CyberSecurity dan Forensik Digital e-ISSN: 2615-8442
Vol. 8, No. 1, Mei 2025, hlm. 43-52

Analisis Forensik *Mobile* Pada Aplikasi *E-Commerce* Menggunakan Metode *Association Of Chief Police Officers*

Rizal Prambudi[1], Imam Riadi[2], Murinto[3]

[1,3]Informatika, Universitas Ahmad Dahlan, Yogyakarta, Indonesia
[2]Sistem Informasi, Universitas Ahmad Dahlan, Yogyakarta, Indonesia
Email: [1]2407048005@webmail.uad.ac.id , [2]imam.riadi@is.uad.ac.id, [3]murintokusno@tif.uad.ac.id

Abstrak

Media sosial merupakan platform daring yang memungkinkan komunikasi tanpa batas waktu dan lokasi, memfasilitasi interaksi antar pengguna. Walaupun fungsionalitasnya luas, media sosial sering disalahgunakan untuk berbagai tindakan kejahatan siber. Salah satu aplikasi yang banyak disalahgunakan untuk kegiatan ilegal adalah aplikasi *e-commerce* yang menyediakan berbagai transaksi jual beli. Aplikasi *e-commerce* menyimpan data pribadi di perangkat digital yang bisa digunakan sebagai bukti digital dalam kegiatan kriminal. Penelitian ini bertujuan mendapatkan bukti digital dari skenario kasus penipuan aplikasi *e-commerce* dengan menerapkan teknik forensik pada perangkat *mobile* serta menggunakan kerangka kerja *Association of Chief Police Officers* (ACPO). Bukti digital meliputi gambar, video, dan pesan teks. Keakuratan *tools* yang digunakan dengan mengintegrasikan metode ACPO dalam mengekstraksi bukti digital juga menjadi fokus dalam penelitian. Penelitian ini menggunakan Oxygen Forensic Detective dan MOBILedit Forensic Express sebagai *tools*. Bukti digital yang berhasil dipulihkan dari perangkat bukti berupa gambar dan video. Hasil penelitian menunjukkan bahwa Oxygen Forensic Detective berhasil memperoleh bukti digital sebesar 37%, sementara MOBILedit Forensic Express memperoleh bukti sebesar 26%. Hasil ini mengindikasikan bahwa metode forensik digital efektif dalam mengungkap bukti kejahatan di aplikasi *e-commerce*, dengan Oxygen Forensic Detective lebih unggul dibandingkan MOBILedit Forensic Express. Pemilihan alat forensik yang tepat berperan penting dalam investigasi digital.Kajian ini diharapkan dapat mendorong penerapan integrasi metode ACPO dan penggunaan *tools* forensik dalam mengungkapkan bukti digital kejahatan melalui *e-commerce*.

Kata kunci: *media sosial, forensik digital, kejahatan siber, ACPO, aplikasi e-commerce*

Mobile Forensic Analysis Of E-Commerece Applications Using The Association Of Chief Police Officers Method

Abstract

Social media is an online platform that enables communication without time and location constraints, facilitating interaction between users. However, these platforms are often misused for various cybercrimes. One type of application frequently exploited for illegal activities is e-commerce applications, which provide various buying and selling transactions. E-commerce applications store personal data on digital devices that can be used as digital evidence in criminal activities. This study aims to obtain digital evidence from a fraud case scenario involving an e-commerce application by applying forensic techniques on mobile devices and using the Association of Chief Police Officers (ACPO) framework. The digital evidence includes images, videos, and text messages. Another objective of this research is to assess the accuracy of the forensic tools used when integrating the ACPO method to extract digital evidence. This study utilizes Oxygen Forensic Detective and MOBILedit Forensic Express as the forensic tools. The digital evidence successfully retrieved from the device consists of images and videos. The results show that Oxygen Forensic Detective managed to extract 37% of digital evidence, while MOBILedit Forensic Express recovered 26%. In conclusion, digital forensic techniques are effective in uncovering evidence of crimes within e-commerce applications, with Oxygen Forensic Detective outperforming MOBILedit Forensic Express. Selecting the appropriate forensic tool plays a crucial role in digital investigations. This research is expected to encourage the integration of the ACPO method and the use of forensic tools in revealing digital evidence of crimes conducted through e-commerce.

***Keywords**: social media, digital forensics, cybercrime, ACPO, e-commerce applications*

1. PENDAHULUAN

Dalam era digital yang semakin berkembang pesat, transaksi daring melalui platform *e-commerce* menjadi salah satu tren yang mendominasi aktivitas ekonomi masyarakat. Sejak 2020, jumlah pengguna *e-commerce* di Indonesia terus meningkat hingga mencapai 58,63 juta pada 2023 (Kementerian Perdagangan RI, 2024). Menurut Fema, et al. (2022), belanja konsumen melalui platform *e-commerce* meningkat setelah pandemi dimulai. Kementerian Perdagangan RI (2024), memprediksi pengguna *e-commerce* di Indonesia akan terus meningkat hingga 99,1 juta pengguna pada tahun 2029.

Shopee merupakan layanan *e-commerce* terpopuler di Indonesia yang memiliki jutaan pengguna aktif setiap harinya. Aplikasi *e-commerce* sekarang menyediakan berbagai fitur seperti belanja daring, pembayaran elektronik, dan layanan pengiriman barang yang memudahkan transaksi masyarakat. Namun, di balik kemudahan yang ditawarkan, meningkatnya transaksi digital juga membuka peluang bagi berbagai bentuk kejahatan siber, seperti penipuan, pencurian data pribadi, dan aktivitas ilegal lainnya. Pengadilan Negeri Surabaya (2025) mencatat, setidaknya ada 494 kasus penipuan transaksi online yang terdaftar hingga tahun 2025.

Forensik digital merupakan bidang penting untuk menyelidiki kejahatan dunia maya dan menganalisis bukti digital. Bidang ini melibatkan berbagai subdisiplin, termasuk forensik langsung, forensik jaringan, dan forensik seluler, yang merupakan bidang yang paling umum ditangani di Indonesia (Iman, Susanto and Inggi, 2020). Proses ini biasanya mencakup pengumpulan, analisis, dan penyajian bukti di pengadilan (Ramadhan, Zaini and Mardafora, 2022). Triase forensik digital, mirip dengan triase medis, memprioritaskan bukti potensial untuk diselidiki, yang bertujuan untuk mempercepat proses pengumpulan dan pemeriksaan di tempat kejadian perkara (Subektiningsih, 2020). Perkembangan forensik digital di Indonesia telah dipelajari melalui tinjauan sistematis, menganalisis penerapannya dalam investigasi kejahatan dunia maya (Aisyah, et al., 2022). Menurut Meha, et al. (2021), *e-commerce* mengubah transaksi konvensional menjadi aktivitas pasar virtual sehingga berdampak signifikan terhadap pertumbuhan ekonomi digital. Namun, literatul ilmiah yang membahas dampak kejahatan digital dalam platform ini secara mendalam masih terbatas.

Pertumbuhan pengunaan *e-commerce* yang sejalan dengan peningkatan risiko keamanan dan kejahatan siber memerlukan metode forensik digital sebagai solusi praktis untuk mengungkapkan bukti-bukti kejahatan. Untuk memerangi ancaman tersebut, organisasi perlu memahami jenis serangan dunia maya saat ini, menerapkan strategi keamanan yang efektif, dan memanfaatkan alat dan teknologi keamanan dunia maya yang tepat (Laksana and Mulyani, 2024). Analisis forensik digital menjadi salah satu solusi yang sangat diperlukan. Forensik digital merupakan proses pengumpulan, analisis, dan interpretasi data elektronik dengan tujuan untuk menemukan bukti digital yang relevan dalam sebuah investigasi (Ramadhan, Zaini and Mardafora, 2022). Dalam konteks aplikasi *e-commerce*, analisis forensik digital bertujuan untuk mengidentifikasi dan memitigasi aktivitas yang mencurigakan serta mendukung proses penegakan hukum.

Salah satu metode yang digunakan dalam investigasi forensik digital adalah pendekatan *Association of Chief Police Officers* (ACPO). Metode ini mengutamakan prinsip bahwa bukti digital harus tetap utuh dan dapat diterima di pengadilan (Safitri, Riadi and Sunardi, 2023). Metode ini juga berfungsi melacak perkembangan investigasi forensik secara transparan (Prasongko, Yudhana and Riadi, 2022). Penerapan metode ini akan dibantu dengan *tools* forensik lainnya seperti MOBILedit Forensic dan Oxygen Forensic Detective.

MOBILedit Forensic adalah perangkat yang memungkinkan pengguna dapat mengakses dan mengekstrak berbagai jenis data dari ponsel pintar, termasuk pesan, kontak, riwayat panggilan, dan informasi SIM card (Setiawan and Riadi, 2024). Oxygen Forensic Detective merupakan alat forensik digital yang digunakan untuk menganalisis bukti dari perangkat seluler, khususnya dalam investigasi kejahatan dunia maya. Beberapa penelitian telah menggunakan alat ini untuk mengekstrak dan memeriksa bukti digital dari ponsel pintar Android (Lestari, Lubis and Siregar, 2023).

Dalam konteks ini, sejumlah studi terdahulu memberikan fondasi penting namun masih memiliki keterbatasan. Zakarneh (2024) dalam studinya mengenai investigasi forensik seluler pada platform WhatsApp menyoroti bahwa meskipun banyak penelitian telah membahas alat dan teknik forensik digital, integrasi kerangka ACPO masih sering diabaikan. Hal ini membatasi efektivitas pendekatan forensik digital dalam menangani kejahatan siber secara menyeluruh, khususnya dalam konteks *e-commerce*. Tinjauan komprehensif oleh Sutikno (2024) mengevaluasi berbagai *tools* forensik seluler namun menunjukkan adanya kesenjangan penelitian terkait belum digunakannya pendekatan ACPO untuk meningkatkan efektivitas investigasi. Sementara itu, penelitian oleh Tuharea, Luthfi, and Ramadani (2023) menyoroti kemajuan dalam forensik digital melalui penerapan *Small Scale Digital Device Forensics* (SSDDF) dan analisis metadata media sosial. Studi ini mengatasi beberapa keterbatasan sebelumnya dengan mengintegrasikan metodologi untuk ekstraksi bukti yang lebih efektif dari perangkat digital ringkas dan platform sosial, meskipun belum difokuskan pada konteks *e-commerce*. Selain itu, penelitian oleh Riadi and Yudhana (2023) mengevaluasi alat forensik seluler untuk investigasi kejahatan digital, dengan fokus pada perbandingan dan penilaian teknis berbagai *tools*. Namun, studi ini tidak secara khusus

membahas penerapannya dalam konteks deteksi penipuan *e-commerce* atau menghubungkannya dengan kerangka kerja ACPO, sehingga belum menjawab kebutuhan akan metodologi yang sistematis dalam investigasi digital berbasis *e-commerce*.

Saat ini, penelitian forensik digital yang secara spesifik menelaah aplikasi *e-commerce* di Indonesia masih tergolong minim, terutama yang menggunakan pendekatan sistematis seperti metode *Association of Chief Police Officers* (ACPO) dan membandingkan beberapa *tools* forensik secara empiris. Oleh karena itu, penelitian ini hadir untuk mengisi celah tersebut dengan mengintegrasikan metode ACPO ke dalam proses investigasi digital pada aplikasi e-commerce, serta melakukan evaluasi terhadap dua tools forensik digital terkemuka. Tujuannya adalah untuk menilai keandalan, validitas, dan keterpakaian bukti digital dalam konteks investigasi siber. Dengan pendekatan ini, penelitian diharapkan memberikan kontribusi signifikan dalam pengembangan metodologi forensik digital yang lebih terstruktur, aplikatif, dan dapat dijadikan referensi dalam proses penegakan hukum di Indonesia.

2. Studi Literatur

Tahap ini bertujuan mengumpulkan referensi terkait analisis forensik data pada aplikasi *e-commerce* Shopee. Sumber informasi diperoleh dari jurnal, artikel, dan buku di platform seperti *Google Scholar*, *ResearchGate*, dan *ScienceDirect*, dengan kata kunci seperti "Forensik Digital", "Investigasi E-Commerce", dan "Metode ACPO dalam Forensik Digital". Informasi yang dikumpulkan membantu memahami konsep forensik digital dan merancang metode investigasi yang tepat.

Beberapa studi sebelumnya telah menunjukkan efektivitas berbagai metode dan alat forensik digital dalam proses investigasi kejahatan siber. Misalnya, penelitian oleh Mualfah, Syam, dan Baidarus (2023) menerapkan pendekatan National Institute of Justice (NIJ) dalam menganalisis aplikasi *Signal Messenger*, mencakup lima tahap utama yaitu identifikasi, pengumpulan, pemeriksaan, analisis, dan pelaporan. Dalam studi tersebut, Oxygen Forensic Detective mampu mengekstrak lima dari enam artefak digital, menghasilkan tingkat keberhasilan sebesar 83,33%. Sementara itu, Belkasoft Evidence Center hanya berhasil memperoleh empat dari enam artefak, dengan tingkat keberhasilan 66,67%.

Penelitian lain oleh Setyawan (2023) menggunakan kerangka kerja NIST dalam analisis forensik terhadap aplikasi *Skype*. Hasilnya menunjukkan bahwa Oxygen Forensic Suite menunjukkan performa tertinggi dengan tingkat keberhasilan 98%, diikuti oleh Belkasoft Evidence Center sebesar 88% dan MOBILedit Forensic Express sebesar 84%. Di sisi lain, studi Yudhana et al. (2022) menggunakan pendekatan DFRWS untuk menganalisis data dari aplikasi *WhatsApp*. Mereka menemukan bahwa MOBILedit Forensic Express memiliki tingkat akurasi 84,6% dalam proses ekstraksi data, sementara HashMyFiles mencapai akurasi 100% dalam memverifikasi keaslian bukti digital.

Selanjutnya, Riadi, Yudhana, dan Fanani (2023) melakukan kajian terhadap aplikasi *MiChat* dengan menerapkan metode ACPO. Penelitian ini menunjukkan bahwa tahapan dalam metode ACPO terutama perencanaan, akuisisi, analisis, dan pelaporan dapat secara efektif digunakan dalam pemulihan bukti digital, khususnya ketika menggunakan alat seperti MOBILedit Forensic. Selain itu, Aziz et al. (2021) membandingkan kerentanan tiga aplikasi pesan instan *Skype*, Telegram, dan *WhatsApp* dan menemukan bahwa *Skype* cenderung lebih rentan terhadap analisis forensik dibandingkan dua aplikasi lainnya, dengan tingkat kerentanan yang lebih tinggi mencapai sekitar 66%.

Berdasarkan temuan-temuan tersebut, dapat disimpulkan bahwa sebagian besar penelitian forensik digital masih terfokus pada platform media sosial dan aplikasi pesan instan. Berbeda dengan penelitian-penelitian sebelumnya, penelitian ini memberikan kontribusi dengan mengkaji forensik digital pada konteks aplikasi *e-commerce*, khususnya Shopee, yang hingga saat ini belum banyak dieksplorasi dalam kajian akademik.

Adapun keterbatasan dalam penelitian ini meliputi beberapa aspek penting. Pertama, proses *rooting* tidak dilakukan terhadap perangkat uji. Hal ini dimaksudkan untuk menjaga integritas prosedur ACPO yang menekankan pada prinsip non-intervensi terhadap sistem asli demi mempertahankan validitas bukti digital. Kedua, penelitian ini dilakukan dalam konteks aplikasi *e-commerce*, suatu area yang masih relatif minim dijadikan objek studi dalam ranah digital forensik, sehingga pembanding sistematis secara langsung masih terbatas. Kebanyakan literatur terdahulu lebih banyak mengulas aplikasi media sosial, yang memiliki karakteristik berbeda *dari e-commerce* dalam hal struktur data dan model komunikasi digital.

3. METODOLOGI

Penelitian ini berfokus pada analisis forensik data dalam aplikasi *e-commerce* menggunakan metode ACPO. Terdapat metode forensik digital lain yang telah dikembangkan untuk membantu investigasi kejahatan siber, seperti *Digital Forensic Research Workshop* (DFRWS), *National Institute of Standards and Technology* (NIST), dan *National Institute of Justice* (NIJ). Metode ACPO dipilih dalam penelitian ini karena kemampuannya memastikan setiap tahapan penanganan bukti dilakukan sesuai dengan standar hukum yang berlaku, dengan demikian, hasil analisis dapat dijadikan sebagai bukti yang valid dalam prosedur hukum (Dahlan, Yudhana and Yuliansyah, 2024). Metode ini

memberikan keunggulan dalam proses investigasi forensik digital, terutama dalam kasus yang berkaitan dengan transaksi dan komunikasi pengguna di aplikasi *e-commerce*. ACPO lebih fleksibel dan dapat diterapkan langsung di lapangan. Dengan prosedur yang sistematis, ACPO memungkinkan pengumpulan, penyimpanan, serta analisis bukti secara cepat, sehingga dapat mencegah risiko kehilangan atau perubahan data, terutama pada transaksi atau percakapan yang telah dihapus.

Pemilihan Oxygen Forensic Detective dan MOBILedit Forensic Express dalam penelitian ini didasarkan pada kemampuan memberikan keseimbangan antara akurasi hasil, efisiensi waktu, keunggulan teknis, efisiensi biaya, dan kemudahan penggunaan dibandingkan dengan *tools* forensik mobile lain seperti Cellebrite UFED, MSAB XRY, atau Magnet AXIOM yang cenderung mahal dan memerlukan pelatihan intensif. (Alblooshi et al., 2024). Oxygen Forensic Detective dikenal memiliki kemampuan analisis mendalam terhadap berbagai data digital, termasuk riwayat lokasi, komunikasi, data aplikasi media sosial, serta dukungan fitur *Optical Character Recognition* (OCR) dan analisis hubungan sosial yang memperkuat proses investigasi digital. Selain itu, Oxygen Forensic Detective juga mendukung berbagai jenis sistem operasi dan perangkat mobile, sehingga fleksibel dalam berbagai skenario forensik.

Sementara itu, MOBILEdit Forensic menawarkan kelebihan dari sisi antarmuka pengguna yang intuitif dan proses ekstraksi data yang cepat. MOBILEdit Forensic mendukung berbagai jenis perangkat dan format *file*, serta cepat beradaptasi dengan pembaruan aplikasi mobile terbaru (Maxsutbekova, 2023).

Penelitian ini menggunakan beberapa alat dan bahan untuk proses ekstraksi dan analisis data dari aplikasi *e-commerce*. Alat dan bahan tersebut dirincikan dalam Tabel 1.

Tabel 1. Alat dan Bahan Penelitian

Kategori	*Hardware/Tools*	Fungsi
Hardware	Ponsel Vivo 1904	Objek penelitian
Hardware	Laptop NEC Versapro	*Workstation* untuk analisis forensik
Hardware	USB *Connector*	Penghubung ponsel dengan laptop
Software	Aplikasi *e-commerce*	Aplikasi investigasi penelitian
Software	Oxygen Forensic Detective 17.1.0.131	Aplikasi forensik digital
Software	MOBILedit Forensic Express 7.4.1.21502	Aplikasi forensik digital

Alat-alat ini memungkinkan proses pemulihan data secara langsung dari perangkat, sehingga mendukung investigasi kasus yang berkaitan dengan dugaan kecurangan atau pelanggaran dalam transaksi *e-commerce*. Tahapan penelitian ini dapat dilihat pada Gambar 1.

Gambar 1. Metodologi Penelitian

Gambar 1 menunjukkan tahapan penelitian yang dilakukan, yaitu studi literatur, pembuatan skenario kasus, dan proses analisis menggunakan metode ACPO.

3.1. Skenario Kasus

Pada tahap ini, penelitian dilakukan melalui pendekatan berbasis simulasi terhadap kasus penipuan dalam aplikasi *e-commerce*, khususnya Shopee. Skenario yang digunakan tidak berasal dari kejadian nyata, melainkan dirancang berdasarkan pola umum dari kasus-kasus penipuan digital yang telah dilaporkan dalam berbagai studi sebelumnya. Seluruh data yang dianalisis dalam penelitian ini merupakan data simulasi yang dikembangkan oleh peneliti secara independen, menggunakan skenario forensik fiktif yang dirancang untuk tujuan akademik dan pengujian metode forensik digital Proses perolehan data dilakukan melalui rekayasa aktivitas pengguna di dalam aplikasi Shopee pada perangkat uji internal, yang sepenuhnya dilakukan oleh peneliti. Tidak ada data yang berasal dari pengguna asli, sistem produksi, ataupun perangkat eksternal yang memuat informasi pribadi pihak ketiga.

Dengan demikian, pendekatan ini menjamin bahwa seluruh prosedur penelitian dilakukan secara etis, tanpa melanggar hak privasi individu mana pun. Hal ini sejalan dengan prinsip-prinsip etika penelitian digital yang menekankan perlindungan data pribadi dan tidak diperolehnya informasi sensitif tanpa izin (CIOMS, 2021). Selain itu, perangkat yang digunakan untuk pengujian tidak terhubung dengan lingkungan produksi sebenarnya, melainkan hanya berfungsi sebagai sarana simulasi dalam kondisi terkendali. Pendekatan semacam ini telah diakui secara luas dalam komunitas ilmiah sebagai metode yang sah dan etis untuk menguji sistem atau aplikasi yang sensitif, khususnya ketika akses terhadap data aktual dapat menimbulkan risiko privasi atau pelanggaran hukum.

Dalam skenario ini, pelaku menggunakan ponsel pintar sebagai alat transaksi. Pelaku berhasil ditangkap, dan ponsel pintar Android miliknya diamankan sebagai barang bukti untuk proses investigasi dan pengadilan. Skenario diilustrasikan seperti Gambar 2.

Gambar 2. Skenario Kasus

Skenario ini menggambarkan kejadian di mana korban membeli barang sesuatu melalui aplikasi *e–commerce*. Namun, setelah menerima barang tersebut, korban menyadari bahwa barang yang diterima tidak sesuai dengan apa yang dibeli di aplikasi. Korban kemudian menghubungi pihak pelaku, tetapi tidak mendapat respon dan akun korban diblokir oleh pelaku. Korban melaporkan insiden tersebut kepada pihak kepolisian. Dalam investigasi awal, diketahui bahwa pelaku telah menghapus pesan dari korban yang berisi 12 pesan teks, 5 foto, dan 2 video untuk menghilangkan barang bukti. Sebagai langkah lanjutan, polisi mengamankan sebuah ponsel Vivo 1904 yang digunakan pelaku dan melakukan analisis forensik digital. Laporan hasil investigasi kemudian disusun sebagai dokumen resmi yang nantinya akan digunakan dalam proses pembuktian di pengadilan.

Forensik digital, seperti tergambar dalam skema tersebut, berperan penting dalam mendukung penegakan hukum karena memungkinkan aparat mengakses dan menganalisis bukti digital secara sistematis. Namun, proses ini juga dihadapkan pada tantangan dalam mengotentikasi dan memastikan integritas bukti digital yang akan diajukan di persidangan. Keakuratan hasil investigasi sangat bergantung pada prosedur teknis yang diterapkan serta alat bantu yang digunakan, sehingga penting bagi institusi penegak hukum untuk mengadopsi teknologi yang andal dan pendekatan yang sesuai dengan standar hukum yang berlaku agar bukti digital dapat diterima secara sah di pengadilan (Agarwal et al., 2024).

3.2. Analisis *Association of Chief Police Officers*

Penelitian ini berfokus pada variabel-variabel seperti media, pesan teks, ID pengguna, dan dokumen. Variabel-variabel ini dianalisis untuk mengungkap bukti digital terkait kasus penipuan *e-commerce* dengan menggunakan MOBILedit Forensic dan Oxygen Forensic. Gambar 3 menggambarkan tahapan kerangka kerja ACPO (Prasongko, Yudhana and Riadi, 2022).

Gambar 3. Tahapan ACPO

Tahapan ACPO sebagai berikut:

1. ***Plan***: Fase perencanaan mencakup penyusunan rencana investigasi, penentuan tindakan yang akan diambil, alat dan perangkat lunak yang digunakan, serta memastikan bahwa proses investigasi mengikuti prosedur forensik digital seluler.
2. ***Capture***: Pada tahap ini, bukti data didokumentasikan, disimpan, dan dikumpulkan. Ekstraksi data dari perangkat seluler dilakukan dengan aman dan cepat, didukung oleh alat ekstraksi khusus, baik perangkat lunak maupun perangkat keras yang tersedia.
3. ***Analyze***: Proses ini melibatkan pengumpulan data secara menyeluruh dengan metode yang sah secara teknis untuk memperoleh informasi yang relevan dan menjawab pertanyaan yang mendorong pengumpulan serta penyelidikan data. Data yang terkumpul kemudian dianalisis dan dibandingkan untuk mendapatkan hasil yang valid.
4. ***Present***: Tahap terakhir menyajikan data yang telah dianalisis beserta rekomendasi untuk tindakan selanjutnya.

4. HASIL DAN PEMBAHASAN

Penelitian ini berhasil mendapatkan bukti digital melalui proses ekstraksi dan analisis data pada aplikasi *e–commerce*. Hasil penelitian akan dipaparkan berdasarkan skema ACPO.

4.1. *Plan*

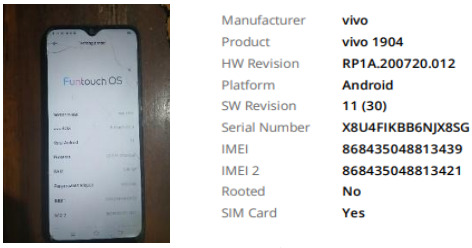
Tahap ini menjelaskan secara rinci langkah-langkah penelitian meliputi perancangan skenario penelitian serta persiapan alat dan materi yang diperlukan. Selanjutnya, tahap investigasi difokuskan pada pencarian dan pengumpulan bukti digital yang relevan, berdasarkan variabel yang telah ditentukan, seperti pesan teks, video, foto, dan dokumen untuk mendukung tujuan penelitian atau penyelidikan. Data yang didapatkan sebagai barang bukti di ponsel korban terdapat di Tabel 2.

Tabel 2. Data Barang Bukti di Ponsel Korban

No	Kategori Data	Total Data
1	Teks Pesan	12
2	Video	2
3	Gambar	5

Tabel 2 menampilkan parameter penelitian yang harus ditemukan di ponsel pintar milik pelaku. Parameter tersebut berfungsi sebagai sumber utama dalam proses analisis untuk mendukung investigasi dan pengumpulan bukti digital. Setiap parameter memuat informasi penting seperti komunikasi berbasis teks, rekaman video, serta gambar yang berpotensi menjadi bukti pendukung. Peneliti mengandalkan parameter ini untuk menelusuri jejak digital yang relevan dengan kasus yang ditangani. Data yang ditemukan kemudian dianalisis menggunakan perangkat lunak forensik sesuai dengan kebutuhan investigasi. Keberadaan data yang sesuai sangat menentukan arah dan hasil dari proses penyelidikan. Spesifikasi perangkat pelaku yang

menjadi sumber data digital ditunjukkan secara rinci pada Gambar 4.

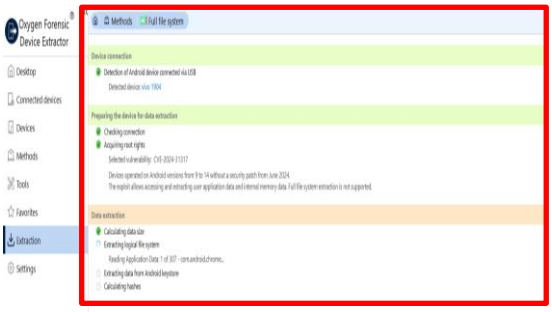


Gambar 4. Spesifikasi Perangkat

Gambar 4 memperlihatkan perangkat Android yang digunakan pelaku sebagai bukti fisik dalam kasus penipuan *e-commerce*. Perangkat ponsel ini berada dalam kondisi *non-root*, yang berarti sistem operasinya tidak mengalami modifikasi. Langkah ini diambil untuk memastikan keaslian, integritas, dan kredibilitas bukti selama proses investigasi sesuai dengan prosedur ACPO sendiri.

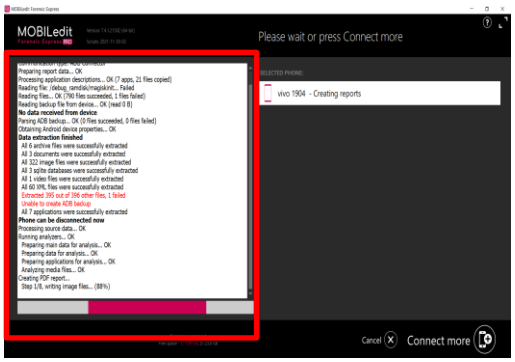
4.2. *Capture*

Tahap pengambilan data mencakup proses pengumpulan dan pencatatan informasi digital yang di dapatkan dari proses akuisisi. Tahap ini mengumpulkan dan mengklasifikasikan data temuan sesuai kategorinya masing-masing. Umumnya, data ini diperoleh melalui proses *capture*, yang dalam hal ini dapat dilakukan menggunakan alat seperti Oxygen Forensic Detective dan MOBILedit Forensic Express. Proses akuisisi menggunakan Oxygen Forensic Detective ditunjukkan pada Gambar 5.



Gambar 5. Proses Akuisisi Oxygen Forensic

Gambar 5 menunjukkan proses akuisisi data digital menggunakan perangkat lunak Oxygen Forensic yang dilakukan melalui metode *full file system*. Metode ini memungkinkan pengambilan seluruh data yang tersimpan di dalam perangkat, termasuk data tersembunyi atau yang telah dihapus. Proses akuisisi ini membutuhkan waktu selama 1 jam 36 menit 57 detik, yang mencerminkan kompleksitas dan volume data pada perangkat yang dianalisis. Hasil dari proses ini memberikan gambaran menyeluruh terkait aktivitas digital pelaku yang terekam di dalam perangkat. Sebagai pembanding, peneliti juga melakukan proses akuisisi menggunakan perangkat lunak forensik lainnya untuk memastikan validitas dan konsistensi hasil data. Proses akuisisi menggunakan MOBILedit Forensic Express ditunjukkan secara visual pada Gambar 6.



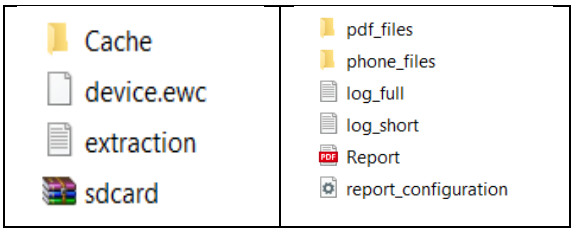
Gambar 6. Proses Akuisisi MOBILedit Forensic Express

Gambar 6 menujukkan proses akuisisi menggunakan MOBILedit Forensic melalui proses *physical imaging*. Proses akuisisi menggunakan MOBILedit Forensic Express membutuhkan waktu 45 menit 8 detik. Proses akuisisi dari Oxygen Forensic Detective dan MOBILedit Forensic Express menghasilkan data akuisisi berbentuk *directory imaging* yang kemudian diverifikasi menggunakan kode hash. Kode hash berfungsi memastikan bahwa file bukti dari perangkat Android tetap autentik dan dapat dipertanggungjawabkan sebagai barang bukti dalam persidangan. Kode hash yang dihasilkan terdapat pada Tabel 3.

Tabel 3. Kode Hash *Directory Imaging*

Nama File	MD5
AROOT 2025-02-01 18-01-40	dafad907182d37f9719fea065ead e577
vivo 1904 (2025-02-01 20h45m08s)	a578d96ec8a41f8d52bf347ecec1 f3c2

Directory imaging yang telah diketahui kode hash kemudian diekstrak dan dianalisis lebih lanjut oleh *tools* untuk mendapatkan informasi yang relevan. Hasil ekstraksi menggunakan kedua *tools* ditunjukkan pada Gambar 7.



Gambar 7. Hasil Ekstraksi

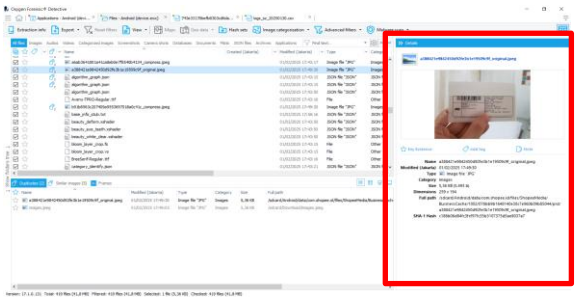
Gambar 7 memperlihatkan perbandingan hasil ekstraksi data dari perangkat seluler yang dilakukan oleh dua perangkat lunak forensik, yakni Oxygen Forensic Detective dan MOBILedit Forensic Express. Peneliti menggunakan Oxygen Forensic untuk melakukan ekstraksi data yang kemudian menghasilkan beberapa folder utama seperti folder *Cache* dan *file* seperti *device.ewc*, *extraction*, dan *sdcard*. Folder-folder tersebut menyimpan berbagai

jenis informasi, termasuk data *cache* aplikasi, hasil *parsing* perangkat, *file* sistem, serta data dari kartu *SD*. Di sisi lain, penggunaan MOBILedit Forensic menghasilkan struktur direktori yang berbeda. *Tools* ini menghasilkan folder seperti *pdf_files*, *phone_files* dan *file* seperti *log_full*, *log_short*, *Report*, dan *report_configuration*. Setiap folder menyimpan jenis data tertentu, seperti dokumen dalam format PDF, *file* perangkat, catatan aktivitas, serta laporan dan konfigurasi ekstraksi. Hal ini menggarisbawahi pentingnya pemilihan dan kombinasi alat forensik yang tepat guna memaksimalkan keberhasilan pengumpulan bukti digital dalam berbagai kondisi kasus.

Perbedaan hasil ekstraksi dari kedua *tools* tersebut menunjukkan bahwa setiap perangkat lunak memiliki metode pengelompokan data yang khas. Meskipun begitu, keduanya tetap berhasil mengambil informasi digital penting yang nantinya akan dianalisis lebih dalam pada tahap selanjutnya untuk mendukung proses investigasi forensik digital.

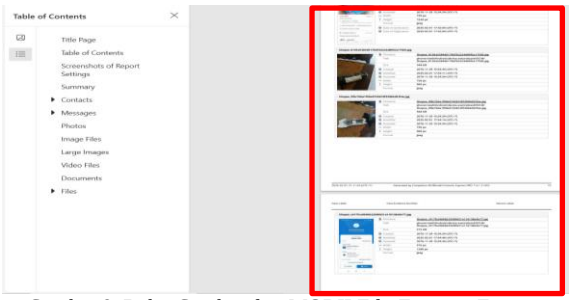
4.3. *Analyze*

Tahap ini merupakan proses analisis terhadap hasil ekstraksi file yang diperoleh menggunakan Oxygen Forensic Detective dan MOBILedit Forensic Express. Analisis dilakukan untuk mengidentifikasi informasi penting dari data yang telah diekstrak. Masing-masing alat menunjukkan hasil analisis yang sama yaitu data yang telah terhapus dari ponsel pintar masih dapat dipulihkan, sehingga dapat digunakan informasi tambahan dalam penyelidikan kasus kejahatan *e-commerce*. Bukti gambar yang dipulihkan oleh Oxygen Forensic Detective terdapat pada Gambar 8.



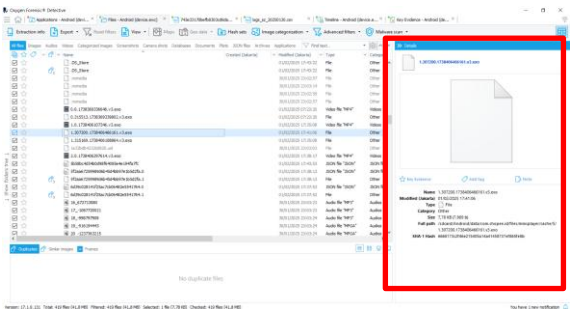
Gambar 8. Bukti Gambar dari Oxygen Forensic Detective

Gambar 8 menunjukkan informasi detail dari sebuah gambar yang telah dianalisis menggunakan perangkat lunak forensik. Informasi yang ditampilkan mencakup nama *file*, ukuran *file*, tanggal pembuatan, serta berbagai metadata lainnya yang relevan dengan proses investigasi digital. Metadata tersebut berfungsi sebagai bukti penting untuk menelusuri asal-usul *file*, waktu akses, dan potensi manipulasi data. Dengan data ini, peneliti dapat memastikan keaslian *file* serta mengidentifikasi hubungan antara gambar dan aktivitas digital lainnya. Selain itu, proses pemulihan *file* gambar yang sebelumnya terhapus atau tersembunyi juga menjadi bagian dari tahap penting dalam pengumpulan bukti. Bukti gambar yang berhasil dipulihkan menggunakan MOBILedit Forensic Express ditunjukkan secara visual pada Gambar 9.



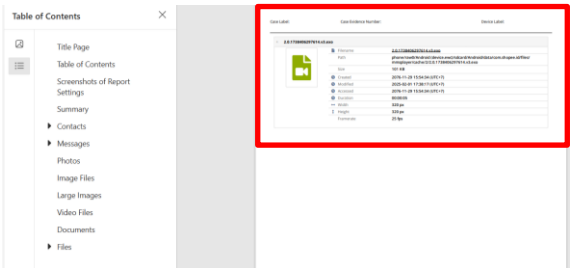
Gambar 9. Bukti Gambar dari MOBILEdit Forensic Express

Gambar 9 menampilkan hasil bukti digital dalam bentuk gambar dari ponsel pintar pelaku yang diperoleh menggunakan *tools* MOBILEdit Forensic Express. Pada gambar tersebut, terdapat informasi detail seperti nama *file*, ukuran, tanggal pembuatan, serta metadata lain yang relevan. Bukti video yang dipulihkan oleh Oxygen Forensic Detective terdapat pada Gambar 10.



Gambar 10. Bukti Video dari Oxygen Forensic Detective

Gambar 10 menampilkan hasil ekstraksi *file* video dari perangkat seluler, disertai metadata yang mencakup nama *file*, tanggal pembuatan, ukuran *file*, serta lokasi penyimpanannya. Bukti video yang dipulihkan oleh MOBILedit Forensic Express terdapat pada Gambar 11.



Gambar 11. Bukti Video dari MOBILEdit Forensic Express

Gambar 11 menampilkan bukti video pada *tools* MOBILEdit Forensic Express, yang menunjukkan *file* video hasil ekstraksi dari perangkat penyimpanan, lengkap dengan metadata seperti nama *file*, ukuran, dan tanggal pembuatan. Berdasarkan gambar tersebut, kedua *tools* berhasil memulihkan data yang

terhapus, termasuk pesan dalam bentuk gambar dan video. Namun data berupa pesan teks yang telah terhapus dari perangkat bukti tidak dapat dipulihkan oleh kedua *tools*.

4.4. *Present*

Pada tahap penelitian ini telah ditemukan bukti gambar pada ponsel pintar pelaku, tetapi gambar tersebut mengalami perubahan ukuran dari gambar asli. Perubahan terjadi karena fitur pada aplikasi *e-commerce* melakukan kompresi data secara otomatis. Bukti video juga ditemukan pada ponsel pintar pelaku, yang mana video tersebut juga mengalami kompresi kualitas dan ukuran. Namun, bukti pesan teks tidak berhasil ditemukan karena kedua *tools* tidak dapat mengakses sistem ponsel pelaku secara menyeluruh. Hal ini karena ponsel pelaku belum melakukan proses *rooting*. Proses rooting dapat mengakses seluruh aspek ponsel lebih mendalam termasuk mengembalikan pesan teks yang telah terhapus (Yalçın and Yıldırım, 2024). Proses *rooting* sengaja tidak dilakukan sebagai upaya menjaga prinsip metode ACPO yang memperhatikan aspek legalitas dan prosedur hukum.

Pada tahap ini, ditampilkan bukti digital yang berhasil diperoleh menggunakan perangkat lunak Oxygen Forensic Detective dan MOBILedit Forensic Express. Hasil analisis berupa data digital, seperti pesan teks dan file media, dirangkum dalam Tabel 4. Tabel tersebut juga menyajikan perbandingan efektivitas kedua *tools* berdasarkan persentase keberhasilan dalam proses pengumpulan data, yang dihitung menggunakan Persamaan 1. (Hidayah and Fachri, 2025):

$$P_{ar} = \frac{\sum \ Vfound}{\sum \ Vtotal} \times 100 \quad (1)$$

Catatan:
P_{ar}= Nilai indeks keakuratan alat forensik.
$Vtotal$ = Total jumlah variabel yang digunakan.
$Vfound$= Total variabel yang berhasil diperoleh.

Tabel 4. Hasil Analisis *Tools* Forensik

Jenis Data	Jumlah	Oxygen Forensic Detective	MOBILedit Forensic Express
Pesan Teks	12	0	0
Pesan Video	2	2	1
Pesan Gambar	5	5	4
Total	19	7	5
Presentase	100%	37%	26%

Berdasarkan Tabel 4, hasil analisis bukti digital menunjukkan adanya perbedaan kinerja antara *tools* forensik Oxygen Forensic Detective 37% dan MOBILEdit Forensic Express 26%. Perbedaan tingkat keberhasilan kedua alat ini tergolong kecil dan kemungkinan tidak signifikan secara statistik. Dari total 12 teks yang dikirim, kedua *tools* belum mampu mengidentifikasi pesan teks yang telah dihapus. Kedua *tools* tersebut juga dapat mendeteksi video, di mana Oxygen Forensic berhasil menemukan 2 dari 2 video yang telah dihapus, sementara MOBILEdit Forensic berhasil menemukan 1 dari 2 video yang telah dihapus. Dalam kategori file gambar, terdapat total 5 artefak, dengan seluruh gambar telah dihapus dari pesan. Oxygen Forensic berhasil menemukan 5 gambar, tanpa berhasil memulihkan file yang dihapus dalam obrolan, sementara MOBILEdit Forensic mengidentifikasi 4 file gambar dari 5 gambar yang telah dihapus. Kedua *tools* belum mampu memulihkan 100% data karena perangkat yang digunakan tidak dalam kondisi *rooted* atau memiliki akses penuh, sehingga menyebabkan keterbatasan dalam proses ekstraksi data. Perangkat tidak di-*root* untuk menjaga keaslian dan integritas bukti serta menghindari risiko kerusakan atau perubahan data yang dapat mempengaruhi validitas hasil forensik dalam konteks hukum.

Hasil ini berbeda dengan studi sebelumnya, seperti Mualfah, Syam, dan Baidarus (2023) yang menemukan Oxygen Forensic Detective mampu memulihkan 83,33% bukti digital pada aplikasi *Signal Messenger*, serta Setyawan (2023) yang melaporkan tingkat keberhasilan Oxygen Forensic Suite mencapai 98% pada analisis data *Skype*. Perbedaan ini kemungkinan disebabkan oleh jenis aplikasi, kondisi perangkat, serta metode pengujian yang digunakan. Penelitian ini juga sejalan dengan Riadi, Yudhana, dan Fanani (2023) yang menunjukkan Oxygen Forensic memiliki performa unggul dalam pemulihan data digital meskipun dengan keterbatasan akses pada perangkat yang tidak di-*root*. Sebagai saran, penelitian selanjutnya dapat menggunakan metode lain dan perangkat yang di-*root* secara legal untuk keperluan akademik dan penelitian lebih lanjut, guna memperluas akses data dan mendalami analisis. Temuan ini juga menguatkan hasil sebelumnya bahwa Oxygen Forensic Detective menunjukkan performa lebih baik dibanding MOBILEdit Forensic Express, khususnya dalam pemulihan data digital pada aplikasi *e-commerce*.

5. KESIMPULAN

Penelitian ini mengevaluasi efektivitas Oxygen Forensic Detective dan MOBILedit Forensic Express dalam memulihkan bukti digital terhapus dari aplikasi *e-commerce* menggunakan kerangka kerja ACPO. Oxygen Forensic berhasil memulihkan 37% data, sedangkan MOBILedit hanya mencapai 26%. Pemulihan pesan teks tidak berhasil dilakukan karena tersimpan di direktori sistem yang membutuhkan proses *rooting*, yang tidak dilakukan agar keaslian perangkat tetap terjaga. Proses autentikasi menggunakan *hash* tidak dapat diterapkan karena aplikasi Shopee mengompresi file secara otomatis saat unggah, sehingga nilai *hash* berubah. Kondisi ini menunjukkan bahwa keterbatasan akses teknis dan perubahan *hash* dapat mempersulit pembuktian di pengadilan. Oleh karena itu, penelitian lanjutan disarankan menggunakan metode DFRWS, prosedur *rooting* yang sah, *tool* forensik dengan akses sistem

mendalam, serta memperkuat *chain of custody* guna menjaga integritas bukti.

DAFTAR PUSTAKA

Agarwal, G., Bhatt, R., Pathak, P., Kumar, A., Kumar, A. and Pandey, S., 2024. Digital Forensics and the Law: A Computer Engineering Perspective. pp.1–6. https://doi.org/10.1109/icccnt61001.2024.10725628.

Aisyah, N., Putra, A.S., Safrizal, S., Valentino, V. H., Zikriah, Z., Prasetyo, B.S., and Nurhayati, N., 2022. Analisa Perkembangan Digital Forensik Dalam Penyidikan Cybercrime Di Indonesia Secara Systematic Review. *Jurnal Esensi Infokom : Jurnal Esensi Sistem Informasi Dan Sistem Komputer*, [e-journal] 6(1), pp.22–27. https://doi.org/10.55886/infokom.v6i1.452.

Alblooshi, A., Aljneibi, N., Iqbal, F., Ikuesan, R., Badra, M. and Khalid, Z., 2024. Smartphone Forensics: A Comparative Study of Common Mobile Phone Models. pp.1–6. https://doi.org/10.1109/isdfs60797.2024.10527262.

Alshammari, A., 2023. Detection and Investigation Model for the Hard Disk Drive Attacks using FTK Imager. *International Journal of Advanced Computer Science and Applications*, [e-journal] 14(7), pp.767–774. https://doi.org/10.14569/IJACSA.2023.0140784.

Aziz, M.A., Sulistyo, W.Y., Astari, R., 2021. *Komparatif Anti Forensik Aplikasi Instant Messaging Berbasis Web Menggunakan Metode Association of Chief Police Officers (ACPO)*. [online] Available at: https://doi.org/10.53863/juristik.v1i01.341.

CIOMS, 2021. *International ethical guidelines for health-related research involving humans*. Geneva: Council for International Organizations of Medical Sciences. Available at: https://cioms.ch/publications/product/international-ethical-guidelines/ [Accessed 29 May 2025].

Dahlan, K.A., Yudhana, A., and Yuliansyah, H., 2024. File carving Analyze of Foremost and Autopsy on external SSD mSATA using the Association of Chief Police Officer Method. *ILKOM Jurnal Ilmiah*, [e-journal] 16(3), pp.283–295. https://doi.org/10.33096/ilkom.v16i3.2360.283-295.

Fema, C.A., Rakhmad, N., Bonda, P.Y.E., Ramli, D., and Maulana, A., 2022. Studi Komparasi Tingkat Konsumsi Masyarakat Melalui E-Commerce Sebelum dan Sesudah Masa Pandemi COVID-19. *Jurnal Kajian Ilmiah*, 22(1), [e-journal] pp.53–66. https://doi.org/10.31599/jki.v22i1.951.

Hardjono, B., Widjaja, A.E., Rhizma, M.G.A., Tjahyadi, H., Haryani, C.A., Renatan, W., 2020. *Komunikasi Nirkabel: dengan Aplikasinya di Bidang Telekomunikasi dan Informatika*. Yogyakarta: Penerbit ANDI.

Hidayah, A., and Fachri, F., 2025. Analisis Bukti Digital Terhadap Kasus Prostitusi Online Pada Aplikasi Michat Menggunakan Metode ACPO. *Jurnal Mahasiswa Teknik Informatika*, 9(1), pp.906–912. https://doi.org/10.36040/jati.v9i1.12441

Iman, N., Susanto, A., and Inggi, R., 2020. Analisa Perkembangan Digital Forensik dalam Penyelidikan Cybercrime di Indonesia (Systematic Review). *Jurnal Telekomunikasi Dan Komputer*, [e-journal] 9(3), pp.186. https://doi.org/10.22441/incomtech.v9i3.7210.

Kementerian Perdagangan RI. 2024. *Perdagangan Digital (E-Commerce) Indonesia Periode 2023*. Jakarta: Kementerian Perdagangan RI.

Lestari, Y.D., Lubis, Y.F.A., and Siregar, F.A., 2023. Analisis Perbandingan Kinerja Root Explorer Dan Oxygen Forensic Detective Pada Forensic Digital. *Jurnal Syntax Fusion*, [e-journal] 3(08), pp.832–846. https://doi.org/10.54543/fusion.v3i08.350.

Maniar, N.A.I., and Yuniati, T., 2023. Implementasi Mobile Forensic Pada Aplikasi Michat Dan Telegram Dengan Framework Nist 800-101. *Cyber Security Dan Forensik Digital*, [e-journal] *5*(2), pp.60–65. https://doi.org/10.14421/csecurity.2022.5.2.3764.

Maxsutbekova, N., 2023. Mobile Device Forensics. Elsevier eBooks. pp.613–623. https://doi.org/10.1016/b978-0-12-823677-2.00240-3.

Mualfah, D., Muhammad Iqbal Syam and Baidarus, 2023. Analisis perbandingan tools mobile forensic menggunakan metode national institute of justice (NIJ). *Jurnal CoSciTech (Computer Science and Information Technology)*, 4(1), pp.283–292. https://doi.org/10.37859/coscitech.v4i1.4767.

Pengadilan Negeri Surabaya, 2025. Sistem Informasi Penelusuran Perkara. [online] Available at: https://sipp.pn-surabayakota.go.id/list_perkara [Accessed 21 May 2025].

Permana, L.A., Hakim, F., Subhi, Y.A., and Rivaldo, P., 2023. Analisis Forensik Keaslian Gambar Menggunakan Autopsy. *Jurnal*

JOCOTIS-Journal Science Informatica and Robotics E, 1(2), pp.39–45. Available from: https://jurnal.ittc.web.id/index.php/jct/article/view/435

Prasongko, R.Y., Yudhana, A., and Riadi, I., 2022. Analisis Penggunaan Metode ACPO (Association of Chief Police Officer) pada Forensik WhatsApp. *Jurnal Sains Komputer & Informatika*, 6(2), pp.1112–1120. http://dx.doi.org/10.30645/jsakti.v6i2.520

Ramadhan, R.A., Zaini A.K., and Mardafora, J., 2022. Pelatihan Investigasi Digital Forensik. *Jurnal Pengabdian Masyarakat Dan Penerapan Ilmu Pengetahuan*, [e-journal] 3(2), pp.1–6. https://doi.org/10.25299/jpmpip.2022.11003.

Riadi, I. and Yudhana, A., 2023. Mobile Forensic Tools for Digital Crime Investigation: Comparison and Evaluation. *International Journal of Safety and Security Engineering*, 13(1), pp.11–19. https://doi.org/10.18280/ijsse.130102.

Riadi, I., Yudhana, A. and Fanani, G. P. I., 2023. Comparative Analysis of Forensic Software on Android-based MiChat using ACPO and DFRWS Framework. *Jurnal RESTI (Rekayasa Sistem dan Teknologi Informasi)*, 7(2), pp.286–292. https://doi.org/10.29207/resti.v7i2.4547.

Safitri, Y., Riadi, I., and Sunardi, S., 2023. Mobile Forensic for Body Shaming Investigation Using Association of Chief Police Officers Framework. *MATRIK : Jurnal Manajemen, Teknik Informatika Dan Rekayasa Komputer*, [e-journal] 22(3), pp.651–664. https://doi.org/10.30812/matrik.v22i3.2987.

Setiawan, D. and Riadi, I., 2024. *Mobile Forensic WhatsApp Services in Online Fraud Cases using Digital Forensic Research Workshop Methods General Terms*. *International Journal of Computer Applications*, 186(34), 49-56. DOI: 10.5120/ijca2024923908

Setyawan, M.R., 2023. *Perbandingan Tools Forensik Dalam Analisis Bukti Digital Pada Aplikasi Skype Menggunakan Framework NIST*. [online] Available at: https://doi.org/10.51544/jurnalmi.v8i2.4580

Subektiningsih, S., 2020. Pendekatan Model Bisnis Untuk Pemetaan Triage Forensics. *Explore*, [e-journal] *10*(2), pp.27. https://doi.org/10.35200/explore.v10i2.351.

Sutikno, T., 2024. Mobile forensics tools and techniques for digital crime investigation: a comprehensive review. *International Journal of Informatics and Communication Technology*, 13(2), p.321. https://doi.org/10.11591/ijict.v13i2.pp321-332.

Tuharea, I.R., Luthfi, A. and Ramadani, E., 2023. Enhancing Digital Forensic Investigation: A Focus on Compact Electronic Devices and Social Media Metadata. *Journal of Information Systems and Informatics*. https://doi.org/10.51519/journalisi.v5i4.594

Yalçın, N. and Yıldırım, T., 2024. Logical Image Acquisition and Analysis of Android Smartphones. *Journal of Computer and Communications*, 12(04), pp.139–152.https://doi.org/10.4236/jcc.2024.124011

Yudhana, A., Riadi, I., Yudhi Prasongko, R., Dahlan, A., Ahmad Yani Tamanan, J. and Soepomo, J., 2022. Forensik WhatsApp Menggunakan Metode Digital Forensic Research Workshop (DFRWS).7(1). Available at: 10.30591/jpit.v7i1.3639

Zakarneh, S.K., 2024. Mobile Forensic Investigation on iOS & Android Smartphones: Case Study Investigation on WhatsApp. *International Journal of Applied Sciences and Smart Technologies*, 6(1), pp.63–98. https://doi.org/10.24071/ijasst.v6i1.6770.