Cendekia: Jurnal Hukum, Sosial & Humaniora*, *1*(1), 1–12. https://doi.org/10.33087/wjh.v6i1.614

Khanafseh, M., Qatawneh, M., & Almobaideen, W. (2019). A survey of various frameworks and solutions in all branches of digital forensics with a focus on cloud forensics. *International Journal*

of Advanced Computer Science and Applications, *10*(8), 610–629. https://doi.org/10.14569/ijacsa.2019.0100880

Kolla, V. R. K. (2022). A Comparative Analysis of OS Forensics Tools. *International Journal for Research in Applied Science and Engineering Technology*, *10*(11), 494–502. https://doi.org/10.22214/ijraset.2022.47346

Nurhairani, H., & Riadi, I. (2019). Analysis Mobile Forensics on Twitter Application using the National Institute of Justice (NIJ) Method. *International Journal of Computer Applications*, *177*(27), 35–42. https://doi.org/10.5120/ijca2019919749

Patil, R. Y., & Devane, S. R. (2022). Network Forensic Investigation Protocol to Identify True Origin of Cyber Crime. *Journal of King Saud University - Computer and Information Sciences*, *34*(5), 2031–2044. https://doi.org/10.1016/j.jksuci.2019.11.016

Pribadi, B., Rosdiana, S., & Arifin, S. (2023). Digital forensics on facebook messenger application in an android smartphone based on NIST SP 800-101 R1 to reveal digital crime cases. *Procedia Computer Science*, *216*(2022), 161–167. https://doi.org/10.1016/j.procs.2022.12.123

Ramadhan, R. A., & Mualfah, D. (2020). 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*, *5*(2), 183–192. https://doi.org/10.25299/itjrd.2021.vol5(2).5750

Riadi, I., Herman, H., & Rafiq, I. A. (2022). Mobile Forensic Investigation of Fake News Cases on Instagram Applications with Digital Forensics Research Workshop Framework. *International Journal of Artificial Intelligence Research*, *6*(2), 1–9. https://doi.org/10.29099/ijair.v6i2.311

Riadi, I., Yudhana, A., & Barra, M. A. (2021). Forensik Mobile pada Layanan Media Sosial LinkedIn. *JISKa: Jurnal Informatika Sunan Kalijaga*, *6*(1), 9–20. https://doi.org/10.14421/jiska.2021.61-02

Riadi, I., Yudhana, A., & Fanani, G. P. I. (2023). Comparative Analysis of Forensic Software on Android-based MiChat using ACPO and DFRWS Framework. *Jurnal RESTI (Rekayasa Sistem dan Teknologi Informasi)*, *7*(2), 286–292.

https://doi.org/10.29207/resti.v7i2.4547

Ruslan, T., Riadi, I., & Sunardi, S. (2022). Forensik Multimedia Berbasis Mobile Menggunakan Metode National Institute of Justice. *Jurnal SAINTEKOM*, *12*(1), 69–80. https://doi.org/10.33020/saintekom.v12i1.210

Salih, K., & Dabagh, N. (2023). Digital Forensic Tools: A Literature Review. *Journal of Education and Science*, *32*(1), 109–124. https://doi.org/10.33899/edusj.2023.137420.1304

Sukamto, P., Ispandi, Putra, A. S., Aisyah, N., & Toufiq, R. (2022). Forensic Digital Analysis for CCTV Video Recording. *International Journal of Science, Technology & Management*, *3*(1), 284–291. https://doi.org/10.46729/ijstm.v3i1.460

Sunardi, Herman, & Ardiningtias, S. R. (2022). A Comparative Analysis of Digital Forensic Investigation Tools on Facebook Messenger Applications. *Journal of Cyber Security and Mobility*, *11*(5), 655–672. https://doi.org/10.13052/jcsm2245-1439.1151

Turanovic, J. J., & Siennick, S. E. (2022). The causes and consequences of school violence: A review. *School Violence: Causes, Prevention and Safety Measures*, *February*, 1–80. https://static1.squarespace.com/static/5b7ea2794cde7a79e7c00582/t/63762f5db88a7a5f5f822573/1668689758430/causes+school+violence.pdf

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. https://doi.org/10.29207/resti.v4i6.2635

Yaacoub, J. P. A., Noura, H. N., Salman, O., & Chehab, A. (2022). Advanced digital forensics and anti-digital forensics for IoT systems: Techniques, limitations and recommendations. *Internet of Things (Netherlands)*, *19*. https://doi.org/10.1016/j.iot.2022.100544

Yao, M., Chelmis, C., & Zois, D. S. (2019). Cyberbullying ends here: Towards robust detection of cyberbullying in social media. *In The World Wide Web Conference*, 3427–3433. https://doi.org/10.1145/3308558.3313462

Zhu, C., Huang, S., Evans, R., & Zhang, W. (2021). Cyberbullying Among Adolescents and Children: A Comprehensive Review of the Global Situation, Risk Factors, and Preventive Measures. *Frontiers in Public Health*, *9*, 1–12. https://doi.org/10.3389/fpubh.2021.634909

Yana Safitri Seorang mahasiswa Magister Informatika di Universitas Ahmad Dahlan. Peminatan bidang keahlian adalah dalam bidang Forensik. Disiplin ilmunya adalah Forensik Digital, yang mencakup kasus-kasus *Cyberbullying* pada aplikasi pesan instan dan media sosial. Tesisnya berjudul "Analisis Investigasi Forensik Cyberbullying pada IMO Messenger Berbasis Android Menggunakan Kerangka Kerja Association of Chief Police Officers".

Imam Riadi merupakan Guru Besar dalam Bidang Ilmu Sistem Informasi sejak Tahun 2023. Peminatan bidang keahlian yang ditekuni: Keamanan Informasi, Keamanan Siber, Forensik Digital, dan Jaringan Komputer. Gelar Doktor didapatkan dari Program Studi Ilmu Komputer, Universitas Gadjah Mada pada tahun 2014. Gelar Magister didapatkan pada Program Studi Ilmu Komputer, Universitas Gadjah Mada pada tahun 2004. Gelar Sarjana didapatkan dari Program Studi Pendidikan Teknik Elektro, Universitas Negeri Yogyakarta (UNY) pada tahun 2001. Mulai Tahun 2002 sampai sekarang menjadi Dosen Tetap pada Program Studi Informatika Program Magister Universitas Ahmad Dahlan, Yogyakarta.

Sunardi merpakan seorang guru besar di Universitas Ahmad Dahlan. Ia mendapatkan gelar Ph.D. dari Universiti Teknologi Malaysia, Malaysia, di bidang teknik elektro. Disiplin ilmuninya meliputi teknik elektro dan telekomunikasi, sistem informasi komunikasi, dan komunikasi nirkabel. Sejak tahun 2016, ia menjadi dosen tetap di program Magister Informatika di Universitas Ahmad Dahlan (UAD). Mata kuliah yang dia ajarkan meliputi Metodologi Penelitian dan Publikasi, Teori Informasi, Proposal Tesis, dan Tesis.