INVESTIGASI FORENSIK DIGITAL KASUS PELECEHAN SEKSUAL PADA LAYANAN MEDIA SOSIAL X DENGAN METODE ACPO

Nuratikah [1], Sunardi [2], Imam Riadi [3]
[1] Magister Informatika, Universitas Ahmad Dahlan, Yogyakarta
[2] Program Studi Teknik Elektro, Universitas Ahmad Dahlan, Yogyakarta
[3] Program Studi Sistem Informasi, Universitas Ahmad Dahlan, Yogyakarta
2407048010@webmail.uad.ac.id

ABSTRAK

Kasus pelecehan seksual Kasus pelecehan seksual berbasis daring pada layanan media sosial X menimbulkan tantangan dalam praktik forensik digital, terutama ketika pelaku menghapus pesan sehingga artefak komunikasi tidak lagi terlihat pada aplikasi. Permasalahan ini menyulitkan proses pembuktian dan menuntut investigasi yang sistematis serta dapat dipertanggungjawabkan secara hukum. Penelitian ini bertujuan menganalisis proses pemulihan barang bukti digital pada kasus pelecehan seksual daring menggunakan metode Association of Chief Police Officers (ACPO). Metode ACPO diterapkan melalui tahapan Plan, Capture, Analyze, dan Present dengan memanfaatkan dua tools forensik, yaitu MOBILedit Forensic Express dan Magnet AXIOM. Objek analisis berupa artefak Direct Message yang meliputi 17 pesan teks, 2 gambar, 2 video, 1 pesan suara, dan 2 informasi akun. Hasil penelitian menunjukkan bahwa MOBILedit Forensic Express berhasil memulihkan seluruh artefak gambar, video, dan informasi akun, namun hanya sebagian pesan teks dan tidak memulihkan pesan suara. Sementara itu, Magnet AXIOM berhasil memulihkan gambar, video, dan pesan suara secara lengkap, tetapi memiliki keterbatasan dalam pemulihan pesan teks dan informasi akun. Secara kumulatif, kombinasi kedua tools menghasilkan pemulihan penuh pada artefak multimedia dan akun, sedangkan pesan teks hanya mencapai 58,52%. Temuan ini menegaskan bahwa penggunaan lebih dari satu tools forensik dalam kerangka metode ACPO dapat meningkatkan efektivitas pengumpulan barang bukti digital pada investigasi pelecehan seksual di media sosial.

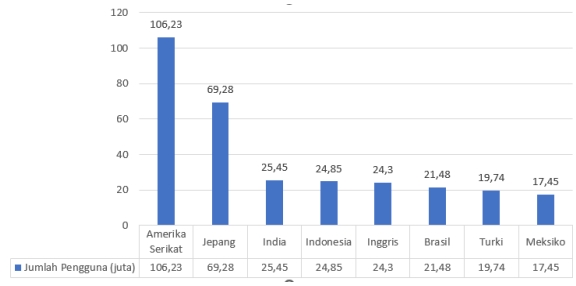
Kata kunci: *forensik Digital; ACPO; Magnet AXIOM; MOBILedit; Media Sosial X; Pelecehan Seksual*

1. PENDAHULUAN

Perkembangan teknologi informasi telah membawa perubahan signifikan dalam pola komunikasi manusia, khususnya melalui pemanfaatan media sosial sebagai sarana pertukaran informasi dan interaksi sosial. Di sisi lain, intensitas penggunaan media sosial juga meningkatkan potensi penyalahgunaan teknologi dalam bentuk kejahatan siber, termasuk tindak kekerasan seksual berbasis daring (*online sexual harassment*) [1]. Salah satu *platform* yang mengalami pertumbuhan pengguna yang pesat adalah Twitter, yang saat ini dikenal sebagai X. Platform ini menyediakan fitur *Direct Message* yang memungkinkan pertukaran pesan dalam berbagai format, seperti teks, gambar, video, dan pesan suara[2].

Dalam konteks kekerasan seksual berbasis daring, pelaku kerap mengirimkan konten bermuatan seksual yang tidak diinginkan oleh korban, baik dalam bentuk pesan teks, media visual, maupun rekaman suara [3]. Tantangan utama dalam penanganan kasus ini adalah kebiasaan pelaku menghapus pesan setelah dikirim, sehingga artefak komunikasi tidak lagi terlihat pada antarmuka aplikasi. Kondisi tersebut menyulitkan proses pembuktian digital dan menuntut penerapan teknik forensik yang mampu memulihkan artefak tersembunyi secara sah dan dapat dipertanggungjawabkan [4].

Tingginya penggunaan layanan media sosial X semakin memperbesar risiko terjadinya penyalahgunaan fitur komunikasi. Indonesia tercatat sebagai negara dengan jumlah pengguna X terbesar keempat di dunia [5], yang menunjukkan skala potensi insiden kejahatan siber yang signifikan.



Gambar 1. Jumlah Pengguna Layanan Media Sosial X

Distribusi pengguna global layanan media sosial X ditampilkan pada Gambar 1 berdasarkan data dari dataindonesia.id yang merujuk pada laporan We Are Social dan Meltwater[6]. Skala penggunaan yang besar ini menegaskan urgensi pengembangan pendekatan forensik digital yang efektif untuk mendukung proses penegakan hukum.

Forensik digital berperan penting dalam mengidentifikasi, mengamankan, menganalisis, dan menyajikan barang bukti digital pada kasus yang melibatkan perangkat dan layanan berbasis teknologi informasi [7]. Metode *Association of Chief Police Officers* (ACPO) merupakan salah satu kerangka kerja yang banyak diterapkan karena menekankan prinsip integritas data, keterulangan proses, dan akuntabilitas investigasi [8]. Sejumlah penelitian terdahulu telah

menerapkan metode ACPO pada berbagai *platform* komunikasi digital, seperti WhatsApp [9], MiChat [10], Discord [11][12], dan Skype[13], yang menunjukkan fleksibilitas metode ini dalam menangani beragam artefak digital.

Namun demikian, efektivitas investigasi forensik digital tidak hanya ditentukan oleh metode yang digunakan, tetapi juga oleh *tools* forensik yang diterapkan. Magnet AXIOM dikenal memiliki keunggulan dalam analisis artefak berbasis *cloud* dan media sosial, sedangkan MOBILedit Forensic Express lebih optimal dalam proses ekstraksi data dari perangkat Android [14][15]. Beberapa penelitian menunjukkan bahwa penggunaan lebih dari satu *tools* forensik dapat meningkatkan keberhasilan pemulihan artefak digital, terutama pada *platform* yang menerapkan mekanisme keamanan seperti enkripsi dan penghapusan otomatis [16][17].

Kajian forensik digital dengan metode ACPO pada layanan media sosial X, khususnya kasus kekerasan seksual daring dengan skenario penghapusan Direct Message, masih terbatas dan belum mengkaji secara komprehensif perbandingan hasil ekstraksi Magnet AXIOM dan MOBILedit Forensic Express, sehingga terdapat celah penelitian. Penelitian ini berada dalam bidang Sistem Komputer dan Informatika, khususnya forensik digital dan keamanan sistem informasi. Kontribusi penelitian terletak pada penguatan investigasi forensik kasus kekerasan seksual daring melalui penerapan metode ACPO dengan kombinasi dua tools forensik sebagai acuan teknis bagi praktisi dan penegak hukum. Tujuan penelitian ini adalah menganalisis pemulihan artefak Direct Message yang telah dihapus pada media sosial X, meliputi pesan teks, gambar, video, pesan suara, dan informasi akun, menggunakan Magnet AXIOM dan MOBILedit Forensic Express.

2. TINJAUAN PUSTAKA

Penelitian forensik digital dalam tiga tahun terakhir menunjukkan kecenderungan penggunaan metode terstandar dan pendekatan multi-tools dalam investigasi media sosial. Najla (2025) menerapkan metode ACPO pada platform TikTok dan menunjukkan bahwa kombinasi tools forensik meningkatkan validitas barang bukti digital [18]. Safitri (2024) membuktikan adanya perbedaan signifikan kemampuan ekstraksi antar tools forensik mobile terhadap artefak aplikasi [19]. Riadi et al. (2025) menegaskan bahwa integrasi ACPO dengan tools forensik mobile mampu memperkuat proses pembuktian. Sejalan dengan itu, Alawi et al. (2025) menunjukkan bahwa pendekatan multi-tools berbasis standar forensik meningkatkan kredibilitas investigasi barang bukti digital [20].

2.1. Forensik Digital

Forensik digital merupakan disiplin ilmu yang mempelajari proses identifikasi, pengumpulan, analisis, dan penyajian barang bukti digital secara sistematis serta dapat dipertanggungjawabkan secara hukum [21][22]. Barang bukti digital memiliki sifat volatil dan mudah dimodifikasi, sehingga proses investigasi harus mengikuti prosedur baku untuk menjaga integritas dan keaslian data[23]. Forensik digital berperan penting dalam pemulihan data yang telah dihapus atau disembunyikan oleh pelaku kejahatan siber, termasuk pada platform media sosial menegaskan bahwa artefak digital dapat tetap dipulihkan meskipun telah dihapus dari antarmuka aplikasi, selama masih tersimpan pada sistem atau media penyimpanan

2.2. Kekerasan Seksual Berbasis Daring

Kekerasan seksual berbasis daring *(online sexual harassment)* merupakan bentuk kekerasan seksual yang difasilitasi oleh teknologi digital, seperti pengiriman pesan bermuatan seksual tanpa persetujuan melalui media sosial[10]. Praktik ini sering terjadi pada fitur komunikasi privat dan sulit terdeteksi karena pelaku dapat menghapus pesan setelah dikirim menekankan bahwa bukti digital pada kasus kekerasan seksual daring memiliki peran krusial dalam pembuktian hukum, sehingga memerlukan pendekatan forensik yang kuat dan dapat dipertanggungjawabkan

2.3. Media Sosial X sebagai Objek Forensik Digital

Layanan media sosial X menyediakan fitur *Direct Message* yang memungkinkan pertukaran pesan teks, gambar, video, dan pesan suara. Dalam konteks forensik digital, *platform* media sosial menyimpan artefak komunikasi baik pada perangkat pengguna maupun dalam struktur data aplikasi, sehingga memungkinkan pemulihan artefak meskipun pesan telah dihapus [24].juga menyatakan bahwa aplikasi pesan instan dan media sosial meninggalkan jejak digital dalam bentuk *database, cache,* dan metadata yang dapat dianalisis secara forensik.

2.4. Barang Bukti Digital

Barang bukti digital pada fitur Direct Message meliputi pesan teks, gambar, video, pesan suara, serta informasi akun. Setiap artefak memiliki karakteristik penyimpanan yang berbeda, sehingga memengaruhi tingkat keberhasilan pemulihan data [12]. menjelaskan bahwa artefak multimedia cenderung lebih mudah dipulihkan dibandingkan pesan teks yang tersimpan dalam database aplikasi

2.5. ACPO

Metode *Association of Chief Police Officers* (ACPO) merupakan kerangka kerja forensik digital yang menekankan prinsip integritas data, akuntabilitas, dan keterulangan proses investigasi. ACPO membagi proses investigasi ke dalam empat tahapan utama, yaitu *Plan, Capture, Analyze, dan Present,* guna memastikan bahwa barang bukti digital tetap sah dan dapat diterima di pengadilan[25]. Hanna

(2025) menyatakan bahwa penerapan standar seperti ACPO meningkatkan kredibilitas hasil investigasi forensik digital

3. METODE PENELITIAN

3.1. Investigasi dengan Metode ACPO

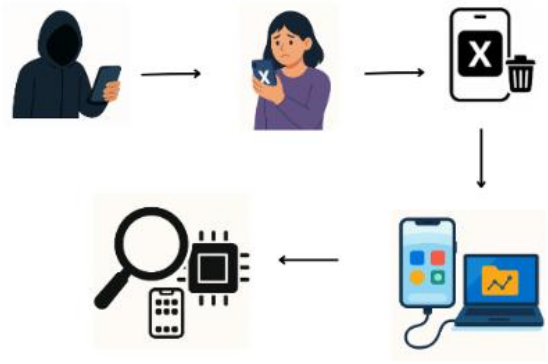
Gambar 2. Tahapan Metode ACPO

Metode ACPO terdiri dari empat tahapan utama pada seperti pada Gambar 2 dengan uraian seperti berikut.

a. *Plan.* Tahapan awal berisi perencanaan investigasi yang mencakup identifikasi tujuan, penentuan perangkat digital yang dijadikan objek forensik, serta pemilihan *tools* yang tepat untuk proses akuisisi dan analisis bukti digital. Penelitian ini menetapkan dua *smartphone* Android sebagai objek pemeriksaan, yaitu perangkat pelaku dan korban, serta memilih MOBILedit Forensic Express dan Magnet AXIOM sebagai *tools* utama untuk proses ekstraksi data [28]
b. *Capture.* Tahapan ini berfokus pada proses pengumpulan bukti digital dari perangkat. Proses dimulai dengan pengamanan perangkat, aktivasi USB Debugging, koneksi perangkat ke komputcr, dan pelaksanaan akuisisi menggunakan MOBILedit Forensic Express dan Magnet AXIOM. Seluruh aktivitas dicatat untuk memastikan tidak terjadi perubahan pada data asli dan integritas bukti digital tetap terjaga [29].
c. *Analyze.* Analisis dilakukan terhadap artefak digital yang berhasil diekstraksi, mencakup 17 pesan teks, 2 gambar, 2 video, 1 pesan suara, dan 2 informasi akun dari fitur *Direct Message* layanan media sosial X. Setiap artefak diperiksa berdasarkan isi pesan, metadata, lokasi penyimpanan, serta konsistensi relasi antar data untuk mendukung pembuktian forensik [30].
d. *Present.* Tahap akhir berisi penyusunan laporan forensik digital secara sistematis, objektif, dan kronologis. Laporan memuat hasil akuisisi, analisis, temuan utama, serta interpretasi bukti digital untuk mendukung proses pembuktian dalam konteks hukum [19]

3.2. Skenario Kasus

Skenario kejadian mensimulasikan kasus *sexual harassment* berbasis daring melalui layanan media sosial X. Simulasi ini terdiri dari lima tahapan utama yang tampilkan pada Gambar 3.



Gambar 3. Tahapan Skenario Kasus

Penjelasan skenario kasus *sexual harassment* daring melalui layanan media sosial X sesuai yang ditampilkan pada Gambar 4 diuraikan seperti berikut.

a. Pengiriman Pesan oleh Pelaku. Pelaku pengiriman pesan bermuatan seksual kepada korban melalui fitur *Direct Message* yaitu 17 pesan teks, 2 gambar, 2 video, 1 pesan suara, dan 2 informasi akun sebagai bentuk tindakan pelecehan seksual berbasis daring melalui layanan media sosial X.
b. Pesan Diterima oleh Korban. Korban menerima pesan dalam berbagai format tersebut melalui fitur *Direct Message* sebagai gambaran nyata pola pelecehan seksual digital yang terjadi secara langsung dan bersifat pribadi melalui aplikasi layanan media sosial X.
c. Penghapusan Pesan oleh Pelaku. Setelah terkirim, pesan di fitur *Direct Message* dihapus oleh pelaku sebagai bentuk upaya menghilangkan jejak digital.
d. Akuisisi Data. Peneliti melakukan akuisisi data dari perangkat pelaku menggunakan Magnet AXIOM dan MOBILedit Forensic Express untuk menyalin isi perangkat tanpa mengubahnya.
e. Analisis. Barang bukti digital yang diperoleh dianalisis berdasarkan metode ACPO. *Tools* forensik digunakan sebagai alat bantu, sementara peneliti bertanggung jawab penuh atas interpretasi data.

4. HASIL DAN PEMBAHASAN

4.1. *Plan*

Tahap perencanaan dilakukan sesuai prinsip metode ACPO yang menekankan perlindungan integritas data digital. Peneliti menetapkan dua smartphone Android milik pelaku dan korban sebagai objek forensik, yang kemudian diamankan dan didokumentasikan melalui pencatatan identitas fisik serta pengambilan foto awal. Pemeriksaan awal mencakup kondisi operasional perangkat, mekanisme pengamanan, dan kesiapan perangkat lunak forensik.

Selanjutnya dilakukan pemetaan awal sumber bukti digital pada layanan media sosial X, meliputi

pesan langsung, konten, metadata komunikasi, dan file media, agar proses akuisisi lebih terarah. Perencanaan juga mencakup pemilihan Magnet AXIOM dan MOBILedit Forensic Express untuk meningkatkan keandalan hasil melalui verifikasi silang. Tahap ini diakhiri dengan penyusunan prosedur dokumentasi dan chain of custody, serta pertimbangan aspek hukum, etika, dan mitigasi risiko guna memastikan seluruh proses investigasi sesuai prinsip metode ACPO dan dapat dipertanggungjawabkan secara ilmiah maupun hukum.

Tabel 1. Data Asal

No.	Data Digital	Metadata	Jumlah
1		Status: Terhapus Sumber: X DM Pengirim: MaleLukman Penerima: failasajibi	17
2		Ukuran: 1.29 MB Dimensi: 1024x1024 px Tipe: PNG	1
3		Ukuran : 36.65 KB Dimensi: 332x244 px Tipe: JPG	1
4		Ukuran: 813 KB Dimensi: 576x1024 px Durasi: 00:19 Tipe: MP4	1
5		Ukuran: 2.26 MB Dimensi: 892x576 px Durasi: 00:19 Tipe: MP4	1
6		Ukuran: 86 KB Durasi: 6 detik Tipe: MP3	1
7		Akun pelaku: MaleLukman (@MaleLukma) Akun korban: failasajibi (@failasajibi) Tipe: Akun X	2

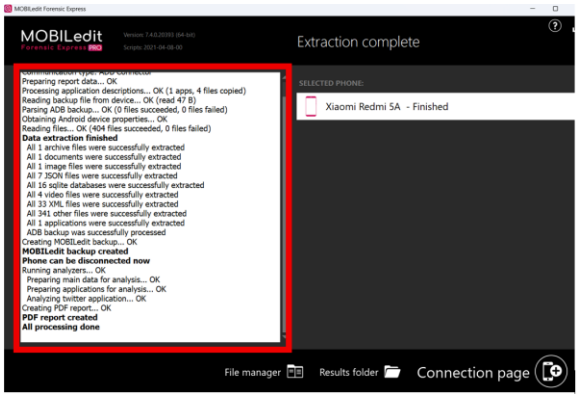
Tabel 1 menampilkan serangkaian variabel yang merepresentasikan data digital yang dianalisis dalam proses investigasi forensik. Variabel-variabel tersebut mencakup akun media sosial berupa pesan teks, file gambar, video, pesan suara, dan informasi akun. Setiap elemen dilengkapi dengan informasi teknis berupa metadata, yang meliputi ukuran file, resolusi atau dimensi visual, durasi, dan format file. Tujuan penyusunan tabel ini adalah untuk memberikan representasi komprehensif terhadap karakteristik teknis data digital yang menjadi subjek analisis dalam pembuktian forensik. Pendataan variabel secara sistematis berperan sebagai dasar analisis yang mendukung proses penelusuran jejak digital, analisis temuan forensik, serta pengujian keabsahan data hasil ekstraksi. Tabel ini berkontribusi dalam memperkuat upaya validasi data melalui penyajian yang sistematis, sehingga mendukung akurasi temuan dan mempertegas pertanggungjawaban ilmiah dalam setiap tahap analisis data digital.

4.2. *Capture*

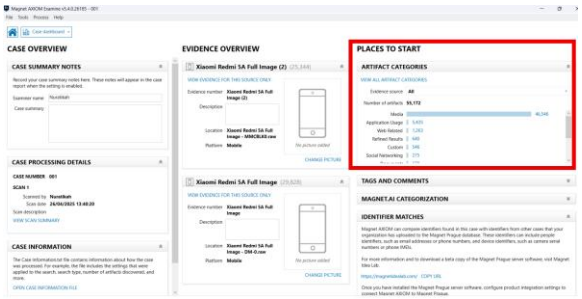
Penelitian ini menerapkan metode forensik statis pada tahap akuisisi data digital. Dua smartphone diamankan sebagai barang bukti, yaitu Samsung Galaxy J2 Prime (Android 6.0.1) milik korban dan Redmi 5A (Android 7.1.2) milik pelaku. Untuk memperoleh akses penuh ke sistem file, kedua perangkat dilakukan rooting menggunakan TWRP dan SuperSU, dengan keberhasilan divalidasi melalui Root Checker.

Selanjutnya, USB Debugging diaktifkan dan perangkat dihubungkan ke komputer melalui mode Transfer File (MTP). Akuisisi data dilakukan menggunakan MOBILedit Forensic Express dan Magnet AXIOM dengan menjaga keutuhan data asli. Integritas bukti dijamin melalui perhitungan hash MD5 dan SHA1, serta dokumentasi identitas perangkat, waktu penyimpanan, dan struktur direktori hasil ekstraksi. Seluruh proses dilaksanakan sesuai

prinsip forensik digital agar tidak terjadi perubahan pada data asli.



Gambar 4. Hasil Ekstraksi MOBILedit

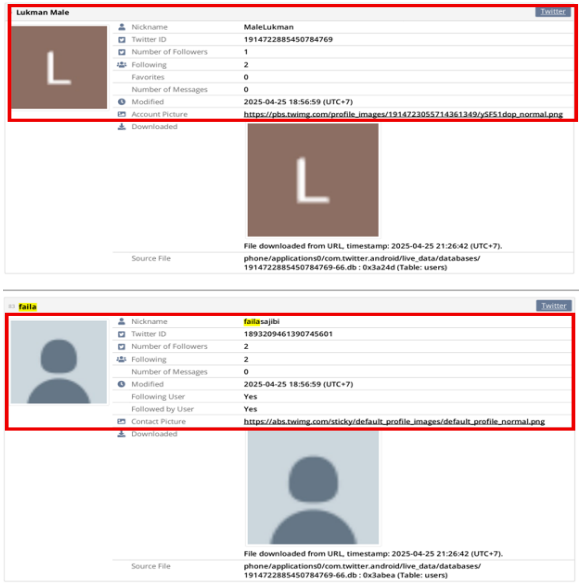


Gambar 5. Hasil Ekstraksi Magnet Axiom

Gambar 4 dan Gambar 5 menampilkan hasil ekstraksi data menggunakan MOBILedit Forensic Express dan Magnet AXIOM terhadap smartphone yang dijadikan objek forensik. Hasil ekstraksi dari MOBILedit menunjukkan berbagai artefak digital umum, seperti informasi aplikasi, file media, dan data sistem, yang digunakan sebagai identifikasi awal bukti digital.

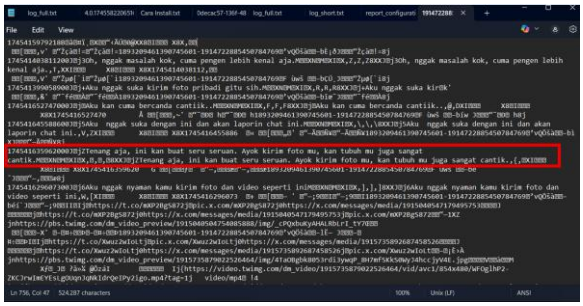
Sementara itu, Magnet AXIOM menyajikan artefak secara lebih terstruktur, khususnya data yang berkaitan dengan aktivitas pada layanan media sosial X, termasuk pesan langsung, metadata komunikasi, dan file media pendukung. Perbandingan hasil ekstraksi dari kedua tools ini dilakukan sebagai bentuk verifikasi silang untuk memastikan konsistensi, kelengkapan, serta keandalan artefak digital yang diperoleh dalam proses investigasi forensik digital.

Analisis dilakukan terhadap data hasil akuisisi dari perangkat korban dan pelaku untuk mengidentifikasi bukti digital terkait kasus *sexual harassment* berbasis daring melalui layanan media sosial X. Proses ini menggunakan MOBILedit Forensic Express dan Magnet AXIOM untuk menelusuri *Direct Mssage*, yaitu 17 pesan teks, 2 gambar, 2 video, 1 pesan suara, dan 2 informasi akun. Setiap bukti diperiksa berdasarkan konteks dan metadata guna mendukung pembuktian secara forensik.



Gambar 6. Bukti Hasil Ekstraksi akun di MOBILedit Forensic Express

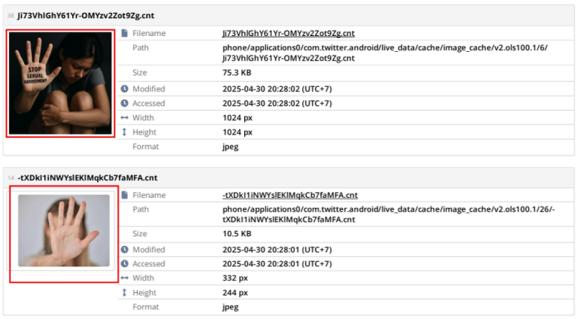
Gambar 6 menunjukkan bahwa hasil ekstraksi akun layanan media sosial X dari perangkat pelaku menggunakan MOBILedit Forensic Express. Data yang ditampilkan mencakup informasi akun seperti nama pengguna (*nickname*), Twitter ID, jumlah pengikut (*followers*), akun yang diikuti (*following*), serta tautan gambar profil. Selain itu, metadata terkait waktu modifikasi akun dan lokasi sumber file basis data juga terdokumentasi. Kedua akun ini diduga terlibat dalam komunikasi yang mengarah pada *sexual harassment* berbasis daring terhadap korban. Informasi ini menjadi bagian penting dalam proses analisis dan pelacakan aktivitas pelaku di layanan media sosial X.



Gambar 7. Bukti Hasil Ekstraksi pesan teks OBILedit Forensic Express

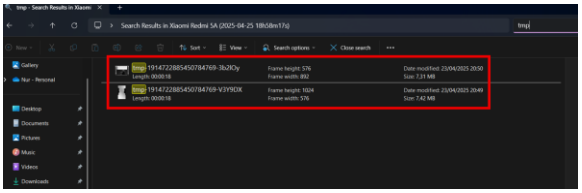
Gambar 7 menunjukkan bahwa dari total 17 pesan yang terdapat pada layanan media sosial X, sebanyak 10 pesan berhasil diekstraksi menggunakan *tools* MOBILedit. Hasil ekstraksi tersebut menunjukkan bahwa meskipun sebagian pesan telah dihapus oleh pengguna, mayoritas isi komunikasi masih dapat dipulihkan. Informasi pesan yang berhasil diperoleh menjadi komponen penting dalam menelusuri pola interaksi digital antara pihak-pihak yang terlibat. Walaupun tidak seluruh pesan dapat

direkonstruksi secara lengkap, data yang tersedia tetap memberikan kontribusi signifikan dalam mendukung proses investigasi forensik digital.



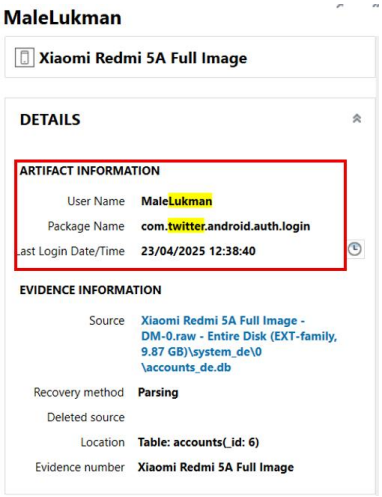
Gambar 8. Bukti Hasil Ekstraksi Gambar MOBILedit Forensic Express

Gambar 8 menunjukkan bukti hasil ekstraksi bukti digital berupa gambar dari perangkat pelaku yang diperoleh menggunakan MOBILedit Forensic Express dalam kasus pelecehan seksual berbasis daring melalui layanan media sosial X. Gambar tersebut ditemukan dalam direktori *cache* layanan media sosial X dan menunjukkan file berhasil ditemukan, yang diduga dikirim oleh pelaku sebagai bagian dari komunikasi bermuatan pelecehan seksual. Setiap file gambar dilengkapi dengan informasi teknis seperti nama file, ukuran, tanggal modifikasi dan akses, serta metadata lainnya yang relevan untuk dianalisis lebih lanjut dalam konteks investigasi forensik digital.



Gambar 9. Hasil Ekstraksi video di MOBILedit Forensic Express

Gambar 9 menampilkan dua file video yang berhasil diekstraksi melalui *tools* MOBILedit Forensic Express. Kedua file memiliki durasi 19 detik dan ditemukan dalam direktori com.twitter.android/live_external/files/, yang mengindikasikan keterkaitan dengan aktivitas pengguna pada layanan media sosial X. Kedua file tersebut berhasil diputar dan divisualisasikan, serta menampilkan isi yang relevan. Meskipun nama file dan waktu modifikasi menunjukkan hubungan yang konsisten, perbedaan ukuran file mengisyaratkan adanya kemungkinan perbedaan konten atau metode kompresi. Oleh karena itu, diperlukan verifikasi lanjutan untuk memastikan relevansi file tersebut dalam konteks investigasi. Identifikasi barang bukti digital ini memberikan dasar yang kuat bahwa file video tersebut dapat dijadikan sebagai bagian dari rangkaian bukti digital yang mendukung proses pembuktian secara forensik.



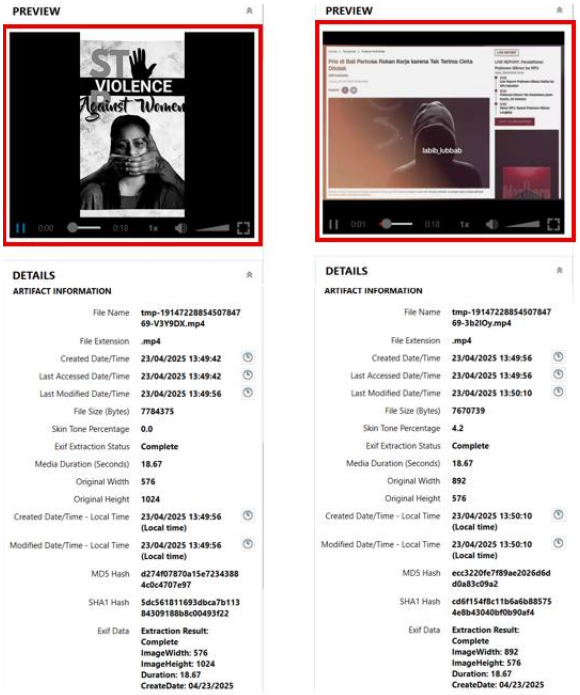
Gambar 10. Hasil ekstraksi akun Magnet AXIOM

Gambar 10 menunjukkan bahwa hasil ekstraksi akun menggunakan Magnet AXIOM, hanya ditemukan satu akun layanan media sosial X aktif pada perangkat Xiaomi Redmi 5A, yaitu akun dengan nama pengguna MaleLukman yang di simulasikan sebagai akun pelaku. Akun ini tercatat terakhir login pada 23 April 2025 pukul 12:38:40. Tidak ditemukan akun lain, termasuk milik korban, dalam hasil analisis. Hal ini dimungkinkan karena akun korban tidak pernah *login* di perangkat tersebut, atau data telah terhapus sebelum proses akuisisi dilakukan.

Gambar 11. Hasil ekstraksi foto Magnet AXIOM

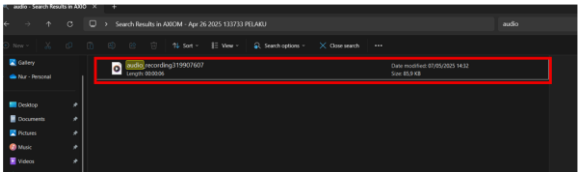
Gambar 11 menunjukkan hasil ekstraksi file gambar dari perangkat Xiaomi Redmi 5A menggunakan *tools* Magnet AXIOM. Barang bukti digital tersebut berasal dari layanan media sosial X dan ditemukan pada direktori penyimpanan internal, meskipun sebelumnya telah dihapus oleh pengguna.

Proses ekstraksi dilakukan melalui metode akuisisi logis, yang memungkinkan pemulihan data tanpa mengubah struktur asli perangkat. Setiap file dilengkapi dengan informasi teknis seperti nama file, ukuran, format, waktu akses terakhir, lokasi penyimpanan, serta nilai *hash* MD5 dan SHA1. Nilai *hash* ini memastikan integritas dan keaslian file sehingga barang bukti digital dapat diverifikasi, ditelusuri asalnya, dan digunakan dalam analisis forensik digital yang mendalam.



Gambar 12. Hasil ekstraksi video Magnet AXIOM

Gambar 12 menunjukkan bahwa hasil ekstraksi menggunakan Magnet AXIOM menemukan dua bukti digital berupa video, salah satunya bernama VID20240423_125429.mp4. Video ini ditemukan dalam direktori layanan media sosial X pada perangkat Xiaomi Redmi 5A. Selain berhasil divisualisasikan melalui fitur *preview*, metadata file juga berhasil diperoleh, mencakup nama file, waktu akses, durasi, ukuran, serta nilai *hash* (MD5 dan SHA1) yang sah. Analisis lebih lanjut menunjukkan bahwa file ini merupakan hasil unduhan yang terhubung dengan aktivitas akun pelaku, dengan catatan jalur penyimpanan yang lengkap. Struktur data file juga terbaca secara utuh dan konsisten saat ditelusuri melalui tampilan heksadesimal Magnet AXIOM sehingga memperkuat keabsahan file sebagai barang bukti digital forensik. Kedua video ini mendukung pembuktian digital dalam kasus yang diteliti dan sah digunakan sebagai bukti dalam proses investigasi forensik.



Gambar 13. Hasil ekstraksi pesan suara Magnet AXIOM

Gambar 13 menunjukkan bahwa ekstraksi menggunakan Magnet AXIOM berhasil menemukan satu file pesan suara dari layanan media sosial X bernama audio_recording179907007.m4a yang tersimpan pada direktori Attachments. File berukuran 849 KB ini memiliki waktu modifikasi terakhir 30 April 2025 pukul 23:58 serta metadata lengkap, sehingga sah sebagai bukti digital forensik. Temuan ini membuktikan adanya komunikasi audio antara pelaku dan korban yang meskipun telah dihapus dari aplikasi, masih tersimpan pada sistem file perangkat dan dapat dipulihkan menggunakan tools forensik yang tepat.

4.3. *Present*

Tahap *Present* merupakan bagian akhir dari metode ACPO, dimana hasil analisis forensik digital yang telah diperoleh disusun secara sistematis dan dilaporkan guna mendukung proses pembuktian dalam konteks hukum. Penelitian ini melakukan perbandingan efektivitas dua *tools* forensik yaitu MOBILedit Forensic Express dan Magnet AXIOM dalam mengekstraksi lima jenis barang bukti digital pada *tools* yaitu 17 pesan teks, 2 gambar, 2 video, 1 pesan suara, dan 2 informasi akun dari layanan media sosial X [22]. Hasil perbandingan disajikan dalam bentuk tabel dan uraian analitis untuk memudahkan interpretasi perbedaan kemampuan masing-masing tools. Penyusunan laporan dilakukan dengan memperhatikan prinsip akurasi, keterulangan, dan transparansi proses investigasi. Tahap ini memastikan bahwa seluruh temuan forensik dapat dipertanggungjawabkan secara ilmiah dan hukum.

Tabel 2. Hasil Ekstraksi MOBILedit Forensic Express dan Magnet AXIOM

Jenis Bukti Digital	Jumlah	MobilEdit Forensic Express	Magnet AXIOM	Total
Teks	17	10	0	10
Gambar	2	2	2	2
Video	2	2	2	2
Pesan Suara	1	0	1	1
Akun	2	2	1	2
Total	24	16	6	17

Pada Tabel 4 dapat kita lihat kedua *tools* memiliki efektivitas yang sama yaitu mampu mengekstraksi empat dari lima jenis barang bukti digital. MOBILedit Forensic Express berhasil mengekstraksi 100% pesan gambar, video, dan akun, sedangkan teks hanya mampu didapatkan 10 dari 17

dan tidak mampu mendapatkan pesan suara. Magnet AXIOM memperoleh pesan gambar, video, dan suara, sedangkan akun didapatkan 50% dan pesan teks tidak dapat dipulihkan. Secara akumulatif, kedua *tools* forensik mampu mendapatkan gambar, video, suara, dan akun sebesar 100%, sedangkan pesan teks hanya mampu dipulihkan sebesar 58,52%.

Perbedaan dalam cakupan jenis barang bukti digital ini menunjukkan bahwa meskipun efektivitas keduanya tampak sama secara kuantitatif, kapabilitas teknis masing-masing *tools* berbeda dalam menjangkau bukti digital tertentu. Namun justru perbedaan ini bernilai positif karena dapat saling melengkapi hasil investigasi digital secara menyeluruh, objektif, dan dapat dipertanggungjawabkan secara forensik.

5. KESIMPULAN DAN SARAN

Penelitian ini mengkaji pemulihan artefak digital pada kasus sexual harassment daring di media sosial X menggunakan metode ACPO dengan tools MOBILedit Forensic Express dan Magnet AXIOM. Hasil menunjukkan artefak gambar, video, pesan suara, dan informasi akun berhasil dipulihkan 100%, sementara pesan teks hanya 58,52% dan tidak berhasil diekstraksi oleh Magnet AXIOM, sehingga menjadi artefak paling rentan hilang. Temuan ini menegaskan perlunya penggunaan lebih dari satu tools forensik karena perbedaan kemampuan parsing. Penelitian ini berkontribusi pada pemetaan kemampuan tools dalam kerangka ACPO, namun masih terbatas pada jumlah perangkat dan platform, sehingga penelitian lanjutan diperlukan dengan cakupan yang lebih luas.

DAFTAR PUSTAKA

[1] N. Aisyah *et al.*, "Analisa Perkembangan Digital Forensik Dalam Penyidikan Cybercrime Di Indonesia Secara Systematic Review," *J. Esensi Infokom J. Esensi Sist. Inf. dan Sist. Komput.*, vol. 6, no. 1, hal. 22–27, Mei 2022, doi: 10.55886/infokom.v6i1.452.

[2] D. P. Medianti, M. A. Haris, dan M. Hamid, "Analisa Dan Pencarian Bukti Forensik Digital Pada Aplikasi Media Social Twitter Menggunakan Metode National Institute Standard Of Technology," *Dintek*, vol. 17, no. 2, hal. 23–33, Sep 2024.

[3] G. Agarwal, R. Bhatt, P. Pathak, A. Kumar, A. Kumar, dan S. Pandey, "Digital Forensics and the Law: A Computer Engineering Perspective," in *2024 15th International Conference on Computing Communication and Networking Technologies (ICCCNT)*, IEEE, Jun 2024, hal. 1–6. doi: 10.1109/ICCCNT61001.2024.10725628.

[4] Herman, Imam Riadi, dan irhash Ainur Rafiq, "Forensik Seluler pada Media Sosial Menggunakan Metode," *Tek. dan Teknol. Terap.*, vol. 1, no. 2, hal. 2023, 2023.

[5] E. Hakimah, K. Dewi, A. Suharso, dan C. Rozikin, "Implementasi Cosine Similarity Dalam Analisis Investigasi Cyberbullying Pada Twitter Dengan Framework Nist," Bekasi, Mei 2022.

[6] DataIndonesia.id, "Jumlah Pengguna Media Sosial Global," 2024.

[7] M. F. Mubarok Nahdli, M. K. Biddinika, dan I. Riadi, "Forensic Analysis of the WhatsApp Application Using the National Institute of Justice Framework," *Int. J. Adv. Data Inf. Syst.*, vol. 5, no. 2, Sep 2024, doi: 10.59395/ijadis.v5i2.1328.

[8] M. Rizki Setyawan dan F. Tella, "Forensic Analysis Of Dana Applications Using The ACPO Framework," *J. Ris. Sist. Inf. Dan Tek. Inform.*, vol. 8, no. 1, hal. 1–8, Feb 2023.

[9] R. Y. Prasongko, A. Yudhana, dan I. Riadi, "Analisis Penggunaan Metode ACPO (Association of Chief Police Officer) pada Forensik WhatsApp," *J. Sains Komput. Inform.*, vol. 6, no. 2, hal. 1112–1120, Sep 2022.

[10] A. Hidayah dan F. Fachri, "Analisis Bukti Digital Tergadap Kasus Prostitusi Online Pada Aplikasi Michat Menggunakan Metode Acpo," *Jati (Jurnal Mhs. Tek. Inform.*, vol. 9, no. 1, Feb 2025.

[11] M. Giovani, "Analisis Forensik Aplikasi Discord Pada Android Berdasarkan Acpo Framework.," *J. Inf. Syst. Manag. Digit. Bus.*, vol. 1, no. 3, hal. 307–313, Apr 2024, doi: 10.59407/jismdb.v1i3.441.

[12] A. Tofik dan G. Zaida Muflih, "Akuisisi Barang Bukti Digital Pada Aplikasi Discord Menggunakan Metode Acpo," *Jati (Jurnal Mhs. Tek. Inform.*, vol. 8, no. 6, Des 2024.

[13] M. R. Setyawan dan M. F. Hasa, "Analisis Forensik Digital Pada Skype Berbasis Windows 10 Menggunakan Framework ACPO," *J. Ilm. Betrik Besemah Teknol. Inf. dan Komput.*, vol. 13, no. 2, hal. 111–119, 2022.

[14] M. Moreb, S. Salah, dan B. Amro, "A Novel Framework for Mobile Forensics Investigation Process," *Int. J. Comput. Digit. Syst.*, vol. 15, no. 1, hal. 125–136, Jul 2024, doi: 10.12785/ijcds/160110.

[15] Y. Safitri, Muhammad Amirul Mu'min, dan Galih Pramuja Inngam Fanani, "Analisis Komparatif Tools Forensik Digital dalam Investigasi Jejak Kejahatan pada Aplikasi Pesan Instan: Sebuah Tinjauan Sistematis," *Sci. J. Comput. Sci. Informatics*, vol. 1, no. 2, hal. 68–75, Jul 2024, doi: 10.34304/scientific.v1i2.335.

[16] K. Gupta, D. Oladimeji, C. Varol, A. Rasheed, dan N. Shahshidhar, "A Comprehensive Survey on Artifact Recovery from Social Media Platforms: Approaches and Future Research Directions," *Inf.*, vol. 14, no. 12, Nov 2023, doi: 10.3390/info14120629.

[17] A. Q. I. Hidayat, E. I. Alwi, dan A. W. M. Gaffar, "Studi Forensik Digital: Analisis Bukti Video TikTok dengan Metode DFRWS," *J. Minfo Polgan*, vol. 13, no. 1, hal. 1138–1146, Agu

2024, doi: 10.33395/jmp.v13i1.13966.
[18] B. S. Najla dan I. Riadi, "Forensic Website Analysis of Movie Piracy on TikTok using the ACPO Framework," *Int. J. Comput. Appl.*, vol. 187, no. 38, hal. 56–63, 2025.
[19] Y. Safitri, I. Riadi, dan S. Sunardi, "Mobile Forensic for Body Shaming Investigation Using Association of Chief Police Officers Framework," *MATRIK J. Manajemen, Tek. Inform. dan Rekayasa Komput.*, vol. 22, no. 3, hal. 651–664, 2023, doi: 10.30812/matrik.v22i3.2987.
[20] H. S. Alawi dan I. Riadi, "Jurnal Informatika : Jurnal pengembangan IT Analisis Forensik Digital terhadap Kasus Penipuan pada E - Commerce Menggunakan Metode ACPO," *J. Inform. J. Pengemb. IT*, vol. 10, no. 3, hal. 789–801, 2025, doi: 10.30591/jpit.v10i3.8604.
[21] T. Ruslan, I. Riadi, dan S. Sunardi, "Analisis Forensik Digital Pada Whatsapp Dan Facebook Menggunakan Metode NIST," *J. Fasilkom*, vol. 13, no. 02, hal. 286–292, 2023, doi: 10.37859/jf.v13i02.5540.
[22] H. Syahida Alawi, I. Riadi, dan S. Sunardi, "Improving Credibility of Digital Evidence Investigation in E-Commerce Fraud Cases using ISO/IEC 27037," *Int. J. Adv. Data Inf. Syst.*, vol. 6, no. 2, hal. 479–495, Agu 2025, doi: 10.59395/ijadis.v6i2.1408.
[23] Reski Badillah, Andi Yulia Muniar, Abd. Rahman, Febri Hidayat Saputra, Mansyur, dan Supriadi Sahibu, "Digital Forensic Evidence Analysis In Revealing Defamation On Social Media (Twitter) Using The Static Forensics Method," *Ceddi J. Inf. Syst. Technol.*, vol. 2, no. 2, hal. 22–33, Des 2023, doi: 10.56134/jst.v2i2.45.
[24] W. Y. Sulistyo, S. A. Pratiwi, dan M. H. Z. Hidayatullah, "Analisis Forensik Citra di Platform X Menggunakan Metode Digital Forensic Research Workshop (Dfrws)," *Idealis Indones. J. Inf. Syst.*, vol. 8, no. 1, hal. 10–20, Jan 2025, doi: 10.36080/idealis.v8i1.3293.
[25] H. S. Alawi, I. Riadi, dan S. Sunardi, "Analisis Forensik Digital terhadap Kasus Penipuan pada E-Commerce Menggunakan Metode ACPO," *J. Inform. J. Pengemb. IT*, vol. 10, no. 3, hal. 789–801, 2025, doi: 10.30591/jpit.v10i3.8604.
[26] I. A. Ghufron Z Muflih, Sunardi., I.Riadi., A.Yudhana., Himawan, "Comparison of Forensic Tools on Social Media Services Using the Digital Forensic Research Workshop Method (DFRWS)," *JIKO (Jurnal Inform. dan Komputer)*, vol. 6, no. 1, hal. 52–61, 2023, doi: 10.33387/jiko.v6i1.5872.
[27] A. Gangwar, "Twitter Forensics On Android with Belkasoft X," 2022, doi: 10.46293/4n6/2022.02.01.07.
[28] A. Alblooshi, N. Aljneibi, F. Iqbal, R. Ikuesan, M. Badra, dan Z. Khalid, "Smartphone Forensics: A Comparative Study of Common Mobile Phone Models," in *2024 12th International Symposium on Digital Forensics and Security (ISDFS)*, IEEE, Apr 2024, hal. 1–6. doi: 10.1109/ISDFS60797.2024.10527262.
[29] Y. Safitri dan M. Amirul Mu, "Mobile Forensic Analysis on IMO Messenger Application Using ACPO and NIJ Frameworks," *Insect*, vol. 11, no. 1, hal. 1–12, 2025.
[30] I. Riadi, Y. Safitri, dan U. Ahmad Dahlan, "Analisis Forensik Cyberbullying pada Aplikasi IMOMessenger Menggunakan Metode Association of ChiefPolice Officers," *J. Bumigora Inf. Technol.*, vol. 5, no. 1, hal. 1–8, Jun 2023, doi: 10.30812/bite/v5i1.2977.