Jurnal Informatika: Jurnal pengembangan IT

Vol. 10, No. 3, 2025
ISSN : 2477-5126, DOI:10.30591/jpit.v10i3.8604

Analisis Forensik Digital terhadap Kasus Penipuan pada E - Commerce Menggunakan Metode ACPO

Hanna Syahida Alawi[1], Imam Riadi[2], Sunardi[3]

[1]*Program Studi Magister Informatika,Universitas Ahmad Dahlan, Jln. Ahmad Yani Tamanan, Yogyakarta, 55191, Indonesia*
[2]*Program Studi Sistem Informasi,Universitas Ahmad Dahlan, Jln. Ahmad Yani Tamanan, Yogyakarta, 55191, Indonesia*
[3]*Program Studi Teknik Elektro,Universitas Ahmad Dahlan, Jln. Ahmad Yani Tamanan, Yogyakarta, 55191, Indonesia.*

Info Artikel

Riwayat Artikel:

Received 2025-03-25
Revised 2025-07-18
Accepted 2025-07-20

Corresponding Author:

Hanna Syahida Alawi

Email:

2407048009@webmail.uad.ac.id

Abstract *– The growth of social media-based e-commerce has increased the risk of cybercrime, particularly fraud cases conducted outside platform systems. TikTok Shop is one of the most widely used platforms, yet the prevalence of transactions outside the official system poses challenges in digital crime investigations. This Research aims to analyze the effectiveness of the ACPO (Association of Chief Police Officers) method in digital forensic investigations to identify and secure electronic evidence related to fraud cases in social media-based e-commerce. The research was conducted using an experimental approach with Belkasoft and MOBILedit Forensic Express forensic tools to extract digital evidence from mobile devices. The initial dataset consisted of 2 accounts, 2 images, 1 video, and 8 chat messages, totaling 13 digital evidence objects. The results showed that Belkasoft successfully extracted images and videos (100%) but failed to retrieve accounts and chat messages, while MOBILedit Forensic Express extracted all evidences (100%) except for the video. By applying ACPO principles, the investigation ensures that all digital evidence is systematically collected while maintaining its integrity for legal proceedings. The findings demonstrate that the ACPO method can be effectively implemented in digital forensic analysis to support cybercrime investigations on social media-based e-commerce platforms. The application of this method contributes to improving the effectiveness of investigations and the validity of digital evidence in the judicial system.*

Keywords: *Digital Forensics, ACPO, TikTok Shop, Electronic Evidence, Online Fraud..*

Abstrak *– Perkembangan e-commerce berbasis media sosial telah meningkatkan risiko kejahatan siber, terutama kasus penipuan yang dilakukan di luar sistem resmi platform. TikTok Shop menjadi salah satu platform yang paling banyak digunakan, tetapi maraknya transaksi di luar sistem menimbulkan tantangan dalam investigasi kejahatan digital. Penelitian ini bertujuan untuk menganalisis efektivitas metode ACPO (Association of Chief Police Officers) dalam proses investigasi forensik digital guna mengidentifikasi dan mengamankan bukti elektronik terkait kasus penipuan pada e-commerce berbasis media sosial. Penelitian dilakukan dengan pendekatan eksperimental menggunakan Belkasoft dan MOBILedit Forensic Express untuk mengekstraksi bukti digital dari perangkat seluler. Dataset awal terdiri dari 2 akun, 2 gambar, 1 video, dan 8 percakapan pesan, sehingga total terdapat 13 bukti digital. Hasil pengujian menunjukkan bahwa Belkasoft berhasil mengekstraksi gambar dan video (100%) tetapi gagal memperoleh akun serta percakapan pesan, sedangkan MOBILedit Forensic Express berhasil mengekstraksi seluruh bukti (100%) kecuali video. Dengan menerapkan prinsip ACPO, investigasi memastikan bahwa seluruh bukti digital dikumpulkan secara sistematis dengan tetap mempertahankan integritasnya agar dapat digunakan dalam proses hukum. Hasil penelitian ini menunjukkan bahwa metode ACPO dapat diimplementasikan secara efektif dalam analisis forensik digital guna mendukung investigasi kejahatan siber di platform e-commerce berbasis media sosial. Penerapan metode ini berkontribusi dalam meningkatkan efektivitas investigasi dan validitas bukti digital dalam sistem peradilan*

Kata kunci*: Forensik Digital, ACPO, TikTok Shop, Bukti Elektronik, Penipuan Online*

I. PENDAHULUAN

Kemajuan teknologi informasi dan komunikasi telah membawa transformasi signifikan dalam berbagai aspek kehidupan manusia, termasuk dalam pola interaksi, perilaku berbelanja, dan mekanisme transaksi daring. TikTok, sebagai salah satu aplikasi media sosial berbasis video yang berkembang pesat, telah memperkenalkan fitur *e- commerce* bernama TikTok Shop [1]. Fitur ini mengintegrasikan elemen hiburan dan perdagangan dalam satu *platform* sehingga menarik perhatian pengguna secara global. Pada kuartal pertama tahun 2024, TikTok mencatat 1,67 miliar pengguna aktif bulanan, dengan Indonesia sebagai salah satu pasar utama memiliki 157,6 juta pengguna aktif [2]. Hal ini menjadikan TikTok Shop sebagai salah satu *platform* dengan potensi besar dalam aktivitas *e-commerce.*

Seiring dengan pertumbuhan, muncul tantangan signifikan terkait dengan keamanan transaksi daring. Popularitas TikTok Shop telah menjadi sasaran bagi pelaku kejahatan siber yang memanfaatkan kelemahan keamanan untuk melakukan berbagai bentuk penipuan, termasuk manipulasi data transaksi, pembayaran di

luar *platform* resmi, dan penjualan produk palsu. Di Asia Tenggara, sekitar 30% pengguna *e-commerce* mengaku pernah menjadi korban penipuan *online*, sedangkan tren kasus penipuan *online* di Idonesia terus meningkat seiring bertambahnya pengguna *platform* media sosial dan *e-commerce* [3]. Penipuan *online shop* pada *platform* media sosial, seperti Instagram dan TikTok, telah menjadi perhatian utama dalam forensik digital. Penelitian sebelumnya telah mengidentifikasi bahwa pelaku dapat menghapus percakapan atau bukti digital lainnya untuk menghindari deteksi sehingga diperlukan metode forensik yang efektif untuk mengidentifikasi dan memulihkan bukti tersebut [4].

Kendala utama yang dihadapi adalah praktik transaksi di luar sistem resmi TikTok Shop, dimana penjual mengarahkan pembeli untuk berkomunikasi melalui fitur pesan dan melakukan pembayaran melalui metode transfer langsung yang sulit untuk dilacak. Praktik ini menurunkan tingkat perlindungan konsumen dan memperumit upaya pengawasan oleh otoritas regulasi. Dalam konteks investigasi forensik digital, kehandalan merupakan aspek krusial yang harus dipenuhi. Banyak otoritas yang bertanggung jawab atas pengembangan dan regulasi forensik digital menegaskan pentingnya memastikan serta membuktikan secara resmi bahwa metode dan alat yang digunakan dalam disiplin ini memiliki tingkat kehandalan yang tinggi [5].

Salah satu pendekatan yang banyak digunakan dalam investigasi forensik digital adalah *Association of Chief Police Officers* (ACPO). Kerangka kerja ini dirancang untuk memastikan bahwa bukti digital dikumpulkan dan dianalisis dengan cara yang dapat diterima di pengadilan [6]. Prinsip-prinsip ACPO telah diterapkan dalam berbagai penelitian forensik digital, termasuk dalam analisis layanan pesan instan [7]. Dalam konteks investigasi *e-commerce*, ACPO memberikan pedoman sistematis untuk memastikan integritas bukti digital. Prinsip ACPO tetap relevan di era modern, tetapi perlu disesuaikan dengan perkembangan teknologi dan metode serangan siber yang semakin canggih [8]. ACPO juga dapat diterapkan dalam analisis forensik pada aplikasi TikTok untuk mengidentifikasi pola kejahatan siber di *platform* media sosial tersebut [9].

Pesan yang terhapus memberikan tantangan besar dalam forensik digital karena keterbatasan waktu dalam pengambilan data, serta kebutuhan keahlian dalam menangani teknologi yang terus berkembang [10]. Forensik digital pada perangkat seluler, khususnya dalam investigasi *e-commerce* TikTokShop, tidak hanya berfokus pada data yang tersimpan di perangkat, tetapi juga harus mencakup analisis fitur lain yang berkaitan dengan ekosistem seluler. Hal ini mencakup jejak digital dari berbagai sensor, data komunikasi dalam jaringan yang digunakan oleh aplikasi, serta informasi yang disimpan oleh platform terkait [11].

Penggunaan alat forensik digital seperti Belkasoft dan MOBILedit Forensic Express telah menjadi topik penelitian penting dalam analisis bukti digital. Penelitian menggunakan MOBILedit Forensic Express sebelumnya menunjukkan hasil 83,33% [12] dan 85,71% [13]. Belkasoft berhasil memperoleh bukti digital dengan tingkat keberhasilan 100% dalam mengekstraksi akun, kontak, gambar, dan video [14].

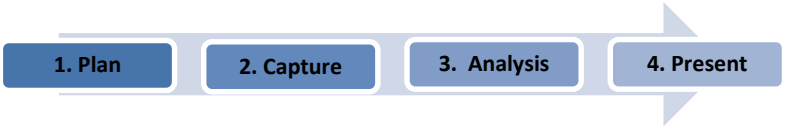
Penelitian ini bertujuan untuk menganalisis efektivitas metode ACPO dalam proses investigasi forensik digital guna mengidentifikasi dan mengamankan bukti elektronik terkait kasus penipuan pada TikTok Shop. Pendekatan eksperimental dilakukan untuk menguji kemampuan alat forensik seperti Belkasoft dan MOBILedit Forensic Express dalam mengekstraksi bukti digital dari perangkat seluler. Dataset awal terdiri dari 2 akun, 2 gambar, 1 video, dan 8 percakapan pesan, sehingga total terdapat 13 objek bukti digital.

Kebaruan penelitian ini terletak pada evaluasi komparatif efektivitas dua alat forensik dalam konteks penipuan pada *e-commerce* berbasis media sosial, serta serta penerapan metode ACPO untuk memastikan integritas dan validitas bukti digital dalam proses hukum. Hasil penelitian ini diharapkan dapat memberikan kontribusi dalam pengembangan strategi investigasi yang lebih efektif dan akurat dalam menghadapi kejahatan siber pada *platform* seperti TikTok Shop.

II. METODE

A. Tahapan Penelitian

Penelitian ini menerapkan metode forensik statis, yaitu proses analisis forensik yang dilakukan setelah insiden penipuan terjadi, dimana percakapan telah berakhir. Pendekatan yang digunakan dalam penelitian ini adalah simulasi dengan skenario penelitian yang dirancang untuk merepresentasikan kasus penipuan di *e-commerce* TikTok Shop. *Framework* yang digunakan dalam penelitian ini adalah ACPO untuk memastikan bahwa proses investigasi bukti digital dilakukan secara sistematis dan sesuai standar hukum. ACPO memiliki prinsip utama yang memastikan bahwa data digital dikumpulkan, dianalisis, dan dilaporkan dengan cara yang dapat diterima dalam proses peradilan [8].



Gambar 1. Tahapan Metode ACPO

Pada tahap investigasi dan analisis, metode forensik statis digunakan dalam ACPO dengan tahapan seperti Gambar 1 dengan penjelasan sebagai berikut:

1. *Plan*, langkah ini diawali dengan menyusun rencana secara rinci mengenai tahapan-tahapan yang akan dilaksanakan dalam proses penelitian. Hal ini mencakup pembuatan skenario penelitian serta persiapan alat dan bahan yang akan digunakan [15].
2. *Capture*. Tahap ini mencakup proses penyimpanan data hasil penelitian yang telah diperoleh kemudian dianalisis lebih lanjut guna mendapatkan temuan yang relevan. Penyimpanan dilakukan dengan memastikan integritas data tetap terjaga agar dapat digunakan dalam proses evaluasi dan interpretasi hasil penelitian [16].
3. *Analysis.* Pada tahap ini, data yang telah dikumpulkan dilakukan proses menggunakan metode yang teruji secara teknis untuk memperoleh informasi yang relevan dan mendukung proses investigasi. Data kemudian dianalisis dan dibandingkan guna menghasilkan temuan penelitian yang valid serta dapat dipertanggungjawabkan secara ilmiah [17].
4. *Present*. Tahap ini mencakup penyajian data penelitian yang telah diolah menjadi informasi yang akurat dan dapat dipertanggungjawabkan. Seluruh tindakan serta hasil penelitian dipaparkan secara menyeluruh disertai rekomendasi yang berkaitan dengan temuan penelitian [18].

Prinsip-prinsip ACPO terkait bukti digital secara eksplisit menekankan pentingnya kompetensi dalam seluruh dokumentasi panduan yang diterbitkan [19]. ACPO menetapkan pedoman bagi penyelidik forensik digital dalam menangani bukti digital guna memastikan integritasnya sehingga dapat diterima di pengadilan. Hal ini disebabkan oleh penerapan hukum yang sama terhadap semua jenis bukti digital sehingga diperlukan prinsip yang seragam untuk menjaga keabsahan dan keandalannya [20].

B . Alat dan Bahan

Penelitian ini menggunakan beberapa alat yang dapat dilihat pada Tabel 1.

TABEL 1
ALAT PENELITIAN

No	Perangkat	Sistem Operasi	Status	Kegunaan
1	Oppo A57	Android Lollipop 5.0.1	*Rooted*	Objek Penelitian
2	Redmi 4X	Android Marsmallow 6.0.1	*Rooted*	Objek Penelitian
3	Laptop	Windows 11 64 Bit	AMD RYZEN 3 8.00 GB RAM	*Workstation* untuk analisis forensik
4	USB Connector			Penghubung *smartphone* dengan *workstation*

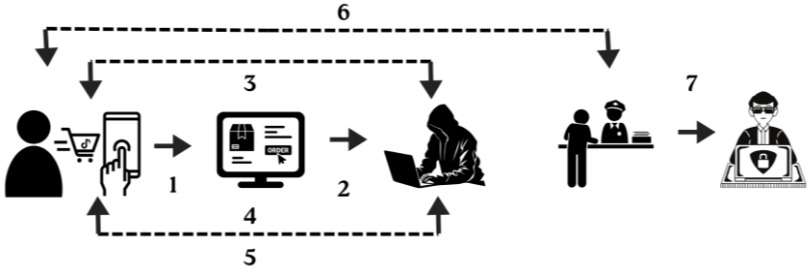
Beberapa *software* yang digunakan untuk mendukung penelitian diperlihatkan pada Tabel 2. *Software* yang digunakan terbagi menjadi *software test*, sistem operasi, alat forensik, dan alat analisis.

TABEL 2
SOFTWARE PENDUKUNG

No	Alat Forensik	Versi	Kegunaan
1	TikTok Shop	2.17.351	*Software test*
2	Windows 11		Sistem operasi *workstation*
3	MOBILedit Forensic Express		Alat forensik & analisis
4	Belkasoft		Alat forensik & analisis
5	Android Debugging Bridge	1.4.3	Komunikasi antara *smartphone* dengan komputer

C . Skenario Penelitian

Skenario kejadian yang mensimulasikan kasus penipuan pada *e-commerce* TikTokShop dalam tujuh tahap utama, berikut penjelasan tiap tahapan pada Gambar 2.



Gambar 2. Skenario Kejadian Penipuan pada *E-Commerce* TikTokShop

1. *Korban membeli barang lewat TikTok Shop*

   Korban tertarik dengan produk yang dijual di TikTok Shop dan melakukan pemesanan melalui *platform* tersebut. Dalam prosesnya, korban berinteraksi dengan penjual melalui fitur chat TikTok Shop untuk mendapatkan informasi lebih lanjut mengenai barang yang akan dibeli, metode pembayaran, dan proses pengiriman.

2. *Pelaku menerima informasi pesanan lalu menjalankan aksi penipuan*

   Setelah menerima informasi pesanan dari korban, pelaku yang menyamar sebagai penjual mulai menjalankan aksinya. Pelaku menghubungi korban melalui chat TikTok Shop dan berusaha membangun kepercayaan dengan memberikan penjelasan terkait produk yang dijual. Namun, dalam percakapan tersebut, pelaku mulai mengarahkan korban ke metode pembayaran di luar TikTok Shop sebagai bagian dari strategi penipuannya.

3. *Pelaku menawarkan harga murah tetapi pembayaran dilakukan di luar TikTok Shop*

   Pelaku meyakinkan korban bahwa jika pembayaran dilakukan secara langsung melalui transfer bank atau metode lain di luar sistem TikTok Shop, korban bisa mendapatkan harga lebih murah atau keuntungan tambahan seperti bonus atau pengiriman lebih cepat. Modus ini digunakan untuk menghindari sistem keamanan dan perlindungan transaksi dari TikTok Shop sehingga korban tidak memiliki perlindungan jika terjadi penipuan.

4. *Korban percaya dan mentransfer sejumlah uang yang diminta serta mengirim bukti pembayaran melalui chat TikTok Shop*

   Tergiur dengan tawaran harga yang lebih murah, korban mengikuti instruksi pelaku dengan mentransfer sejumlah uang sesuai yang diminta. Sebagai bukti transaksi, korban kemudian mengirimkan tangkapan layar atau detail pembayaran melalui chat TikTok Shop tanpa menyadari telah masuk kedalam perangkap penipuan.

5. *Pelaku memblokir korban dan menghapus chat serta bukti transfer yang dikirim korban*

   Setelah menerima uang dari korban, pelaku segera memblokir korban sehingga komunikasi tidak dapat dilanjutkan. Selain itu, pelaku juga menghapus seluruh riwayat chat dan bukti pembayaran yang dikirim oleh korban untuk menghilangkan jejak serta mencegah korban melakukan upaya klaim atau pelacakan.

6. *Korban melapor dan polisi mengumpulkan barang bukti berupa handphone korban dan handphone pelaku*

   Menyadari bahwa dirinya telah menjadi korban penipuan, korban segera melaporkan kejadian ini kepada pihak kepolisian. Sebagai langkah awal penyelidikan, polisi mengumpulkan barang bukti berupa ponsel milik korban, yang berisi riwayat komunikasi dan transaksi dengan pelaku. Jika memungkinkan, perangkat yang digunakan pelaku juga dikumpulkan sebagai barang bukti untuk dianalisis lebih lanjut.

7. *Selanjutnya, barang bukti dianalisis menggunakan tahapan metode ACPO dengan tools MobileEdit dan Belkasoft*

   Untuk mengungkap detil kasus lebih dalam, barang bukti yang telah dikumpulkan dianalisis menggunakan metode forensik digital berdasarkan tahapan ACPO. Proses ini dilakukan dengan *tools* MobileEdit dan Belkasoft, yang memungkinkan penyidik mengekstrak dan menganalisis data dalam perangkat, termasuk pemulihan chat yang telah dihapus, identifikasi transaksi keuangan, serta pencarian informasi terkait identitas pelaku. Hasil dari analisis ini menjadi bukti penting dalam proses penyelidikan dan penegakan hukum terhadap kasus penipuan yang terjadi di *e-commerce* TikTok Shop.

D . Justifikasi Skenario Simulasi

Skenario simulasi yang digunakan dalam penelitian ini dikembangkan berdasarkan pola kejahatan digital yang telah dilaporkan secara publik, dengan memperhatikan aspek relevansi forensik digital terhadap alur komunikasi, jejak transaksi, serta manipulasi sistem pembayaran di luar platform resmi. Setiap skenario menggambarkan potensi bukti digital yang dapat dikumpulkan, diekstraksi, dan dianalisis menggunakan pendekatan forensik.

Pertama, laporan dari Polres Pangandaran mengungkap adanya modus transaksi segitiga di marketplace, di mana pelaku memesan barang dari penjual sah lalu menjualnya kembali kepada korban dengan harga murah. Transaksi dilakukan di luar platform, dan korban mentransfer uang langsung ke pelaku. Sementara itu, penjual tetap mengirim barang ke korban tanpa pernah menerima pembayaran. Dalam konteks digital forensik, skenario ini menghasilkan jejak artefak yang kompleks, seperti log transaksi lintas akun, catatan komunikasi di luar platform, serta perbedaan identitas pengguna antara pelaku dan korban[21].

Kedua, masih berdasarkan laporan dari Polres Pangandaran, modus permintaan transfer ulang dilakukan oleh pelaku dengan menyamar sebagai penjual atau pihak admin dari marketplace, yang kemudian meminta korban mentransfer ulang dana karena alasan kesalahan sistem atau nominal pembayaran. Interaksi biasanya

dilakukan melalui aplikasi pesan instan seperti WhatsApp, yang dalam proses investigasi akan menghasilkan artefak digital berupa log chat, metadata nomor pengirim, serta bukti transfer yang tidak sah. Skenario ini mendukung representasi simulasi yang memvisualisasikan eksploitasi komunikasi di luar sistem dan upaya pemalsuan otoritas[22].

Ketiga, laporan dari Polres Pangandaran juga mencatat kasus penipuan rekening bersama, di mana pelaku meyakinkan korban untuk tidak menggunakan sistem escrow atau rekening bersama yang disediakan oleh platform. Sebagai gantinya, korban diminta mentransfer langsung ke rekening pribadi pelaku. Setelah dana diterima, pelaku menghilang tanpa mengirimkan barang. Dalam pendekatan forensik digital, pola ini menghasilkan celah dalam jejak transaksi resmi platform, namun tetap memungkinkan pelacakan melalui analisis rekening penerima, riwayat komunikasi, dan metadata transaksi dari perangkat korban dan pelaku[23].

Keempat, menurut laporan dari Infobank News, terjadi kasus di platform TikTok Shop di mana pelaku memanipulasi proses refund sehingga dana dikirim bukan ke akun asli pembeli, melainkan ke akun OVO yang telah dibajak sebelumnya. Kejahatan ini menunjukkan eksploitasi sistem pengembalian dana digital serta penyalahgunaan identitas akun pihak ketiga. Dalam konteks investigasi forensik, kasus ini menuntut analisis log aktivitas akun, data login, alamat IP, serta identifikasi perangkat yang digunakan untuk pembajakan dan modifikasi akun[24].

Empat kasus nyata yang dilaporkan menunjukkan bahwa penipuan e-commerce masa kini seringkali melibatkan manipulasi sistem pembayaran, pengalihan transaksi ke luar platform resmi, serta eksploitasi komunikasi langsung antara pelaku dan korban. Modus seperti transaksi segitiga, permintaan transfer ulang, penggunaan rekening pribadi di luar escrow resmi, hingga pengalihan refund ke akun e-wallet yang dibajak, menjadi bukti nyata bahwa pola kejahatan digital semakin kompleks dan variatif. Oleh karena itu, skenario simulasi dalam penelitian ini tidak dibuat secara hipotetis, melainkan merupakan representasi faktual dari pola-pola penipuan yang benar-benar terjadi. Justifikasi berbasis kasus nyata ini memperkuat validitas eksternal penelitian dan mendukung relevansi penerapan metode forensik digital dalam menghadapi tantangan investigasi penipuan e-commerce di dunia nyata.

E . Metode Perbandingan

Perbandingan dilakukan dengan berbagai alat forensik digital berdasarkan data forensik yang tersedia. Tujuan dari metode ini adalah untuk menentukan hasil analisis dalam bentuk angka kuantitatif dengan menggunakan rumus persentase yang terdapat dalam Persamaan (1).

$$Par = P\left(\frac{\sum ar0}{\sum arT}\right) \times 100\% \quad (1)$$

Keterangan:
Par = Indeks akurasi alat forensik yang digunakan.
$\sum$ **ar0** = Jumlah parameter material yang terdeteksi oleh alat forensik.
$\sum$ **arT** = Jumlah total parameter material yang digunakan dalam analisis.

Rumus ini menghitung tingkat akurasi alat forensik dengan membandingkan jumlah parameter yang berhasil dideteksi dengan jumlah total parameter yang digunakan dalam analisis. Nilai yang dihasilkan dinyatakan dalam bentuk persentase, yang menunjukkan seberapa efektif alat forensik dalam mengidentifikasi bukti atau material yang relevan dalam proses investigasi digital [13].

III. HASIL DAN PEMBAHASAN

A. Plan

Pada tahap ini, dilakukan perencanaan rinci terkait langkah-langkah yang akan diambil selama penelitian, termasuk penyusunan skenario simulasi penipuan di *e-commerce* TikTok Shop serta persiapan alat dan perangkat lunak forensik yang dibutuhkan. Selanjutnya, proses investigasi berfokus pada identifikasi dan pengumpulan bukti digital yang relevan berdasarkan variabel yang telah ditentukan, seperti riwayat percakapan dalam chat, bukti transaksi, rekaman video, tangkapan layar, serta data lainnya yang dapat mendukung analisis forensik dalam mengungkap modus operandi pelaku penipuan.

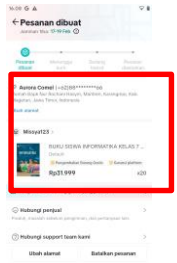
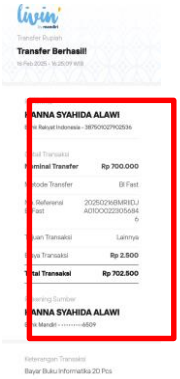
a) *Handphone* pelaku

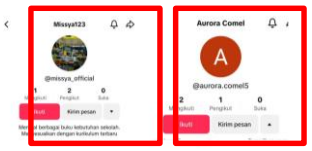
b) *Handphone* korban

Gambar 3. Barang bukti berupa *handphone*

Gambar 3 menunjukkan perangkat Android yang digunakan sebagai barang bukti fisik dalam kasus penipuan *e-commerce* di TikTok Shop. Perangkat ini dianalisis guna memastikan keaslian, integritas, dan validitas barang bukti digital selama proses investigasi forensik. Pemeriksaan dilakukan untuk memperoleh data yang relevan, seperti riwayat percakapan, bukti transaksi, serta jejak digital lainnya yang dapat mendukung proses penyelidikan dan mengungkap modus operandi pelaku

TABEL 3
DATA ASAL

No.	Data Digital	Metadata	Jumlah
1 Gambar	 *Screenshoot* Pemesanan	Ukuran: 235,2 KB Dimensi: 720 x 1280 Tipe : JPG	1
2 Gambar	 *Screenshoot* Pembayaran	Ukuran: 309 KB Dimensi: 1080 x 2580 Tipe: JPG	1
3 Vidio	 Video Barang	Ukuran: 10,0 MB Dimensi: 1080 x 2580 Tipe: MP4 Durasi: 00:00:59:667	1

4	Akun	 Akun Pelaku dan Korban	User Korban :@aurora.comel5 (aurora comel) User Pelaku: @missya_official (Missya123)	2
5	Chat	 Bukti Chat	Pengirim: Missya123 Penerima: aurora comel	8
			Total	13

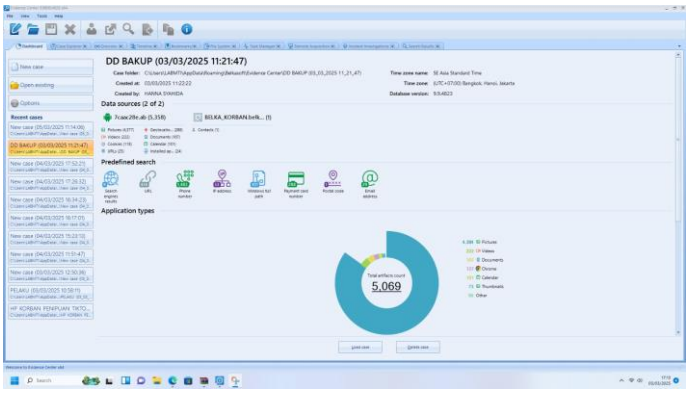
Tabel 3 menyajikan barang bukti digital yang dikumpulkan selama investigasi. Bukti digital yang terdokumentasi mencakup tangkapan layar transaksi, gambar, video, akun pengguna, serta percakapan chat antara korban dan pelaku. Setiap bukti disertai dengan metadata yang mencakup ukuran file, resolusi, format, dan jumlah data yang ditemukan. Penelitian ini bertujuan untuk menganalisis bukti digital guna mengidentifikasi pola penipuan, menelusuri keterlibatan akun tertentu, dan memastikan keaslian dan validitas barang bukti dalam proses forensik digital.

Jumlah dataset yang digunakan dalam penelitian ini memang masih terbatas, namun skenario simulasi yang disusun telah dirancang secara representatif berdasarkan pola penipuan nyata yang terjadi pada platform e-commerce TikTok Shop. Validitas skenario diperkuat dengan rujukan pada kasus-kasus aktual yang dilaporkan di media, sehingga mampu mencerminkan dinamika dan tantangan yang dihadapi dalam investigasi forensik digital sesungguhnya. Dengan fokus utama pada penerapan metode ACPO dan evaluasi efektivitas alat forensik dalam menjaga integritas bukti digital, penelitian ini tetap memberikan kontribusi yang signifikan terhadap pemahaman dan pengembangan pendekatan forensik pada kasus penipuan digital.

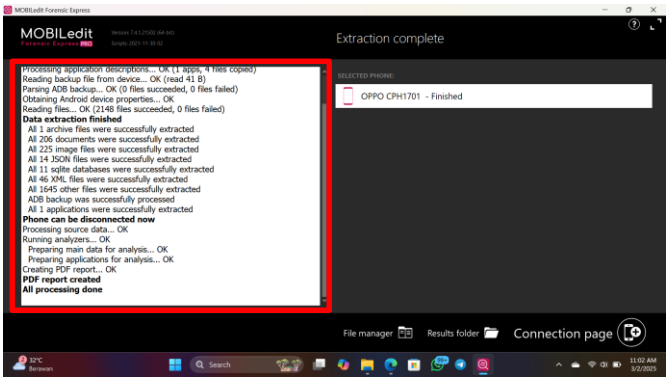
Mekanisme penipuan yang disimulasikan dalam penelitian ini, seperti pembayaran di luar platform dan penghapusan bukti chat, merupakan bentuk umum modus yang banyak dilaporkan oleh korban di Indonesia. Hal ini menunjukkan bahwa meskipun data bersifat terbatas, tingkat relevansi terhadap kejadian nyata tetap tinggi. Penelitian ini tidak hanya menekankan jumlah data, tetapi juga kualitas skenario dan kesesuaian metode terhadap konteks forensik lapangan. Oleh karena itu, hasil yang diperoleh masih memiliki nilai aplikatif dalam mendukung proses investigasi digital pada kasus serupa.

B. Capture

Dalam penelitian ini, metode forensik statis diterapkan dengan beberapa langkah sistematis dalam tahap akuisisi data. Langkah pertama adalah mengamankan *smartphone* sebagai barang bukti untuk memastikan integritas data [25]. Selanjutnya, perangkat dilakukan proses *rooting* guna mendapatkan akses penuh terhadap sistem dan memungkinkan ekstraksi data yang lebih mendalam. Setelah proses *root* selesai, USB *debugging* diaktifkan untuk memfasilitasi komunikasi antara perangkat dan komputer. *Smartphone* dihubungkan ke komputer menggunakan kabel USB. MOBILedit Forensic Express dan Belkasoft dijalankan untuk menangkap



Gambar 4. Hasil ekstraksi Belkasoft

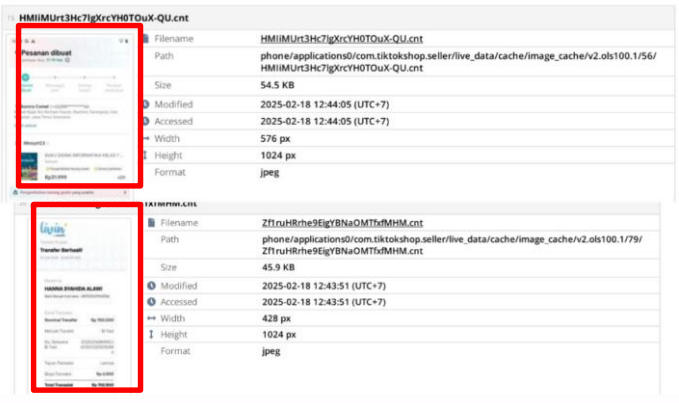


Gambar 5. Hasil Ekstraksi MOBILedit Forensic Express

kemudian mengekstrak data yang relevan. Informasi kasus seperti identitas perangkat, lokasi penyimpanan file investigasi, dan metadata bukti digital dimasukkan untuk memastikan dokumentasi yang akurat. Proses ini bertujuan untuk memperoleh bukti digital secara forensik tanpa mengubah struktur asli data. Hasil ekstraksi pada MOBILedit Forensic Express terdapat pada Gambar 5 dan Belkasoft pada Gambar 4

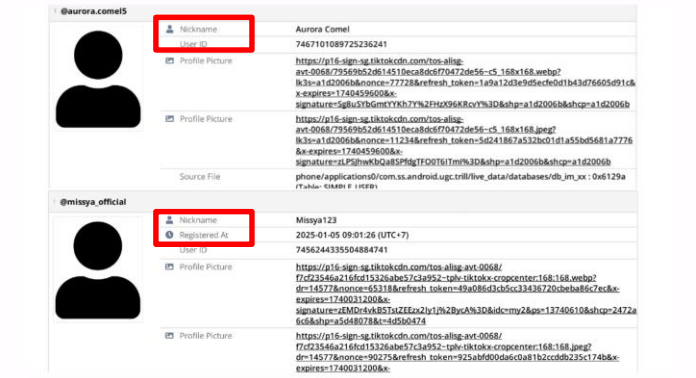
C. Analysis

Pada tahap ini dilakukan analisis mendalam berdasarkan parameter dan data yang telah diperoleh dari proses akuisisi dan ekstraksi sebelumnya. Analisis ini bertujuan untuk mengidentifikasi dan menginterpretasikan bukti digital yang relevan dalam kasus penipuan e-*commerce* di TikTok Shop.



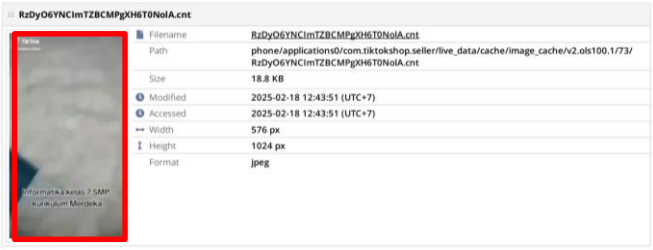
Gambar 6. Bukti Hasil Ekstraksi Gambar MOBILedit Forensic Express

Gambar 6 menunjukkan hasil ekstraksi bukti digital berupa gambar dari perangkat *mobile* yang diperoleh menggunakan MOBILedit Forensic Express dalam investigasi penipuan *e-commerce* di TikTok Shop. Gambar yang ditemukan merupakan bukti pemesanan barang dan bukti pembayaran yang dilakukan di luar *platform* resmi. Setiap gambar dilengkapi dengan detail informasi seperti nama file, ukuran, tanggal pembuatan, dan metadata lainnya yang dapat digunakan untuk analisis lebih lanjut dalam proses forensik digital



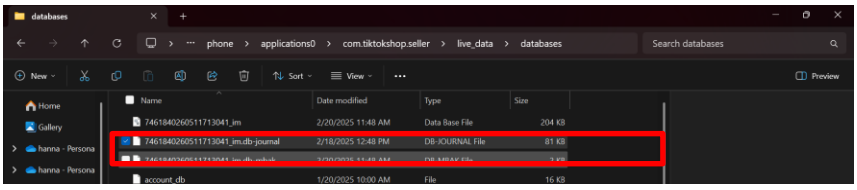
Gambar 7. Bukti Hasil Ekstraksi Akun

Gambar 7 merupakan hasil analisis menggunakan MOBILedit Forensic menunjukkan bahwa akun pengguna yang terlibat dalam transaksi ditemukan dalam basis data aplikasi TikTok Shop. Data yang diperoleh mencakup nickname, user ID, URL gambar profil, serta sumber file basis data tempat informasi tersebut tersimpan. Akun-akun ini diduga memiliki keterkaitan dengan aktivitas penipuan yang sedang diselidiki, dengan metadata yang menunjukkan detail pengguna serta waktu pendaftaran akun. Temuan ini menjadi bukti digital yang dapat digunakan dalam proses investigasi lebih lanjut.



Gambar 8. Bukti Hasil Ekstrasi Cache Cover Vidio

Gambar 8 merupakan hasil ekstraksi data digital menggunakan MOBILedit Forensic Express yang mengungkapkan bahwa dalam aplikasi TikTok Shop hanya ditemukan gambar cover video tanpa file video utuh. Gambar yang diperoleh merupakan cache gambar berformat JPEG, tersimpan dalam direktori aplikasi. Metadata yang terlampir, seperti asal video waktu akses dan modifikasi menunjukkan bahwa gambar tersebut dihasilkan secara otomatis oleh sistem aplikasi. Absennya file video asli dapat disebabkan oleh mekanisme penyimpanan sementara atau penghapusan otomatis oleh aplikasi sehingga diperlukan analisis lebih lanjut untuk memperoleh bukti digital yang lebih lengkap.

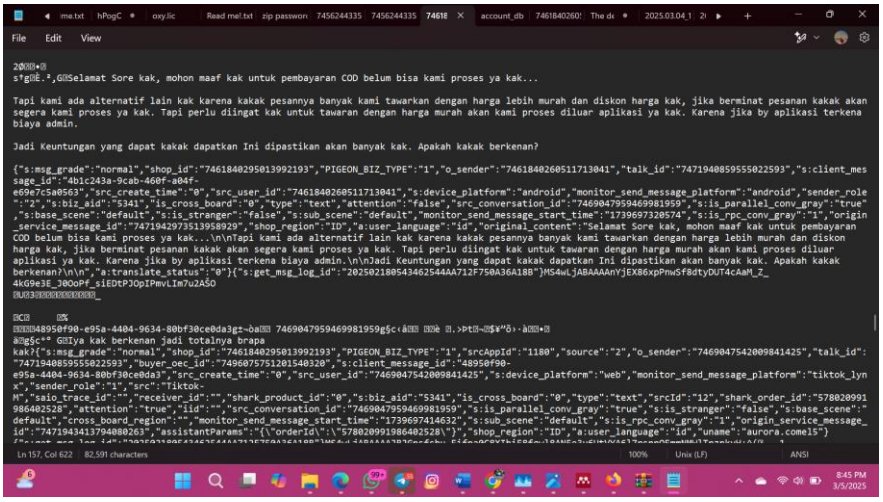


Gambar 4. Bukti Hasil Ekstraksi Chat

Gambar 9 merupakan hasil analisis forensik menggunakan MOBILedit Forensic Express yang menunjukkan bahwa pesan yang telah dihapus tidak dapat ditemukan langsung melalui fitur laporan aplikasi. Namun, melalui pemeriksaan lebih lanjut pada basis data internal aplikasi TikTok Shop, ditemukan file dengan nama sebagaimana yang ditandai dalam gambar, yaitu file berformat DB-JOURNAL. File ini berperan sebagai *log* sementara yang menyimpan perubahan data sebelum diperbarui dalam basis data utama. Keberadaan file ini mengindikasikan bahwa pesan yang dihapus masih dapat dipulihkan dengan teknik forensik lanjutan, seperti analisis struktur basis data SQLite atau penggunaan metode *data carving* untuk merekonstruksi kembali

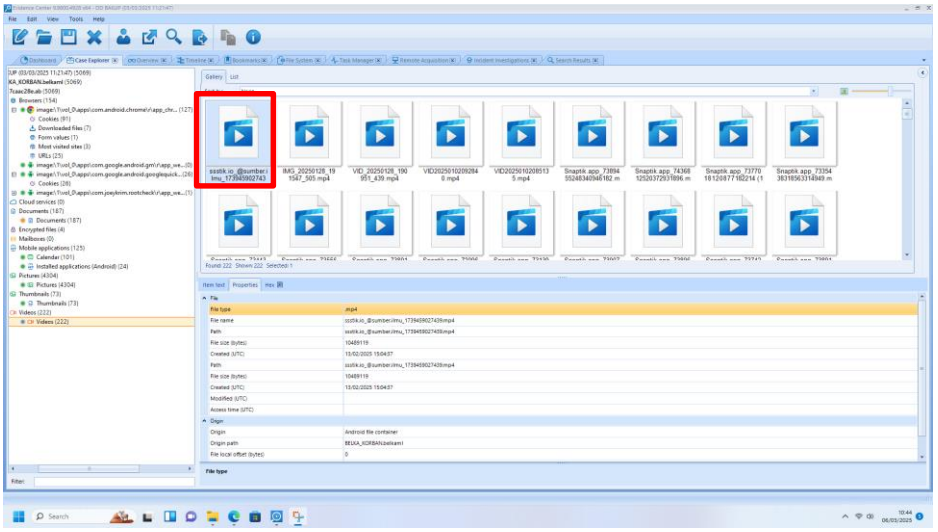
informasi yang hilang.

Pada gambar 10 File yang ditampilkan merupakan DB-JOURNAL, yaitu bagian dari sistem basis data yang digunakan untuk menyimpan perubahan data sebelum diintegrasikan ke dalam basis data utama. Dalam konteks investigasi ini, DB-JOURNAL tersebut berisi *log* percakapan yang telah dihapus oleh pengguna dalam aplikasi TikTokShop.

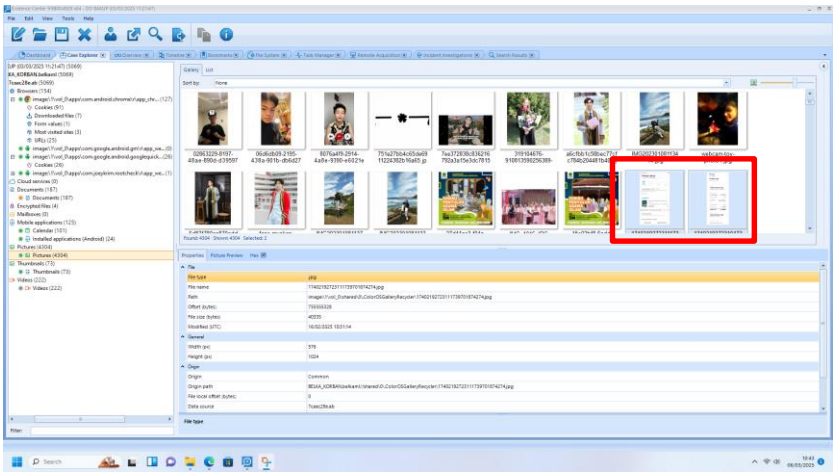


Gambar 5. Isi File DB-JOURNAL

Gambar 11 merupakan hasil analisis menggunakan Belkasoft Evidence Center yang mengungkapkan adanya bukti pembayaran yang dilakukan di luar *platform* dan bukti pemesanan barang yang ditemukan dalam perangkat yang diperiksa.

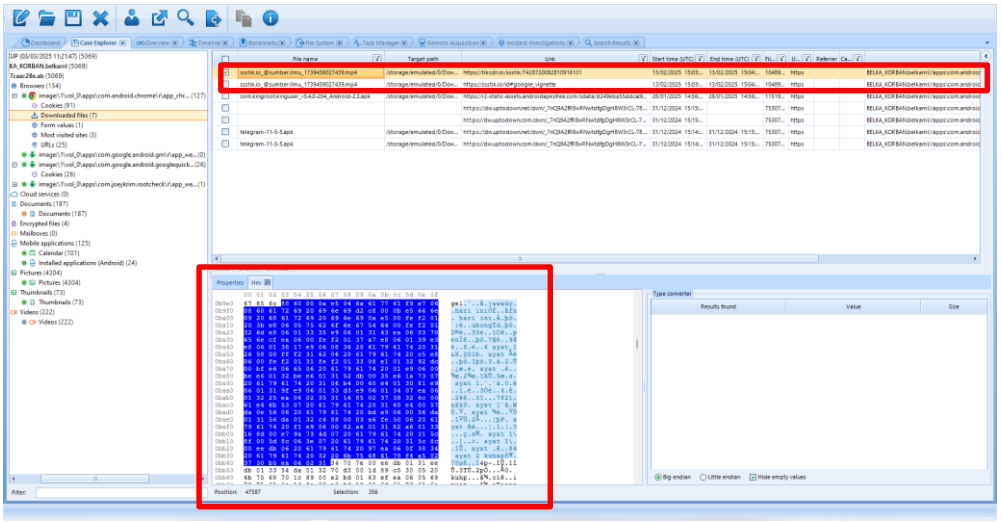


Gambar 6. Bukti Hasil Ekstraksi Detail Asal Gambar pada Belkasoft



Gambar 7. Hasil Ekstraksi Video pada Belkasoft Evidence Center

Gambar 12 menampilkan bukti yang ditemukan menggunakan Belkasoft yakni video dengan nama **ssstik.io_@sumber.ilmu_1739459027439.mp4.** Selain menemukan bukti video, analisis dengan Belkasoft Evidence Center menemukan tautan video yang mengarah ke konten yang digunakan dalam kasus penipuan. Tautan ini berasal dari riwayat unduhan dan *browser* dengan metadata yang mencatat jalur penyimpanan, sumber tautan, dan waktu unduh. Selain itu, analisis heksadesimal menunjukkan struktur data yang konsisten dengan file terkait. Jika tautan ini dijalankan di *browser* maka akan mengarah langsung ke video yang digunakan dalam skema penipuan dan memperkuat bukti digital dalam investigasi forensik yang dapat dilihat pada Gambar 13.



Gambar 8. Bukti Hasil Ekstrasi Detail Asal Vidio pada Belkasoft Evidence Center

D. Present

Pada tahap ini, barang bukti hasil analisis harus disampaikan atau dilaporkan dengan memastikan keabsahannya dalam konteks forensik dan hukum sehingga dapat dipertanggungjawabkan secara valid [6]. Seluruh dokumen pada tahap ini, barang bukti digital yang berhasil diperoleh setelah melalui proses investigasi ditampilkan dalam Tabel 4 yang berisi hasil perolehan barang bukti. Analisis menggunakan MOBILedit Forensic dan Belkasoft menunjukkan hasil yang berbeda dalam mendeteksi data. MOBILedit Forensic berhasil menemukan pesan teks, akun pengguna, dan bukti pemesanan dan pembayaran di luar *platform*, tetapi gagal menemukan file video dan hanya mendapatkan gambar cover video. Sebaliknya, Belkasoft tidak menemukan pesan teks maupun akun pengguna, tetapi berhasil memperoleh gambar, video, dan tautan sumber video dari basis data aplikasi TikTok Shop.

Dengan menerapkan metode ACPO, data yang diperoleh memberikan gambaran lebih jelas mengenai pola komunikasi dan transaksi yang terjadi sebagaimana dirangkum dalam Tabel 4. Tabel tersebut juga menyajikan perbandingan efektivitas kedua tools dalam memperoleh data digital dengan persentase keberhasilan dihitung menggunakan Persamaan (1).

TABEL 4
PERBANDINGAN EFEKTIVITAS MOBILE EDIT FORENSIC DAN BELKASOFT EVIDENCE CENTER

Bukti Digital	Jumlah	MOBILedit Forensic	Belkasoft Evidence Center
Pesan Gambar	2	2	2
Pesan Video	2	0	1
Pesan Teks	8	8	0
Akun	2	2	0
Total	13	12	3

Tabel 5 menyajikan perbandingan efektivitas kedua *tools* dalam memperoleh data digital, selanjutnya persentase keberhasilan dihitung menggunakan Persamaan (1).

TABEL 4
PERBANDINGAN EFEKTIVITAS MOBILE EDIT FORENSIC DAN BELKASOFT EVIDENCE CENTER

MOBILedit Forensic Express:	$Par = \left(\frac{12}{13}\right) \times 100\% = 92{,}3\%$
Belkasoft Evidence Center**:**	$Par = \left(\frac{3}{13}\right) \times 100\% = 23{,}1\%$

IV. SIMPULAN

Penelitian ini menganalisis investigasi forensik digital pada e-commerce TikTok Shop dengan menerapkan metode ACPO untuk memperoleh bukti digital dalam kasus penipuan. Hasil eksperimen menunjukkan bahwa penggunaan dua perangkat lunak forensik, yaitu MOBILedit Forensic Express dan Belkasoft Evidence Center, menghasilkan tingkat keberhasilan yang berbeda dalam proses ekstraksi bukti digital.Secara statistik, MOBILedit Forensic Express berhasil mengekstraksi 12 dari 13 objek bukti digital, dengan tingkat akurasi 92,31%, sedangkan Belkasoft Evidence Center hanya berhasil mengekstraksi 3 dari 13 objek, dengan tingkat akurasi 23,08%. Perbedaan ini menunjukkan variasi signifikan dalam kemampuan masing-masing alat terhadap jenis bukti digital yang berbeda, seperti chat, akun pengguna, gambar, dan video.MOBILedit terbukti efektif dalam memperoleh chat dan akun pengguna, sementara Belkasoft unggul dalam mengekstrak file multimedia dan tautan sumber. Temuan ini menegaskan bahwa tidak ada satu alat yang mampu melakukan akuisisi secara menyeluruh, sehingga pendekatan multi-tools sangat diperlukan untuk memperoleh bukti digital secara optimal dan komprehensif. Penelitian selanjutnya dapat berfokus pada pengembangan teknik rekonstruksi data yang lebih mendalam serta eksplorasi alat forensik lainnya guna meningkatkan efektivitas investigasi terhadap penipuan berbasis *e-commerce*. Penelitian ini belum mencakup variasi perangkat, sistem operasi, atau kondisi teknis seperti chat terenkripsi dan two-factor authentication. Namun, skenario yang digunakan telah merepresentasikan pola penipuan umum yang terjadi di TikTok Shop. Penelitian lanjutan disarankan untuk menambahkan variasi tersebut guna meningkatkan kedalaman dan relevansi analisis forensik digital.

UCAPAN TERIMAKASIH

Ucapan rasa terima kasih kepada Universitas Ahmad Dahlan atas dukungan dan fasilitas yang diberikan dalam penyelesaian penelitian ini. Semoga hasil penelitian ini dapat memberikan kontribusi bagi perkembangan ilmu forensik digital, khususnya dalam investigasi forensik pada kasus penipuan pada *e-commerce.*

DAFTAR PUSTAKA

[1] Q. Wu, Y. Sang, D. Wang, and Z. Lu, "Malicious Selling Strategies in Livestream E-commerce: A Case Study of Alibaba's Taobao and ByteDance's TikTok," *arXiv*, vol. 30, no. 3, pp. 1–30, 2022, doi: 10.1145/3577199.

[2] C. M. Annur, "Ini Media Sosial Paling Banyak Digunakan di Indonesia Awal 2024," Databoks. Accessed: Jun. 17, 2025. [Online]. Available: https://databoks.katadata.co.id/teknologi-telekomunikasi/statistik/66ea436ab12f2/ini-media-sosial-paling-banyak-digunakan-di-indonesia-awal-2024

[3] Kaspersky, "Q2 2023, Kaspersky Catat 7 Juta Lebih Serangan Siber di Indonesia," BPIP.CSIRT. Accessed: Jun. 17, 2025. [Online]. Available: https://csirt.bpip.go.id/posts/q2-2023-kaspersky-catat-7-juta-lebih-serangan-siber-di-indonesia

[4] E. Ariyanti, "Identifikasi Bukti Digital Instagram Web Dengan Live Forensic Pada Kasus Penipuan Online Shop," *Cyber Security*

dan Forensik Digital., vol. 4, no. 2, pp. 58–62, 2022, doi: 10.14421/csecurity.2021.4.2.2436.

[5] C. Neale, I. Kennedy, B. Price, Y. Yu, and B. Nuseibeh, "The case for Zero Trust Digital Forensics," *Forensic Science International: Digital Investigation.*, vol. 40, no. 40, pp. 1–13, 2022, doi: 10.1016/j.fsidi.2022.301352.

[6] K. Anam, A. Yudhana, and H. Yuliansyah, "File carving Analyze of Foremost and Autopsy on external SSD mSATA using the Association of Chief Police Officer Method," *ILKOM Jurnal Ilmiah.*, vol. 16, no. 3, pp. 283–295, 2024.

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

[8] G. Horsman, "ACPO principles for digital evidence: Time for an update?," *Forensic Science International: Reports*, vol. 2, no. January, p. 100076, 2020, doi: 10.1016/j.fsir.2020.100076.

[9] 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, doi: 10.30865/jurikom.v9i4.4738.

[10] H. Heath, Á. MacDermott, and A. Akinbi, "Forensic analysis of ephemeral messaging applications: Disappearing messages or evidential data?," *Forensic Science International: Digital Investigation.*, vol. 46, no. 46, pp. 1–24, 2023, doi: 10.1016/j.fsidi.2023.301585.

[11] G. Humphries, R. Nordvik, H. Manifavas, P. Cobley, and M. Sorell, "Law enforcement educational challenges for mobile forensics," *Forensic Science International: Digital Investigation.*, vol. 38, p. 301129, 2021, doi: 10.1016/j.fsidi.2021.301129.

[12] M. F. Fadillah and T. Yuniati, "Perbandingan Hasil Recovery Tools Mobile Forensic Di Smartphone Android Menggunakan Metode National Institute Of Justice (NIJ)," *Cyber Security dan Forensik Digital.*, vol. 6, no. 2, pp. 54–61, 2024, doi: 10.14421/csecurity.2023.6.2.4172.

[13] R. N. Bintang, R. Umar, and A. Yudhana, "Assess of Forensic Tools on Android Based Facebook Lite with the NIST Method," *Scientific Journal of Informatics*, vol. 8, no. 1, pp. 1–9, 2021, doi: 10.15294/sji.v8i1.26744.

[14] I.Riadi, R.Umar, and M. I. Syahib, "Akuisisi Bukti Digital Viber Messenger Android Menggunakan Metode National Institute of Standards and Technology (NIST)," *J. RESTI Jurnal RESTI (Rekayasa Sistem dan Teknologi Informasi)*, vol. 5, no. 1, pp. 45–54, 2021, doi: 10.29207/resti.v5i1.2626.

[15] A. Tofik, G. Z. Muflih, and T. Informatika, "Akuisisi Barang Bukti Digital Pada Aplikasi Discord," *Jurnal Mahasiswa Teknik Informatika.*, vol. 8, no. 6, pp. 12122–12128, 2024.

[16] A. Hidayah, F. Fachri, and T. Informatika, "Analisis Bukti Digital Terhadap Kasus Prostitusi Online Pada Aplikasi Michat Menggunakan Metode ACPO," Jurnal Mahasiswa Teknik Informatika. vol. 9, no. 1, pp. 906–912, 2025.

[17] M. S. Jafri, S. Raharjo, and M. R. Arief, "Implementation of ACPO Framework for Digital Evidence Acquisition in Smartphones," *CCIT (Creative Communication and Innovative Technology) Journal.*, vol. 15, no. 1, pp. 82–105, 2022, doi: 10.33050/ccit.v15i1.1586.

[18] M. Giovani, "Analisis Forensik Aplikasi Discord Pada Android Berdasarkan Acpo Framework," *Journal of Information Systems Management and Digital Business.*, vol. 1, no. 3, pp. 307–313, 2024, doi: 10.59407/jismdb.v1i3.441.

[19] G. Horsman and A. Dodd, "Competence in digital forensics," *Forensic Science International: Digital Investigation.*, vol. 51, no. July, pp. 1–10, 2024, doi: 10.1016/j.fsidi.2024.301840.

[20] G. Thornton and P. Bagheri Zadeh, "An investigation into Unmanned Aerial System (UAS) forensics: Data extraction & analysis," *Forensic Science International: Digital Investigation.*, vol. 41, 2022, doi: 10.1016/j.fsidi.2022.301379.

[21] Rifqi, "Penipuan Modus Transaksi Segitiga Marak di Marketplace, Ini Cara Kerjanya dan Cara Menghindarinya," Tribata Polres Pangandaran. Accessed: Jun. 16, 2025. [Online]. Available: https://polrespangandaran.id/spkt/penipuan-modus-transaksi-segitiga-marak-di-marketplace-ini-cara-kerjanya-dan-cara-menghindarinya/?utm_

[22] Rifqi, "Permintaan 'Transfer Ulang' Jadi Modus Baru Menjebak Korban,"Tribata Polres Pangandaran. Accessed: Jun. 16, 2025. [Online]. Available: https://polrespangandaran.id/spkt/permintaan-transfer-ulang-jadi-modus-baru-menjebak-korban/?utm_source=chatgpt.com

[23] Rifqi, "Penipuan Rekening Bersama di Marketplace," Tribata Polres Pangandaran. Accessed: Jun. 16, 2025. [Online]. Available: https://polrespangandaran.id/spkt/penipuan-rekening-bersama-di-marketplace/?

[24] M. Ibrahim, "Awas! Modus Penipuan Oknum Penjual TikTok Shop, Refund ke Akun OVO yang Dibajak," Infobanknews. Accessed: Jun. 16, 2025. [Online]. Available: https://infobanknews.com/awas-modus-penipuan-oknum-penjual-tiktok-shop-refund-ke-akun-ovo-yang-dibajak/#google_vignette

[25] A. M. Andre, F. C. Sicoli, L. P. De Melo, F. E. De Deus, and R. T. De Sousa Junior, "Acquisition of digital evidence in Android smartphones," *Proc. 9th Aust. Digit. Forensics Conf.*, no. December, pp. 116–124, 2011, doi: 10.4225/75/57b2c3dc40cf3.