

# Mobile Forensic Analysis on IMO Messenger Application Using ACPO and NIJ Frameworks

**Yana Safitri<sup>1</sup>, Firmansyah<sup>\*2</sup>, Muhammad Amirul Mu'min<sup>3</sup>**

<sup>1</sup>Ilmu Komputer, Sains dan Teknologi, Universitas Qamarul Huda Bagu

<sup>\*2</sup>Ilmu Komputer, Teknik, Universitas Islam Al-Azhar

<sup>3</sup>Ilmu Komputer, Teknik dan Ilmu Komputer, Universitas Muhammadiyah Bima

E-mail: <sup>1</sup>yana2107048011@webmail.uad.ac.id, <sup>\*2</sup>f.firman@unizar.ac.id,

<sup>3</sup>muhamirul98@gmail.com

## Abstrak

*The need for efficient digital forensic tools has become increasingly urgent with the rapid development of digital communication platforms. This study aims to compare forensic frameworks on the Android application IMO Messenger, focusing on the Association of Chiefs of Police (ACPO) and the National Institute of Justice (NIJ) frameworks. The research utilizes the forensic tools MOBILEdit Forensic Express and Autopsy. The primary objective of the study is to gather evidence related to a body-shaming case. The findings show that MOBILEdit Forensic Express Pro achieved a 100% extraction rate, while Autopsy managed only 3.33%. By adhering to the guidelines established by ACPO and NIJ, the data extraction process was conducted following legitimate and accountable procedures. The use of certified tools and appropriate methods ensured that the extracted data remained accurate, valid, and reliable. These findings contribute to advancing knowledge in mobile forensics for addressing cyberbullying, providing valuable insights for investigators.*

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

## 1. PENDAHULUAN

Kemajuan teknologi *smartphone* menggunakan sistem android yang sudah dilengkapi dengan berbagai kemampuan canggih, kemajuan teknologi di dunia saat ini sangat cepat [1]. Manfaat *smartphone* tidak dapat disangkal [2]. Perkembangan forensik *smartphone* Android telah menciptakan potensi yang besar sekaligus tantangan yang menarik [3]. *Smartphone* Android itu sendiri adalah perangkat hibrida yang dapat berfungsi sebagai telepon dan juga beroperasi dengan cara yang lebih ringkas dan portabel dibandingkan dengan komputer [4]. Perkembangan forensik *smartphone* Android telah menciptakan potensi besar serta tantangan menarik [5].

Beberapa aplikasi sistem pesan instan yang bisa digunakan dalam *smartphone* android adalah WhatsApp, Telegram, Line, Kakaotalk, MiChat, IMO Messenger. Aplikasi ini telah berkembang menjadi sangat penting seiring dengan kemajuan era digital sebagai sarana komunikasi [6]. Penelitian ini menggunakan aplikasi pesan instan IMO Messenger sebagai objek, karena aplikasi tersebut belum mendapat perhatian yang memadai dalam konteks forensik digital. IMO

Messenger mempermudah komunikasi antar individu serta berbagi pendapat dan peristiwa sosial penting dibandingkan sebelumnya [7]. Banyak konten yang meragukan dan tidak akurat diproduksi dan dibagikan untuk tujuan yang dianggap menguntungkan [8]. Namun, di balik keuntungannya, program seperti ini juga membawa risiko penyalahgunaan, seperti *cybercrime*, yang dapat berdampak buruk pada individu [9]. Risiko terbesar bagi aplikasi pesan instan saat ini adalah *cyberbullying*. Para penyelidik harus melakukan analisis forensik pada perangkat korban dan tersangka untuk menemukan bukti digital guna memerangi *cyberbullying* yang berbasis pesan singkat [10]. Kategori ini mencakup kategori pelanggaran HAM, pelanggaran HAM terhadap organisasi, dan pelanggaran HAM terhadap masyarakat umum [11]. Salah satu efek merugikan yang saat ini mempengaruhi remaja adalah *cyberbullying* [12].

*Cyberbullying* merupakan bentuk perundungan atau kekerasan yang dilakukan melalui platform digital atau internet. Ini melibatkan penggunaan teknologi, seperti media sosial, pesan teks, email, atau situs web, untuk mengintimidasi, mengancam, atau menghina seseorang dengan tujuan merugikan mental atau emosional korban [13]. Oleh karena itu, investigasi *cyberbullying* menjadi sangat penting untuk mengidentifikasi pelaku, melindungi korban, dan mencegah dampak negatif yang lebih luas terhadap kesehatan mental serta keamanan digital individu [14].

Untuk membantu penyelidik dalam investigasi kejahatan dunia maya yang menggunakan perangkat seluler mengambil artefak, mendekripsi data, dan menganalisisnya, diperlukan teknologi forensik digital [15], [16]. Gambar 1. menunjukkan sejumlah sub-bidang keahlian di bidang investigasi forensik digital.



Gambar 1. Sub-bidang investigasi forensik digital

Gambar 1. merupakan sub-bidang forensik digital, salah satunya adalah forensik *mobile*, yang menjadi fokus utama dalam penelitian ini [17]. Forensik *mobile* merupakan sub-spesialisasi yang berfokus pada penangkapan atau pemulihan bukti digital dari perangkat seluler [18]. Namun, permasalahan sering muncul karena banyaknya alat forensik [19] yang dinilai tidak efektif [20]. Para peneliti menyatakan bahwa setiap alat forensik memiliki kelebihan dan kekurangan [21]. Untuk mendukung proses investigasi di bidang forensik digital, berbagai *tools* pun digunakan [22].

Ada beberapa *framework* yang digunakan pada forensik digital, yaitu *framework* NIST (*National Institute of Standards and Technology*) [23], ABC (*Acquisition, Analysis, and Reporting*), *Analysis Using Cloud Data*, ACPO dan NIJ. Penelitian ini menggunakan *Framework* ACPO dan NIJ. Dengan mengikuti pedoman dari ACPO dan NIJ, data yang diekstrak dari perangkat *mobile* dapat dipastikan bahwa hasilnya sah dan dapat diandalkan. Penggunaan alat yang sah dan prosedur yang benar akan menghasilkan data yang akurat, yang penting untuk analisis lebih lanjut [24]. *Framework* ACPO adalah *framework* yang mencakup empat tahapan inti: *identification*, *preservation*, *analysis*, dan *presentation* [25]. *Framework* NIJ melibatkan lima tahapan, yaitu tahap *identification*, *Collection*, *Examination*, *Analysis*, dan *Reporting* [26]. Untuk menjaga integritas bukti, teknik identifikasi, pelabelan, dan perekaman digunakan dalam langkah ini.

Sejumlah kegiatan merupakan bagian dari tahap pengumpulan, di mana informasi dikumpulkan untuk membantu perburuan bukti kejahatan digital. Pada langkah ini, prosedur digunakan untuk mengekstrak informasi dari sumber data yang relevan dan menjamin konsistensi bukti terhadap gangguan [27].

Studi tentang kejahatan digital telah dilakukan oleh sejumlah peneliti, seperti yang ditunjukkan pada Tabel 1.

Tabel 1. Perbandingan Penelitian terdahulu

Judul	Tools	Hasil
Analisis Forensik Aplikasi Diskord pada Android Berdasarkan ACPO <i>Framework</i>	MOBILEdit dan Autopsy	Dengan menggunakan <i>tools</i> Mobiledit forensic, hanya berhasil menemukan gambar, video, dan dokumen. Sedangkan dengan menggunakan Autopsy, berhasil menemukan ekstrak pesan teks pada cache aplikasi discord.
Komparatif Web-based Instan Messaging Vulnerability Menggunakan Metode Association of Chief Police Officers	FTK Imager dan OSForensik	Hasil vulnerability tertinggi didapat pada aplikasi Skype berbasis web, yaitu sebesar 92%.
Investigasi Stego <i>File</i> Menggunakan <i>Framework</i> National Institute of Justice	FTK Imager, Autopsy, WinHex, Hiderman, dan StegSpy	Hasil ekstraksi menunjukkan bahwa dari 10 <i>file</i> yang diskenariokan telah disusupi Steganografi.
Investigasi Forensik Terhadap Bukti Digital dalam Lingkup Cybercrime	BitLocker Encryption, FTK Imager, dan Autopsy	<i>Tools</i> FTK Imager dan Autopsy masih belum mampu melakukan akuisisi dan analisis data dengan perlakuan penghapusan permanen dan enkripsi (password) pada flash disk menggunakan <i>tools</i> bawaan Windows 10 yaitu BitLocker Drive Encryption.
Perbandingan Hasil Recovery <i>Tools</i> Mobile Forensik di Smartphone Android Menggunakan Metode National Institute of Justice (NIJ) Penelitian ini	Andriller dan MOBILEdit Forensic Express Pro MOBILEdit Forensic Express Pro	Hanya Mobiledit Forensic Express Pro yang dapat melakukan recovery data yang telah dihapus dari objek penyelidikan sedangkan Andriller tidak dapat melakukan recovery terhadap data yang dihapus. MOBILEdit Forensics Express Pro mendapatkan hasil ekstraksi 100%, sementara Autopsy hanya 3,33%. Dengan mengikuti pedoman yang ditetapkan oleh ACPO dan NIJ proses ekstraksi data dilakukan dengan prosedur yang sah dan dapat dipertanggungjawabkan.

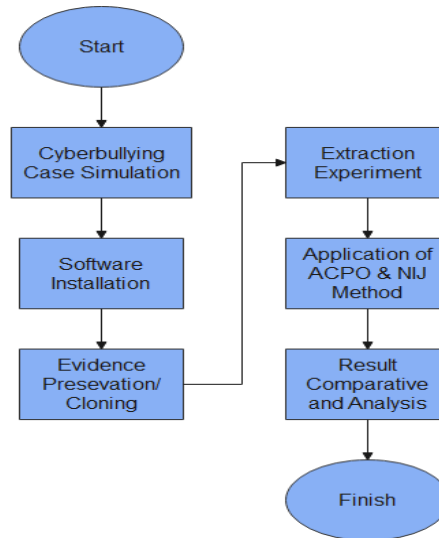
Tabel 1. menunjukkan perbandingan hasil penelitian sebelumnya dengan penelitian ini. Hasil penelitian ini diharapkan dapat membantu aparat penegak hukum dalam meningkatkan kemampuan dalam menyelidiki kasus yang melibatkan komunikasi melalui aplikasi IMO Messenger.

## 2. METODE PENELITIAN

Metode analisis studi kasus dan evaluasi aplikasi *smartphone* IMO Messenger menggunakan *framework* NIJ dan ACPO. Simulasi ini mempunyai tujuan untuk menganalisis dan membandingkan dua *framework* serta *tools* forensik yang ada untuk aplikasi IMO Messenger berbasis android. Tujuannya adalah memeriksa hasil temuan yang telah digunakan secara ilegal.

- 1) Topik penelitian yang akan dibahas lebih rinci. Pada tahap ini, penelitian menggunakan berbagai metode untuk mengumpulkan informasi mengenai mekanisme-mekanisme penelitian.
- 2) Tinjauan pustaka hendaknya menghimpun seluruh informasi yang ada mengenai penelitian serta menyusun kerangka kerja penelitian yang lebih mendalam dan obyektif bagi para peneliti. Hal ini menjamin bahwa strategi tersebut dapat diterapkan di masa depan.

Study Kasus penelitian menggunakan MOBILEdit Forensic Express Pro dan Autopsy untuk melakukan analisis forensik pada aplikasi IMO Messenger berbasis Android. *Flowchart* investigasi dapat dilihat pada Gambar 2.



Gambar 2. *Flowchart* investigasi

Gambar 2. merupakan *flowchart* investigasi dan dijelaskan sebagai berikut:

- 1) IMO Messenger berbasis Android digunakan untuk mensimulasikan kasus *cyberbullying*.
- 2) Seorang saksi ahli menjelaskan tahapan-tahapan untuk menginstall *tools* forensic pada laptop yang akan dipakai untuk menganalisis serta mengumpulkan data atau bukti digital.
- 3) Penyidik harus memastikan perlindungan bukti fisik dengan mengaktifkan *plane mode* pada *smartphone* agar data asli tetap utuh.
- 4) Penyelidik menerapkan berbagai teknik forensic untuk mengekstraksi data dari *smartphone*. *Tool* untuk memindai secara fisik menggunakan MOBILEdit Forensic Express Pro, dan *tool* yang digunakan untuk mengekstrak data digital dari *file* multimedia adalah Autopsy.
- 5) Peneliti mengidentifikasi strategi untuk membantu peneliti dalam melaksanakan kerja lapangan penelitian ini. Penelitian ini menggunakan dua buah *framework* yaitu *framework* ACPO dan NIJ.
  - a. Empat tahapan ACPO adalah:
    - Plan (Perencanaan)*  
Merencanakan proses secara menyeluruh, mencakup identifikasi tujuan, menentukan data yang dibutuhkan, dan merancang metode untuk mengumpulkan informasi.
    - Capture (Pengumpulan)*  
Mengumpulkan data yang telah direncanakan, dapat dengan berbagai metode seperti survei, wawancara, observasi, atau mengakses sumber data lainnya.
    - Analysis (Analisis):*  
Data yang dikumpulkan dianalisis untuk menemukan pola, tren, atau wawasan yang dapat membantu dalam pengambilan keputusan.
    - Present (Presentasi)*  
Hasil dari analisis disajikan. Presentasi bisa berupa laporan, visualisasi data, atau presentasi langsung. Tujuannya untuk menyampaikan informasi dengan cara yang jelas dan mudah dipahami [28].
  - b. NIJ terdiri dari 5 tahapan yaitu:
    - Identification (Identifikasi)*  
Menentukan perangkat atau media yang perlu dicek, misalnya komputer, ponsel, atau perangkat penyimpanan lainnya.
    - Collection (Pengumpulan)*  
Pengumpulan bukti setelah diidentifikasi melibatkan pencadangan data, pengambilan Salinan forensic perangkat, dan mengumpulkan informasi yang berkaitan dengan investigasi.
    - Examination (Pemeriksaan)*

Pemrosesan dan verifikasi bukti yang telah dikumpulkan, bertujuan untuk menemukan informasi yang relevan dan untuk memastikan integritas data tidak rusak selama pengumpulan.

*Analysis (Analisis)*

Bukti yang telah diperiksa dianalisis lebih lanjut untuk mengidentifikasi pola informasi yang dapat digunakan untuk mendukung atau membantah teori atau hipotesis dalam penyelidikan.

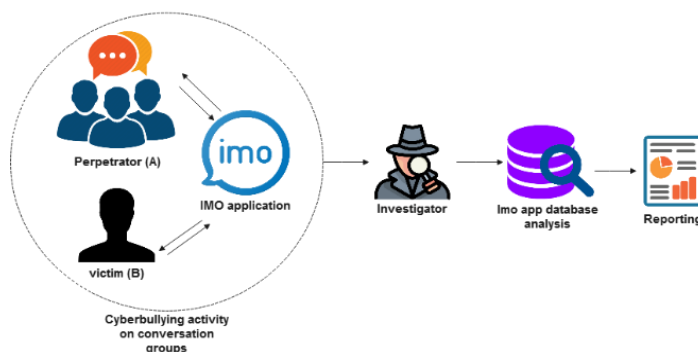
*Reporting (Pelaporan)*

Penyusunan laporan yang menjelaskan temuan dari seluruh investigasi. Laporan harus menyajikan hasil analisis secara jelas dan dapat dipahami, serta menyarankan langkah selanjutnya jika diperlukan. Selain itu, laporan ini juga bisa digunakan sebagai bukti di pengadilan atau untuk tujuan hukum lainnya [29].

- 6) Berdasarkan karakteristik program dan sidik jari digital yang dianalisis, hasil yang diperoleh dari masing-masing alat forensik akan disajikan dan dievaluasi secara transparan. Parameter yang digunakan untuk penelitian, khususnya evaluasi layanan IMO Messenger berbasis Android.

2.1. Skenario Penelitian

Aplikasi yang digunakan untuk mensimulasikan skenario *cyberbullying* adalah aplikasi IMO Messenger berbasis android. Gambar 3 merupakan skenario *cyberbullying* yang menggambarkan interaksi antara korban dengan pelaku.



Gambar 3. Skenario kasus

Gambar 3. mengilustrasikan simulasi yang didasarkan pada percakapan group pada aplikasi IMO Messenger berbasis android yang berakhir secara tiba-tiba. Korban *bullying* terjadi kepada satu anggota dalam group tersebut. Simulasi ini menunjukkan contoh *cyberbullying* dimana ada beberapa pelaku berinteraksi dengan korban yang ada pada group tersebut. Dalam kejadian ini, pelaku melakukan percakapan dengan korban menggunakan aplikasi IMO Messenger berbasis android. Salah satu perangkat yang digunakan pelaku dan didapatkan yaitu *smartphone* Samsung Galaxy Core 2, yang kemudian akan diinvestigasi oleh penyidik.

2.2. Alat Penelitian

Banyak alat yang diperlukan untuk mentransfer data dari aplikasi yang digunakan ke alat yang digunakan. Alat penelitian yang digunakan dapat diklasifikasikan menjadi dua kategori utama: *Hardware* dan *Software*. Beberapa alat penelitian yang diterapkan dalam percobaan ini untuk mengumpulkan data dan informasi mengenai aplikasi IMO Messenger ditunjukkan pada Tabel 2.

Tabel 2. *Hardware* dan *Software* pendukung

<i>Hardware dan Software</i>	<i>Fungsi</i>
Laptop	Untuk melakukan pengiriman data digital, untuk memindahkan data dari <i>smartphone</i> ke perangkat penyimpanan untuk dianalisis.
<i>Smartphone</i>	Menyimpan data penting seperti pesan, panggilan, dan media yang dapat digunakan sebagai bukti dalam investigasi.
MOBILEdit Forensik Express Pro	Proses ekstraksi atau pencadangan data pada <i>smartphone</i> , digunakan untuk aplikasi IMO Messenger berbasis android.

Autopsy	Untuk analisis <i>file</i> media yang telah diekstraksi.
Cable USB	Memberikan akses penuh melalui computer ke <i>smartphone</i> .
Charger Smartphone dan Laptop	Untuk memperpanjang daya agar baterai laptop dan <i>smartphone</i> tetap "hidup" secara konstan.
Tas Faraday	Media untuk melindungi <i>smartphone</i> selama proses pengiriman dan penyimpanan data.

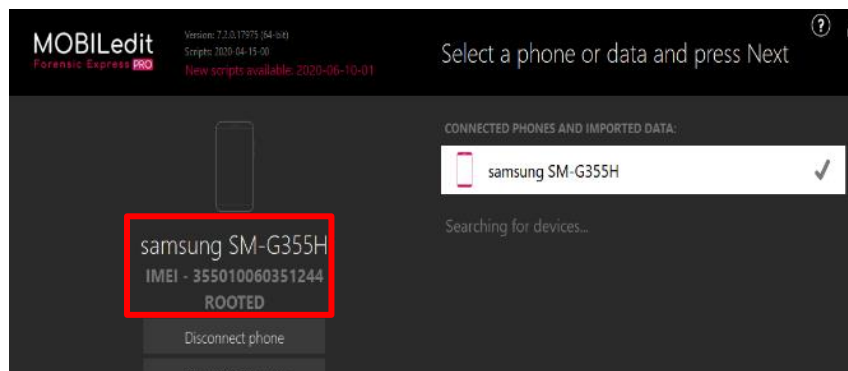
Alat yang tercantum pada Tabel 2 sangat krusial dalam memastikan kelengkapan analisis forensik yang dilakukan, karena setiap perangkat ini memiliki peran penting dalam mendukung proses identifikasi, pengumpulan, dan pemeriksaan bukti digital. Dengan menggunakan alat-alat tersebut, peneliti dapat menjamin bahwa semua tahap analisis dilakukan secara menyeluruh dan akurat, serta membantu memverifikasi konsistensi dan ketepatan hasil yang diperoleh selama proses investigasi. Hal ini penting untuk memastikan bahwa setiap temuan forensik yang dihasilkan dapat dipertanggungjawabkan dan memenuhi standar keandalan yang dibutuhkan dalam suatu penyelidikan.

### 3. HASIL DAN PEMBAHASAN

Prosedur penerapan *framework* NIJ dan ACPO pada forensik IMO Messenger. Prosedur ini menjelaskan langkah-langkah untuk mengumpulkan, memeriksa, serta melindungi data forensik di *platform* IMO Messenger, dengan menggunakan teknik dan konsep yang terdapat pada *framework* ACPO dan NIJ.

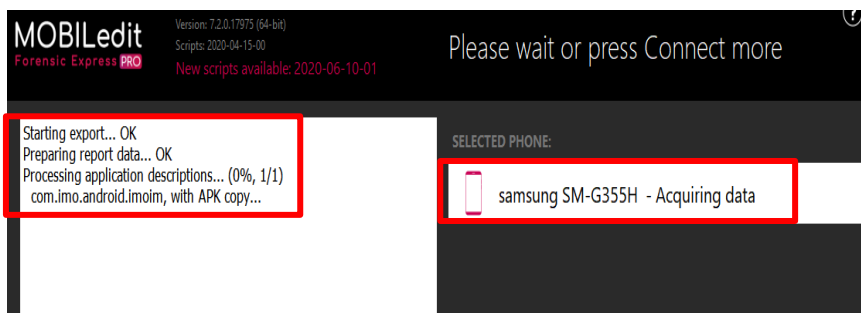
#### 3.1. MOBILEdit Forensic Express Pro

Data yang didapat untuk berkas pelaporan adalah data digital. MOBILEdit Forensic Express Pro memberikan fasilitas untuk menganalisis data fisik dan digital. Data barang bukti fisik dapat diekstraksi dengan MOBILEdit Forensics Express Pro. Penyidik dapat menggunakan MOBILEdit Forensics Express Pro untuk mengambil IMEI (*International Mobile Equipment Identity*) yang hilang atau tidak terbaca serta kartu SIM ICCID dan IMSI. Memanfaatkan MOBILEdit Forensics Express Pro, informasi video, ID, gambar, pesan teks, group, dan data lainnya berhasil diidentifikasi, dapat dilihat pada Gambar 4.



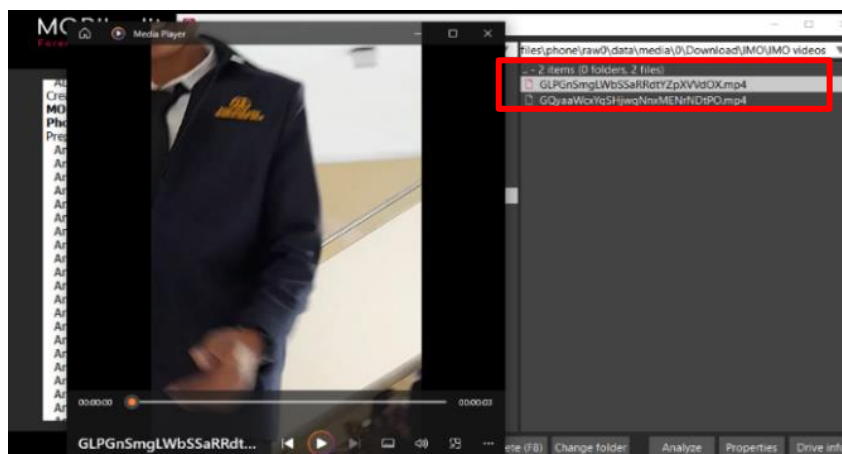
Gambar 4. Penilaian awal pengguna MOBILEdit Forensic Express Pro

Tahap pertama, menggunakan MOBILEedit Forensics Express Pro untuk mengumpulkan data dari barang bukti fisik yang ditunjukkan pada Gambar 4. Sebelum melanjutkan pengumpulan bukti forensik, prosedur ini harus diselesaikan sesegera mungkin dengan menggunakan kabel USB untuk menghubungkan hard drive ke PC atau laptop yang dapat dilihat pada Gambar 5.



Gambar 5. langkah mendapatkan bukti digital menggunakan MOBILEdit Forensic Express Pro

Gambar 5. mempermudah untuk melihat berbagai permasalahan yang muncul saat menggunakan *tools* forensic ini. Bukti digital yang dihasilkan dalam bentuk *file* PDF. Terdapat berbagai macam *file* yang didapat sebagai bukti, termasuk artefak video. Artefak video merupakan komponen penting dari bukti digital yang ditemukan. Bukti artefak video yang ditemukan dapat dilihat pada Gambar 6.

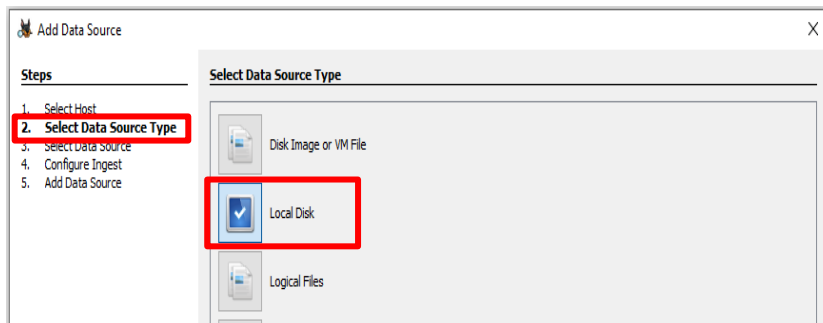


Gambar 6. Artefak vidio di MOBILEdit Forensic Expression Pro

Hasil artefak video yang diperoleh menggunakan *tool* ini ditunjukkan pada Gambar 6. Prosedur tersebut menunjukkan kemampuan *tool* forensic dalam mengidentifikasi artefak video secara efektif, yang merupakan aspek krusial dalam proses penyelidikan forensic. Penerapan *tool* forensic ini memungkinkan penyidik mendapatkan representasi visual dari artefak video, yang dapat berfungsi sebagai bukti digital yang signifikan. Selain itu, hasil ini memberikan detail lebih mendalam mengenai karakteristik dan keluaran bukti digital yang dihasilkan secara efisien, sehingga mendukung proses investigasi secara optimal.

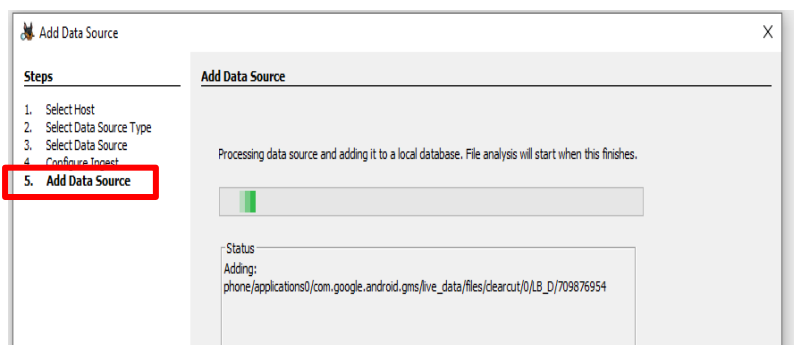
### 3.2. Autopsy

Autopsy, juga dikenal sebagai perangkat lunak forensic digital, yang diterapkan untuk menganalisis data dari berbagai sumber, termasuk *hard drive*, perangkat *mobile*, dan perangkat penyimpanan lainnya. Autopsy adalah *tool* forensic yang biasanya digunakan oleh praktisi forensic digital untuk menganalisis bukti digital yang berkaitan dengan suatu kasus atau perkara pidana. Program ini dapat memfasilitasi analisis, visualisasi, dan ekstraksi data tentang konten dan garis waktu digital yang relevan. Hasil proses Autopsy disajikan pada Gambar 7.



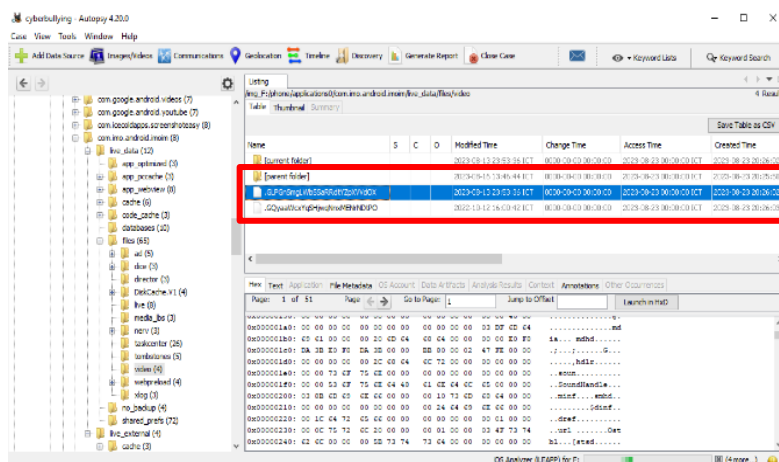
Gambar 7. Memilih tipe data menggunakan Autopsy

Tahapan dalam menentukan *Type* data yang akan diproses menggunakan Autopsy ditunjukkan pada Gambar 7. Jenis tipe data penelitian yang akan digunakan pada penelitian ini adalah *Local Disk Type*. Prosedur akuisisi data memanfaatkan Autopsy untuk menemukan dan mengumpulkan data dari *local disk*, dengan menekankan analisis data yang tersimpan di penyimpanan lokal. Analisis setiap prosedur individu sangat krusial untuk melakukan *scanning* forensik terhadap kumpulan data yang relevan, proses *scanning* dapat dilihat pada Gambar 8.



Gambar 8. Proses scanning digital menggunakan Autopsy

Proses pemindaian digital menggunakan Autopsy diilustrasikan pada Gambar 8, dan analisis dilakukan setelah data berhasil diekstraksi melalui proses pemindaian. Peneliti meneliti data yang telah dikumpulkan secara menyeluruh untuk mengidentifikasi bukti digital, data yang relevan, atau informasi penting lainnya. Prosedur pemindaian dan analisis ini merupakan tahap dasar dalam pendekatan digital forensik yang bertujuan memahami bukti secara komprehensif. Bukti yang diperoleh menggunakan *tool* Autopsy ditampilkan pada Gambar 9.



Gambar 9. Hasil digital dalam Atopsy



Bukti yang didapat menggunakan *tool* Autopsy adalah artefak video, ditampilkan pada Gambar 9. Prosedur ini menunjukkan pentingnya representasi visual, yang merupakan elemen yang sangat krusial pada analisis forensik. Analisis artefak media menggunakan Autopsy memberikan wawasan terhadap artefak digital yang digunakan untuk pemeriksaan. Identifikasi barang bukti digital dapat menghasilkan informasi penting tentang konteks dan karakteristik data yang akan dianalisis, sehingga meningkatkan teknik penelitian digital yang komprehensif.

### 3.3. Reporting

Perbandingan hasil pemeriksaan bukti digital forensik dapat dilakukan dengan bukti-bukti dari bukti digital yang dikumpulkan dalam kasus-kasus yang melibatkan *cyberbullying*. Karena MOBILEdit Forensics Express Pro dapat menangkap berbagai format, termasuk pesan text, photo, video, ID, data hapus, serta group, ini adalah *tool* forensik yang bagus untuk melakukan verifikasi. Sedangkan untuk penggunaan aplikasi Autopsy hanya memperbolehkan penggunaan rekaman video sebagai *file* digital. Dalam kasus *cyberbullying*, video apa pun yang diunggah sebagai bukti digital menjadi informasi krusial. Hasil perbandingan bukti digital berdasarkan *tools* forensik disajikan dalam Tabel 3.

Tabel 3. Perbandingan *tools* forensik

Framework	Parameter Bukti	Alat Forensik	
		MOBILEdit Forensic Express Pro	Autopsy
ACPO	Pesan teks	✓	×
	Video	✓	✓
	ID Pengguna	✓	×
	Data Hapus	✓	×
	Photo	✓	×
	Group	✓	×
NIJ	Pesan teks	✓	×
	Video	✓	✓
	ID Pengguna	✓	×
	Data Hapus	✓	×
	Photo	✓	×
	Group	✓	×
Persentase		100%	33.3%

Tabel 3. menunjukkan presentase menggunakan indeks angka berdasarkan hasil penelitian untuk menilai setiap *tools* forensik. Rumus (1) menunjukkan penjelasan bagaimana indeks angka dihitung sebagai penjumlahan dari evaluasi terkait. Pendekatan ini memberikan fasilitas pemahaman komprehensif tentang peran dan tanggung jawab dari masing-masing *tools* forensik dalam proses investigasi forensik saat ini dengan memberikan gambaran yang nyata dan dapat diverifikasi mengenai keefisienan alat tersebut.

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

Note:

- ∑pn: Total jumlah nilai yang relevan, yang dianggap penting dalam konteks analisis.
- ∑po: Total data yang tersedia.

---

Pon: Presentase indeks nilai yang ingin dihitung [30].

MOBILEdit Forensics Exspress Pro:  $Pon = \frac{6}{6} \times 100\% = 100\%$

Autopsy:  $Pon = \frac{1}{6} \times 100\% = 33.3\%$

Perbedaan antara *framework* ACPO dan NIJ hanya terlihat pada tahap terakhir. Empat langkah proses ACPO adalah *Plan, Capture, Analysis, dan Present*. Lima proses yang terdiri dari NIJ adalah *Identification, Collection, Examination, Analysis, dan Reporting*. *framework* NIJ lebih lugas, mudah dipahami, dan mudah diterapkan. Karena MOBILEdit Forensics Express Pro menggunakan rumus (1) untuk menghasilkan indeks pada setiap *tools* forensik, maka MOBILEdit Forensics Express Pro memiliki keunggulan lebih besar dibandingkan *tools* forensik lainnya dalam hal kemampuannya mengidentifikasi barang bukti digital berdasarkan standar yang ditentukan. Nilai indeks menggunakan *tool* MOBILEdit Forensic Express Pro adalah 100%, sedangkan menggunakan *tool* Autopsy adalah 33.3%.

#### 4. KESIMPULAN

Berdasarkan dari tujuan penelitian, *framework* ACPO dan NIJ digunakan untuk menganalisis peristiwa atau kasus cyberbullying pada aplikasi IMO Messenger berbasis Android. Hasil penelitian menunjukkan bahwa *framework* NIJ memiliki tahapan paling lengkap dan dianggap unggul karena mendukung proses penyidikan secara lebih menyeluruh. Selain itu, pengesahan terhadap *tools* forensik menunjukkan bahwa video merupakan jenis bukti yang paling sering ditemukan selama penyelidikan. MOBILEdit Forensic Express Pro terbukti menjadi *tool* forensik mobile paling efektif dengan tingkat keberhasilan 100% dalam ekstraksi data, sementara Autopsy hanya mencapai tingkat keberhasilan sebesar 33,3%. Hasil perbandingan ini menegaskan keunggulan kinerja MOBILEdit Forensic Express Pro dalam mendukung proses penyelidikan berbasis *framework* forensik. Dengan demikian, penelitian ini berhasil mencapai tujuannya, yakni mengungkap dan menganalisis data menggunakan kedua *framework* forensik. Penelitian selanjutnya disarankan untuk memperluas implementasi *framework* NIJ pada aplikasi lain, menguji lebih banyak *tools* forensik dengan jenis bukti digital yang beragam, mengembangkan metode analisis data yang lebih efisien, serta mengevaluasi keterbatasan *tools* forensik untuk peningkatan performa di masa mendatang.

#### 5. SARAN

Penelitian selanjutnya dapat mengeksplorasi penerapan *framework* forensik NIJ pada platform komunikasi atau aplikasi media sosial lainnya. Hal ini akan membantu menilai adaptabilitas dan efektivitasnya dalam berbagai konteks. Analisis komparatif dengan berbagai *tools* forensik yang lebih luas dapat memberikan pemahaman yang lebih menyeluruh tentang kapabilitas dan keterbatasan masing-masing *tools*. Hal ini termasuk menguji *tools* yang dirancang khusus untuk data multimedia, seperti video atau komunikasi terenkripsi. Penelitian selanjutnya dapat difokuskan pada analisis berbagai jenis bukti digital, seperti pesan terenkripsi, file yang terhapus, data lokasi geografis, atau metadata, untuk meningkatkan cakupan investigasi forensik. Untuk meningkatkan kecepatan dan akurasi investigasi forensik, penelitian dapat difokuskan pada pengoptimalan metode analisis data, termasuk penggunaan otomatisasi dan kecerdasan buatan dalam mengidentifikasi dan mengkategorikan bukti.

---

## DAFTAR PUSTAKA

- [1] 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, doi: 10.1109/ICCA49400.2020.9022838.
- [2] F. Negaresh, M. Kaedi, and Z. Zojaji, "Gender Identification of Mobile Phone Users based on Internet Usage Pattern," *International Journal of Engineering Transactions C: Aspects*, vol. 36, no. 2, pp. 335–347, 2023, doi: 10.5829/ije.2023.36.02b.13.
- [3] M. ALThebaity, S. Mishra, and M. Kumar Shukla, "Forensic Analysis of Third-party Mobile Application," *Helix*, vol. 10, no. 4, pp. 32–38, 2020, doi: 10.29042/2020-10-4-32-38.
- [4] A. Amorim, F. Pereira, C. Alves, and O. Garcia, "Species assignment in forensics and the challenge of hybrids," *Forensic Sci Int Genet*, vol. 48, 2020, doi: 10.1016/j.fsigen.2020.102333.
- [5] J. Qiu, J. Zhang, W. Luo, L. Pan, S. Nepal, and Y. Xiang, "A Survey of Android Malware Detection with Deep Neural Models," *ACM Comput Surv*, vol. 53, no. 6, 2021, doi: 10.1145/3417978.
- [6] D. P. Harahap, "Implementasi Digital Forensik Aplikasi Dompok Digital Dan Pesan Instan Pada Android Dengan Menggunakan Metode NIST," *KOMIK (Konferensi Nasional Teknologi Informasi dan Komputer)*, vol. 6, no. 1, pp. 533–541, 2023, doi: 10.30865/komik.v6i1.5715.
- [7] A. Yavari, H. Hassanpour, B. R. Cami, and M. Mahdavi, "Election Prediction Based on Sentiment Analysis using Twitter Data," *International Journal of Engineering, Transactions B: Applications*, vol. 35, no. 2, pp. 372–379, 2022, doi: 10.5829/ije.2022.35.02b.13.
- [8] M. Farhoodi, A. T. Eshlaghy, and M. R. Motadel, "A Proposed Model for Persian Stance Detection on Social Media," *International Journal of Engineering Transactions C: Aspects*, vol. 36, no. 6, pp. 1048–1059, 2023, doi: 10.5829/ije.2023.36.06c.03.
- [9] G. M. Abaido, "Cyberbullying on social media platforms among university students in the United Arab Emirates," *Int J Adolesc Youth*, vol. 25, no. 1, pp. 407–420, 2020, doi: 10.1080/02673843.2019.1669059.
- [10] A. Ademiluyi, C. Li, and A. Park, "Implications and Preventions of Cyberbullying and Social Exclusion in Social Media: Systematic Review," *JMIR Form Res*, vol. 6, no. 1, pp. 1–12, 2022, doi: 10.2196/30286.
- [11] H. F. Hansen, "Analysis of NIST Methods on Facebook Messenger For Forensic Evidence," *JIRK*, vol. 1, pp. 695–702, 2022, doi: 10.2307/3412739.
- [12] M. Yao, C. Chelms, 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, doi: 10.1145/3308558.3313462.
- [13] H. Nurhairani and I. Riadi, "Analysis Mobile Forensics on Twitter Application using the National Institute of Justice (NIJ) Method," *Int J Comput Appl*, vol. 177, no. 27, pp. 35–42, 2019, doi: 10.5120/ijca2019919749.
- [14] E. H. K. Dewi, A. Suharso, and C. Rozikin, "Implementasi Cosine Similarity Dalam Analisis Investigasi Cyberbullying Pada Twitter Dengan Framework Nist," *Cyber Security dan Forensik Digital*, vol. 5, no. 1, pp. 12–22, 2022, doi: 10.14421/csecurity.2022.5.1.3397.
- [15] M. K. Bhatia, P. Gambhir, S. Sinha, and S. K. Singh, "A Comparative Analysis of OS Forensics Tools," *Int J Res Appl Sci Eng Technol*, vol. 10, no. 11, pp. 494–502, 2022, doi: 10.22214/ijraset.2022.47346.
- [16] T. Hermawan and L. Roselina, "Android Forensic Tools Analysis for Unsend Chat on Social Media," pp. 233–238, 2021.
- [17] 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, pp. 1263–1271, Apr. 2022, doi: 10.30865/mib.v6i2.3946.
- [18] A. Yudhana, I. Riadi, and I. Anshori, "Analisis Bukti Digital Facebook Messenger Menggunakan Metode Nist," vol. 3, no. 1, pp. 13–21, 2018.
- [19] F. Firmansyah, A. Fadlil, and R. Umar, "Evaluasi Optimalisasi Alat Forensik Keamanan Jaringan pada Lalu Lintas Virtual Router," 2023. doi: <https://journal.unnes.ac.id/sju/edukom/article/view/66963>.
- [20] J. Choi, J. Yu, S. Hyun, and H. Kim, "Digital forensic analysis of encrypted database files in instant messaging applications on Windows operating systems: Case study with KakaoTalk, NateOn and QQ messenger," *Digit Investig*, vol. 28, pp. S50–S59, 2019, doi: 10.1016/j.diin.2019.01.011.

- 
- [21] M. El-tayeb, A. Taha, and Z. Taha, "Ingénierie des Systèmes d' Information Streamed Video Reconstruction for Firefox Browser Forensics," *International Information and Engineering Technology Association*, vol. 26, no. 4, pp. 337–344, 2021.
- [22] J. Hou, Y. Li, J. Yu, and W. Shi, "A Survey on Digital Forensics in Internet of Things," *IEEE Internet Things J*, vol. 7, no. 1, pp. 1–15, 2020, doi: 10.1109/JIOT.2019.2940713.
- [23] F. Firmansyah, A. Fadlil, and R. Umar, "Identifikasi Bukti Forensik Jaringan Virtual Router Menggunakan Metode NIST," *Jurnal RESTI (Rekayasa Sistem dan Teknologi Informasi)*, vol. 5, no. 1, pp. 91–98, Feb. 2021, doi: 10.29207/resti.v5i1.2784.
- [24] 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.
- [25] R. I. Ferguson, K. Renaud, S. Wilford, and A. Irons, "PRECEPT: a framework for ethical digital forensics investigations," *Journal of Intellectual Capital*, vol. 21, no. 2, pp. 257–290, 2020, doi: 10.1108/JIC-05-2019-0097.
- [26] J. J. Turanovic and S. E. Siennick, "The causes and consequences of school violence: A review," *School Violence: Causes, Prevention and Safety Measures*, no. February, pp. 1–80, 2022.
- [27] T. Feucht, "The National Institute of Justice (NIJ)," *The Encyclopedia of Research Methods in Criminology and Criminal Justice: Volume II: Parts 5-8*, vol. II, pp. 800–803, 2021, doi: 10.1002/9781119111931.ch152.
- [28] I. Riadi, A. Yudhana, and G. P. I. Fanani, "Comparative Analysis of Forensic Software on Android-based MiChat using ACPO and DFRWS Framework," *Jurnal RESTI (Rekayasa Sistem dan Teknologi Informasi)*, vol. 7, no. 2, pp. 286–292, 2023, doi: 10.29207/resti.v7i2.4547.
- [29] H. Hajar, H. Hermansa, and I. Ilcham, "Investigasi Stego File Menggunakan Framework National Institute of Justice," *CONTEN: Computer and Network Technology*, vol. 4, no. 1, pp. 31–42, 2024, doi: 10.31294/conten.v4i1.3527.
- [30] M. A. Aziz, W. Y. Sulistyono, and S. R. Astari, "Komparatif Anti Forensik Aplikasi Instant Messaging Berbasis Web Menggunakan Metode Association of Chief Police Officers ( ACPO )," *Jurnal Riset Teknologi Informasi dan Komputer (JURISTIK)*, vol. 1, no. 1, pp. 8–15, 2021, doi: 10.53863/juristik.v1i01.341.
-