Jurnal Teknik Informatika (JUTIF)
P-ISSN: 2723-3863
E-ISSN: 2723-3871
Vol. 6, No. 4, August 2025, Page. 2707-2722
https://jutif.if.unsoed.ac.id
DOI: https://doi.org/10.52436/1.jutif.2025.6.4.4999

Efficient Evidence Reduction Technique for Mobile Forensics based on Digital Evidence Object (DEO) Model

Arif Rahman Hakim*[1], Lisa Saputri[2]

[1]Rekayasa Keamanan Siber, Politeknik Siber dan Sandi Negara, Indonesia
[2]Badan Siber dan Sandi Negara, Indonesia

Email: [1]arif.hakim@poltekssn.ac.id

Received : Jun 30, 2025; Revised : July 31, 2025; Accepted : July 31, 2025; Published : Aug 25, 2025

Abstract

The Android operating system (OS) is currently the most widely used platform on smartphones, making it a critical source of digital evidence in cybercrime investigations. With its vast array of applications and features, Android OS generates and stores a significant amount of data, much of which may be relevant to criminal activities. Mobile forensics plays a crucial role in identifying and analyzing this information to produce scientifically valid evidence. However, the process of acquiring and examining data from a smartphone's internal storage typically results in large and complex datasets that can hinder timely forensic analysis. To address this challenge, this paper proposes the implementation of the DEO Model using Python to reduce the volume of digital evidence obtained from Android-based smartphones. The DEO Model employs a structured filtering approach, narrowing the dataset to only those objects relevant to a predefined scenario. This is achieved by applying DEO parameters based on the 5W category theory (Why, When, Where, What, Who), resulting in an optimal and focused dataset. The findings demonstrate that the Python-based DEO Model significantly accelerates the mobile forensic process, and effectively reduces dataset size while both maintaining the evidence integrity and the scenario relevance. The model achieves a very low False Positive Rate (FPR) of 0,00072, indicating a minimal risk of mismatches during the object reduction process. Therefore, the findings confirm the validity and accuracy of the digital evidence obtained. This research highlights the potential of the Python-based DEO Model to enhance the efficiency of forensic investigations on Android smartphones.

Keywords : *Android, DEO Model, Digital Evidence, Digital Investigation, Mobile Forensics.*

1. INTRODUCTION

Saat ini, Android *Operating System* (OS) merupakan sistem operasi yang paling banyak digunakan pada smartphone, sehingga ketika pengguna Android OS meningkat potensi kemungkinan bukti kejahatan dan aktivitas sehari-hari yang disimpan di dalam Android OS juga semakin meningkat [1], [2]. Dengan menggunakan akses internet, pengguna dapat dengan mudah mengirim atau mengakses informasi apapun pada perangkat pengguna lainnya dalam satu waktu untuk tujuan berbagi data atau melakukan aktivitas ilegal. Bahkan sebelum Android OS menjadi sistem operasi yang paling banyak digunakan, sistem operasi ini telah dianggap sebagai sumber informasi yang paling penting karena merupakan gudang informasi yang besar [3]. Hal tersebut disebabkan banyaknya aktivitas dari aplikasi dan fitur *smartphone* berbasis Android OS yang menghasilkan data dan menyimpan informasi dalam jumlah besar pada penyimpanan internal *smartphone* [4], [5].

Forensik digital merupakan bidang sains untuk mengumpulkan, menganalisis, dan menyajikan bukti legal yang ditemukan dari perangkat digital [6]. Salah satu pengembangan dari forensik digital adalah *mobile forensic* . *Mobile forensic* merupakan cabang dari forensik digital yang berhubungan dengan pemulihan bukti digital dari perangkat mobile [7], salah satunya adalah *smartphone*. Bukti vital

mengenai suatu aktivitas di dalam perangkat digital sebagian besar terdapat pada penyimpanan perangkat digital tersebut [8], sementara data lainnya akan tetap tersimpan di penyimpanan bahkan setelah data tersebut dihapus [9]. Untuk mengidentifikasi dan mengetahui aktivitas yang ada pada *smartphone*, analisis forensik memiliki peran penting dalam proses investigasi [10], sehingga *mobile forensic* perlu dilakukan untuk menemukan dan menguji data yang tersimpan di dalam penyimpanan internal *smartphone*. Dalam menemukan bukti digital pada perangkat *mobile*, diperlukan sebuah panduan untuk membantu analis forensik dalam melakukan proses investigasi. NIST SP 800-101 revisi 1 merupakan panduan yang ditujukan untuk mengatasi situasi umum yang mungkin terjadi melibatkan data elektronik digital yang ada pada perangkat *mobile* dan media elektronik di dalamnya [11]. NIST SP 800-101 revisi 1 menyajikan panduan dalam melakukan *mobile forensic* mengikuti empat fase proses forensik, yaitu *collection, examination, analysis*, dan *reporting* [12].

Dalam proses forensik digital, *dataset* yang dihasilkan dari proses ekstraksi data memiliki ukuran yang sangat besar dan struktur yang kompleks [13]. Dengan demikian, proses investigasi forensik menghabiskan banyak waktu karena memerlukan pemeriksaan terhadap semua kapasitas data digital yang tersedia dari perangkat digital [14]. Banyaknya hasil ekstraksi data menyulitkan penguji atau analis forensik untuk mengambil keputusan akhir dalam waktu yang singkat. Sebuah cara atau metode diperlukan untuk dapat membantu analis forensik dalam mereduksi jumlah *dataset* yang akan diforensik [13].

Pada penelitian yang dilakukan oleh Grigaliunas et al (2020), diusulkan sebuah Model *Digital Evidence Object* (DEO) untuk membantu proses forensik digital khususnya pada tahap *examination* dalam mengurangi jumlah data dari perangkat digital menjadi *dataset* yang lebih kecil dan memberikan hasil analisis yang akurat [13]. Reduksi data tersebut ditujukan untuk memfokuskan bukti digital yang ingin diteliti berdasarkan bukti awal yang ditemukan dari studi kasus kejahatan yang terjadi. Pada penelitian lainnya, Grigaliunas & Toldinas (2020) membuat *tool* khusus berdasarkan *Habits Attribution* dan Model DEO untuk membantu ahli forensik dalam mengurangi ukuran data yang diselidiki [14]. Model DEO tersebut didasarkan pada analisis informasi yang diekstraksi selama proses forensik menggunakan teori pengkategorian 5W (*Why, When, Where, What, Who*) dan standar tahapan pada proses forensik digital yaitu *collection, examination, analysis*, dan *reporting*. Hasilnya, Model DEO pada penelitian pertama mampu mengurangi data pada tahap reduksi data dengan menghasilkan dataset yang berukuran kecil. Pada penelitian kedua, dihasilkan sebuah *tool Digital Evidence Investigation of Cybercrime* (DEIC) yang menyediakan evaluasi terkait validitas akurasi dari hasil penelitian pertama. Pada kedua penelitian tersebut, Model DEO dibangun dengan *platform* .NET dan diterapkan pada *Hard Disk Drive* (HDD) berukuran 40 GB.

Meskipun pendekatan tersebut telah menunjukkan potensi signifikan, penggunaan platform berbasis .NET saat ini mulai tergeser oleh bahasa pemrograman Python yang lebih fleksibel dan banyak digunakan dalam analisis data digital [15]. Python menyediakan beberapa *framework* dan *libraries* yang terus berkembang seperti TensorFlow, PyTorch, Pandas, NLTK, dan lain-lain serta lingkungan yang baik dalam melakukan *Computational Science* (CS) sehingga hal tersebut menjadikan Python sebagai pilihan yang baik digunakan untuk analisis data [16] Dengan demikian, penggunaan pemrograman Python pada Model DEO untuk mereduksi data pada penyimpanan internal *smartphone* berbasis Android OS menjadi pembeda pada penelitian ini.

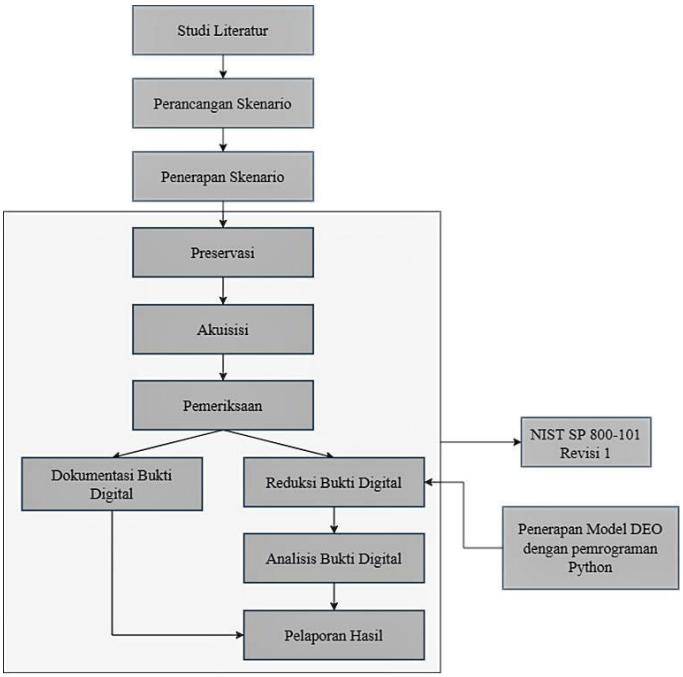
Artikel ini mengusulkan Model DEO pada *mobile forensic* sebagai tahap untuk melakukan reduksi bukti digital terhadap data yang diperoleh saat tahap akuisisi, yaitu penyimpanan internal *smartphone* berbasis Android OS. Model tersebut dijalankan menggunakan bahasa pemrograman Python. Artikel ini memberikan kontribusi berupa penerapan Model DEO pada proses *mobile forensic* terhadap hasil akuisisi penyimpanan internal *smartphone* berbasis Android OS. Selain itu, kontribusi yang diberikan yaitu studi kasus dengan skenario komunikasi nyata dan investigasi yang komprehensif

Jurnal Teknik Informatika (JUTIF)
P-ISSN: 2723-3863
E-ISSN: 2723-3871
Vol. 6, No. 4, August 2025, Page. 2707-2722
https://jutif.if.unsoed.ac.id
DOI: https://doi.org/10.52436/1.jutif.2025.6.4.4999

pada setiap langkah disertai hasil yang lengkap. Di sisi lain, penelitian ini terbatas pada analisis bukti digital pada data yang diperoleh setelah tahap reduksi bukti digital pada hasil akuisisi penyimpanan internal *smartphone* berbasis Android OS.

2. METHOD

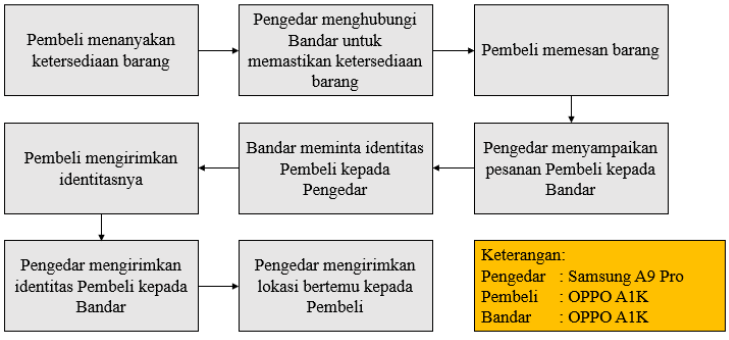
Pada artikel ini, penelitian dilakukan dengan langkah-langkah yang terdiri dari perancangan, skenario, penerapan skenario, dan investigasi forensik terhadap skenario. Investigasi forensik yang dilakukan berbasis NIST SP 800-101 Rev.1 dengan tahapan *mobile forensic* yang meliputi preservasi, akuisisi, pemeriksaan, analisis, dan pelaporan hasil. Lebih lanjut, pada tahapan pemeriksaan akan diterapkan Model DEO berbasis Python untuk mereduksi data yang diinvestigasi. Gambar 1 menunjukkan metodologi berupa langkah-langkah penelitian yang digunakan pada artikel ini.



Gambar 1. Metodologi berupa tahapan penelitian yang digunakan.

2.1. Perancangan Skenario

Perancangan skenario merupakan tahap yang krusial bagi tahapan selanjutnya. Hal tersebut dikarenakan pada tahap ini skenario yang ditentukan dan menjadi inti investigasi forensik dalam memberikan reka peristiwa dalam kasus kejahatan yang terjadi. Dalam artikel ini, skenario yang dirancang berdasarkan alur sebagaimana ditunjukkan pada Gambar 2.



Gambar 2. Skenario yang dirancang disertai alur skenario

Vol. 6, No. 4, August 2025, Page. 2707-2722
https://jutif.if.unsoed.ac.id
DOI: https://doi.org/10.52436/1.jutif.2025.6.4.4999

Dapat dilihat pada Gambar 2, terdapat rancangan skenario komunikasi antara para aktor, yang kemudian rancangan skenario tersebut diterapkan dengan pertukaran pesan SMS menggunakan perangkat yang telah ditentukan.

2.2. Penerapan Skenario

Skenario yang telah dirancang kemudian diterapkan pada tahap ini dan menjadi dasar tahapan *mobile forensic* yang dilakukan. Selain itu, penerapan skenario juga ditujukan untuk memberikan indikator perhitungan FPR dari Model DEO terhadap tindak kejahatan berdasarkan skenario yang dirancang yang tersimpan di dalam penyimpanan internal Samsung Galaxy A9 Pro. Lebih lanjut, dalam rangka mengisolasi objek penelitian, perangkat yang digunakan sebagai wadah penerapan skenario secara khusus hanya digunakan untuk penerapan skenario tidak digunakan untuk kepentingan lainnya.

2.3. Tahapan *Mobile Forensic* NIST SP 800-101 Revisi 1

NIST SP 800-101 Rev.1 merupakan standar atau panduan yang memberikan informasi dasar mengenai *mobile forensic tools* dan tahapan analisis forensik terhadap bukti digital yang ada pada perangkat mobile [11]. Pada bagian ini dijelaskan tahapan *mobile forensic* yang dilakukan pada artikel ini meliputi preservasi, akuisisi, pemeriksaan, analisis, dan pelaporan hasil.

2.3.1. Preservasi

Pada tahap preservasi, dilakukan identifikasi perangkat mobile dan pengumpulan informasi dari perangkat mobile yang diterima sebagai bukti elektronik. Tahap ini bertujuan untuk mengetahui tindakan awal yang dilakukan terhadap bukti elektronik yang diterima. Pada tahap ini didokumentasikan kondisi awal dari bukti elektronik yang diterima, isolasi perangkat terhadap jaringan komunikasi untuk menghindari komunikasi yang mungkin terjadi terhadap bukti elektronik dan mencegah adanya perubahan data di dalam perangkat, dan penyimpanan bukti elektronik.

Dalam skenario artikel ini, perangkat yang dipreservasi yaitu perangkat Pengedar, kondisi perangkat menyala dengan daya 75%, sehingga teknik yang dilakukan pada tahapan akuisisi adalah *live acquisition.* Gambar 3 menunjukkan perangkat yang dilakukan preservasi milik aktor Pengedar, terdiri dari (a) Tampak Depan Perangkat, (b) Tampak Belakang Perangkat, (c) Kondisi Daya Perangkat, dan (d) Isolasi Perangkat dari Jaringan Komunikasi.

(a) (b) (c) (d)

Gambar 3. Preservasi perangkat milik aktor Pengedar

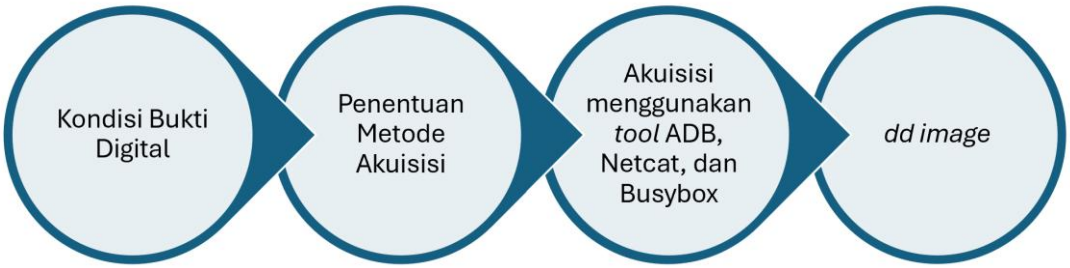
Terlihat pada Gambar 3(c) kondisi daya daya perangkat Samsung Galaxy A9 Pro adalah 75%, sehingga dengan daya sebesar 75% cukup untuk dilakukan akuisisi secara *live* atau kondisi perangkat dalam keadaan menyala. Selanjutnya Gambar 3(d) menunjukkan isolasi perangkat terhadap jaringan yang dilakukan dengan mengaktifkan mode pesawat dan menonaktifkan fitur *Global Positioning System*

Vol. 6, No. 4, August 2025, Page. 2707-2722
https://jutif.if.unsoed.ac.id
DOI: https://doi.org/10.52436/1.jutif.2025.6.4.4999

(GPS). Menonaktifan fitur GPS membantu dalam mempertahankan kondisi daya perangkat sehingga fitur tersebut tidak berjalan di sistem sedangkan mengaktifkan mode pesawat membantu mencegah terjadinya pertukaran sinyal. Untuk selanjutnya, perangkat Samsung Galaxy A9 Pro milik pengedar ini disebut sebagai Bukti Digital 1 (BD1).

2.3.2. Akuisisi

Tahap akuisisi dilakukan berdasarkan hasil identifikasi pada tahap preservasi. Pada tahap ini juga ditentukan tahap akuisisi yang dilakukan adalah *physical acquisition* untuk mendapatkan seluruh informasi yang dibutuhkan [17]. Akuisisi dilakukan terhadap seluruh penyimpanan internal BD1. Teknik akuisisi yang dilakukan adalah *live acquisition* [17], sehingga selama akuisisi berlangsung *smartphone* harus dalam keadaan hidup atau aktif terutama agar dapat memberikan izin akses kepada laptop forensik. Berdasarkan skenario yang telah dirancang, proses akuisisi dilakukan pada penyimpanan internal BD1 menggunakan *tool* ADB [18], Netcat dan BusyBox. Format file yang dihasilkan adalah data dump image (*dd image*). Alur tahapan akuisisi dapat dilihat pada Gambar 4.



Gambar 4. Tahapan akuisisi penyimpanan internal perangkat milik Pengedar

Lebih lanjut, Tabel 1 menunjukkan tahapan perintah dari masing-masing *tool* yang digunakan saat proses akuisisi. Setelah file *dd image* diperoleh, perlu dipastikan bahwa selama proses akuisisi *disk image* yang dihasilkan terjaga integritasnya. Proses memastikan tidak terjadi perubahan pada data *image* dilakukan dengan verifikasi nilai *hash* [19].

Tabel 1. Tools dan Perintah pada Tahapan Akuisisi

Shell	Tool	Perintah
adb	adb	adb -d shell su cat proc/partitions
cmd	adb	adb forward tcp:8888 tcp:8888
adb	busybox	dd if=/dev/block/mmcblk0 | busybox nc -l -p 8888
cmd	netcat	nc.exe 127.0.0.1 8888 > android.dd

Pada Tabel 1 perintah “cat proc/partitions” menampilkan daftar partisi yang terdapat pada penyimpanan BD1 dimana “mmclbk0” merupakan partisi utama yang didalamnya menyimpan seluruh data yang terdapat pada BD1. Kemudian, perintah “adb forward tcp:8888 tcp:8888” dilakukan untuk *port forwarding* melalui shell CMD agar laptop yang bertindak sebagai *forensic workstation* dapat berkomunikasi dengan BD1 untuk mengirimkan data. Perintah “dd if=/dev/block/mmcblk0 | busybox nc -l -p 8888” dilakukan untuk melakukan *data dump* dari BD1 ke *forensic workstation* menggunakan perintah “if” untuk membuat *image file*, diikuti dengan *string* “=/dev/block/mmcblk0” yang merupakan partisi utama dari BD1 yang akan dibuat image file-nya. Selanjutnya, perintah “nc.exe 127.0.0.1 8888 > android.dd” digunakan dalam proses menyalin data. Proses akuisisi ini akan menghasilkan *disk image* dengan nama android.dd.

2.3.3. Pemeriksaan

Tahap pemeriksaan bertujuan untuk memeriksa objek dan struktur entitas sebagai artefak dari image yang diperoleh dari proses akuisisi. Pada artikel ini, tahap pemeriksaan dibagi menjadi dua tahapan, yaitu tahap dokumentasi bukti digital dan tahap reduksi bukti digital. Tahap dokumentasi bukti digital dilakukan untuk mendokumentasikan jumlah data yang terdapat pada *dd image* menggunakan *tool* Autopsy [20] yang kemudian menghasilkan file .csv, sedangkan tahap reduksi bukti digital dilakukan pada file .csv menggunakan Model DEO yang bertujuan untuk mengurangi banyaknya data yang diperoleh termasuk data yang tidak relevan dengan tindakan kejahatan yang terjadi berdasarkan skenario yang telah dirancang sehingga membantu peneliti dalam mempercepat proses analisis bukti digital.

Tahap reduksi bukti digital dilakukan secara berulang sebanyak n kali dengan menetapkan parameter pada pengaturan Model DEO hingga mendapatkan jumlah objek yang paling relevan dengan skenario. Jumlah iterasi ditentukan oleh *forensic examiner* berdasarkan hasil reduksi yang diperoleh. Iterasi dihentikan bilamana hasil reduksi pada iterasi ke-n+1 sama dengan iterasi ke-n.

Cara yang digunakan dalam menganalisis bukti digital adalah manual dengan menelusuri data yang diperoleh dari tahap reduksi bukti digital (*file, log timeline* peristiwa, dan komunikasi yang dilakukan) dan melakukan segmentasi pencarian. Setelah mendapatkan bagian segmen yang dicari, dilakukan analisis pada segmen tersebut beserta data yang terkandung di dalamnya. Hasil dari analisis ini merupakan pembuktian secara ilmiah/forensik terhadap bukti awal mengenai studi kasus yang terjadi, yaitu skenario yang diterapkan sehingga relevansi hasil analisis terhadap data awal diperoleh dari kecocokan antara *timeline* bukti digital dengan studi kasus tindak kejahatan berdasarkan skenario yang dirancang.

2.3.4. Analisis

Pada tahap ini dilakukan analisis berdasarkan data yang diperoleh dari tahap pemeriksaan. Data yang dianalisis terbatas pada data yang diperoleh setelah melakukan reduksi bukti digital menggunakan Model DEO. Pada tahap ini semua bukti digital yang memiliki korelasi dengan tindak kejahatan berdasarkan skenario akan dianalisis, tindakan kejahatan apa yang dilakukan, waktu kejadian peristiwa, dan identitas digital pengguna yang melakukan kejahatan [21]. Setelah itu dilakukan pengambilan keputusan dari hasil analisis terhadap bukti digital yang diperoleh untuk menyimpulkan kasus kejahatan yang terjadi.

2.3.5. Pelaporan Hasil

Tahap ini merupakan penulisan laporan yang berisikan hasil dari tahap analisis dan analisis kesesuaian penelitian. Pada laporan ini dijelaskan mengenai hasil penerapan Model DEO berbasis program Python dalam proses *mobile forensic* berdasarkan persentase reduksi data dan jumlah nilai FPR Model DEO. Dengan demikian, dapat disimpulkan kinerja Model DEO berbasis program Python dalam menginvestigasi kejahatan yang tersimpan di dalam penyimpanan internal BD1 berdasarkan skenario yang telah dirancang. Berikut adalah persamaan FPR.

$$\text{FPR} = \frac{C}{C+D} \quad (1)$$

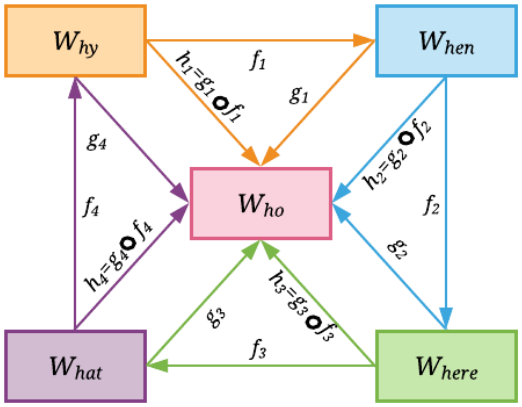
Keterangan:
C = jumlah objek tidak relevan yang dipulihkan
D = jumlah objek tidak relevan yang tidak dipulihkan

Jurnal Teknik Informatika (JUTIF)
P-ISSN: 2723-3863
E-ISSN: 2723-3871
Vol. 6, No. 4, August 2025, Page. 2707-2722
https://jutif.if.unsoed.ac.id
DOI: https://doi.org/10.52436/1.jutif.2025.6.4.4999

2.4. Model DEO untuk Reduksi Data pada Tahapan Pemeriksaan

Ukuran dataset yang besar pada penyimpanan perangkat digital dihasilkan dari banyaknya aktivitas yang terjadi yang dilakukan oleh pengguna. Ketika tindakan investigasi forensik dalam waktu yang cepat perlu dilakukan terhadap suatu perangkat digital, maka dibutuhkan suatu teknik yang mampu mereduksi dataset yang besar menjadi dataset yang kecil tanpa menghilangkan atau meninggalkan informasi penting yang diperlukan.

Model DEO merupakan sebuah cara yang diusulkan dalam penelitian [13] untuk mereduksi data dan menghasilkan dataset yang lebih efisien untuk dianalisis dan disimpulkan secara akurat. Model ini diusulkan oleh Grigaliunas et al berdasarkan analisis ekstraksi informasi dengan proses forensik yang tepat menggunakan elemen dari teori kategori [22], yaitu 5W (*Why, When, Where, What, Who*). Tujuan dari Model DEO adalah mengurangi jumlah data dari perangkat digital untuk mempercepat perolehan bukti digital dengan mengikuti empat fase panduan proses forensik, yaitu *collection, examination, analysis*, dan *reporting*. Tahap *examination* dibedakan menjadi dua bagian, yang pertama adalah dokumentasi (mendokumentasikan konten dan kondisi bukti digital secara lengkap) dan *data reduction*.



Gambar 5. Model *Digital Evidence Object* (DEO)

Berdasarkan Gambar 5, Model DEO memberikan keterkaitan antar kategori sebagai beriku:

a. Jika $f_1 : W_{hy} \rightarrow W_{hen}$ dan jika $g_1 : W_{hen} \rightarrow W_{ho}$ maka terdapat komposisi $h_1 = g_1 \circ f_1 : W_{hy} \rightarrow W_{ho}$
b. Jika $f_2 : W_{hen} \rightarrow W_{here}$ dan jika $g_2 : W_{here} \rightarrow W_{ho}$ maka terdapat komposisi $h_2 = g_2 \circ f_2 : W_{hen} \rightarrow W_{ho}$
c. Jika $f_3 : W_{here} \rightarrow W_{hat}$ dan jika $g_3 : W_{hat} \rightarrow W_{ho}$ maka terdapat komposisi $h_3 = g_3 \circ f_3 : W_{here} \rightarrow W_{ho}$
d. Jika $f_4 : W_{hat} \rightarrow W_{hy}$ dan jika $g_4 : W_{hy} \rightarrow W_{ho}$ maka terdapat komposisi $h_4 = g_4 \circ f_4 : W_{hat} \rightarrow W_{ho}$

3. RESULT

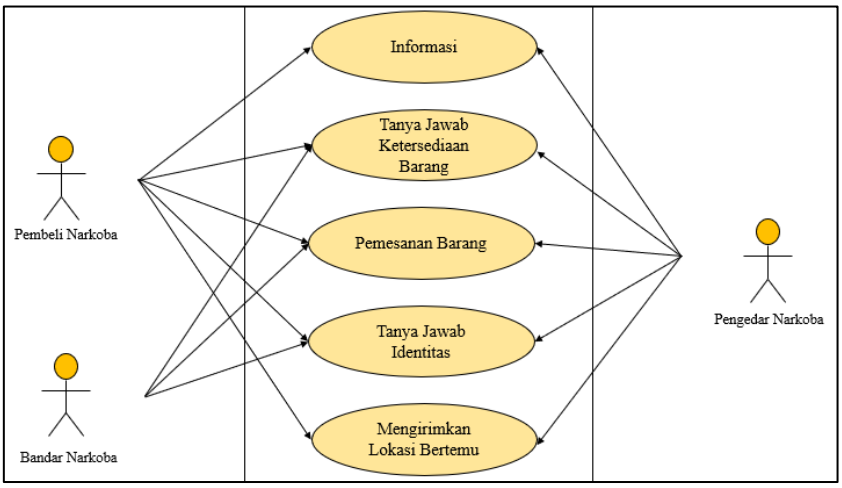
Bagian ini menjelaskan hasil dari tahapan metodologi yang dilakukan khususnya tahap akuisisi hingga analisis. Selain itu, bagian ini juga menjelaskan hasil reduksi data dari tools DEO berbasis python yang dikembangkan disertai tahapan analisis yang menunjukkan kemampuan forensik dalam mengupas kejadian yang telah diskenariokan. Adapun proses preservasi tidak dijelaskan pada bagian ini karena tahapan tersebut lebih ditujukan untuk menjadi kondisi perangkat bukti digital sebelum proses akuisisi. Begitu pun tahap laporan hasil karena tahapan tersebut berfokus pada penulisan laporan untuk didiseminasikan kepada user atau pada proses penegakan hukum [21].

3.1. Perancangan Skenario

Skenario yang dirancang berupa reka tindak kriminalitas jual-beli narkoba yang melibatkan tiga aktor berbahasa Indonesia yaitu; (1) Pengedar, (2) Pembeli, dan (3) Bandar narkoba. Investigasi forensik

Jurnal Teknik Informatika (JUTIF)
P-ISSN: 2723-3863
E-ISSN: 2723-3871
Vol. 6, No. 4, August 2025, Page. 2707-2722
https://jutif.if.unsoed.ac.id
DOI: https://doi.org/10.52436/1.jutif.2025.6.4.4999

dilakukan terhadap perangkat seluler yang digunakan para aktor dalam bertransaksi melalui komunikasi SMS. Gambar 6 menunjukkan diagram *use case* dari rancangan skenario pada artikel ini.



Gambar 6. Diagram *use case* dari rancangan skenario

Dari Gambar 6 dapat dilihat bahwa para aktor dapat bertukar informasi berupa pesan terkait ketersediaan barang, pemesanan barang, tanya jawab identitas sebagai pengenal ketika bertransaksi dan menyepakati lokasi pertemuan transaksi. Masing-masing kelima *use case* yang terdapat pada Gambar 6 selanjutnya dibuat *use case scenario* berupa tabel yang menjelaskan aktor, deskripsi, kondisi awal, skenario normal, skenario alternatif, dan kondisi akhir dari masing-masing *use case*. Tabel 2 menunjukkan salah satu contoh *use case scenario* berupa Tanya Jawab Ketersediaan Barang.

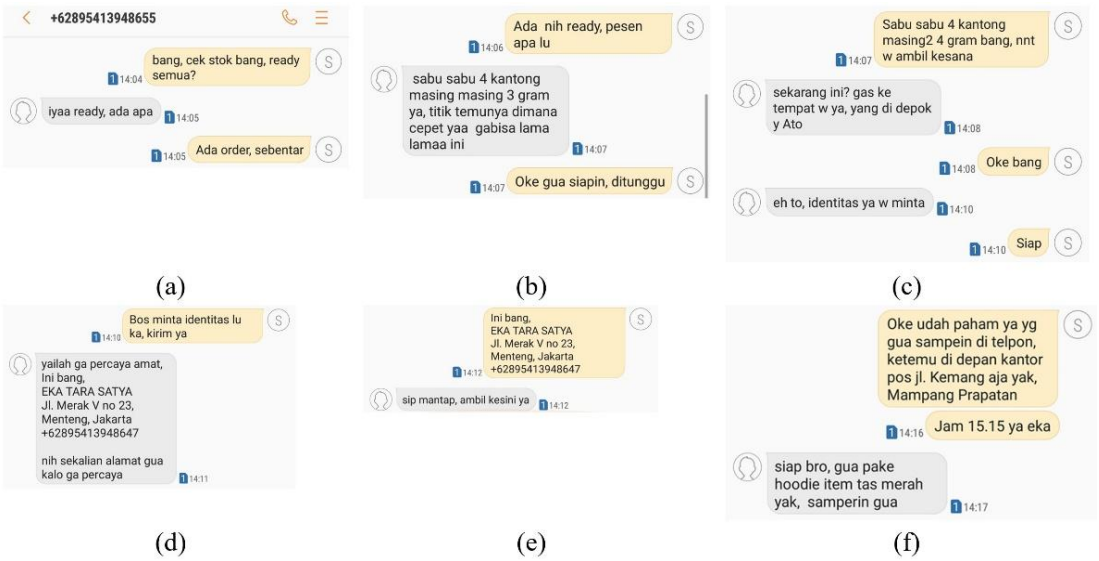
Tabel 2. *Use Case Scenario* berupa Tanya Jawab Ketersediaan Barang

Rincian	Penjelasan
Aktor	Pembeli, Pengedar dan Bandar
Deskripsi	Use case ini menjelaskan ketiga aktor melakukan tanya jawab mengenai ketersediaan barang
Kondisi Awal	Pembeli dan Pengedar belum mengetahui apakah Bandar narkoba memiliki ketersediaan barang
Skenario Normal	(1) Pengedar menghubungi Bandar untuk memastikan ketersediaan barang, (2) Bandar menyampaikan bahwa barang tersedia, (3) Pengedar menyampaikan kepada Pembeli bahwa barang tersedia, (4) Pengedar menanyakan barang yang diinginkan oleh Pembeli
Skenario Alternatif	-
Kondisi Akhir	Pembeli dan Pengedar mengetahui bahwa Bandar menyediakan barang

3.2. Penerapan Skenario

Pada tahapan ini, rancangan skenario dijalankan pada perangkat para aktor dalam berkomunikasi dan melakukan tindak kejahatan jual-beli narkoba. Perangkat yang digunakan untuk aktor Pengedar yaitu Samsung Galaxy A9 Pro dengan Android 7.0, Processor Octa Core, RAM 4 GB, dan penyimpanan internal 32 GB. Perangkat aktor Pengedar inilah yang diskenariokan disita pada saat penangkapan oleh penegak hukum dan selanjutnya dijadikan objek investigasi forensik. Di sisi lain, dua aktor lainnya yaitu Pembeli dan Bandar menggunakan perangkat yang sama yaitu OPPO A1K, yang pada penerapan skenario ini digunakan untuk mendukung skenario komunikasi SMS dengan perangkat aktor Pengedar. Gambar 3 menunjukkan *screenshots* komunikasi SMS pada perangkat aktor Pengedar yang dijadikan objek investigasi forensik.

Jurnal Teknik Informatika (JUTIF)
P-ISSN: 2723-3863
E-ISSN: 2723-3871
Vol. 6, No. 4, August 2025, Page. 2707-2722
https://jutif.if.unsoed.ac.id
DOI: https://doi.org/10.52436/1.jutif.2025.6.4.4999



Gambar 7. S*creenshots* komunikasi SMS pada perangkat aktor Pengedar

SMS yang dikomunikasikan antar para aktor yang ditunjukkan pada Gambar 7 telah disesuaikan dengan skenario yang telah dirancang pada Gambar 6. Dapat dilihat pada Gambar 7 terdiri dari; (a) Pengedar memastikan stok kepada Bandar; (b) Pengedar menerima pesanan dari Pembeli, (c) Pengedar meneruskan pesanan kepada Bandar, (d) Pengedar menerima informasi identitas Pembeli, (e) Pengedar mengirimkan identitas Pembeli kepada Bandar, (f) Pengedar mengirimkan lokasi temu transaksi kepada Pembeli.

3.3. Akuisisi

Setelah menjalankan tools dan perintah pada Tabel 1 secara berurutan, hasil awal yang diperoleh yaitu terlihatnya seluruh partisi yang terdapat pada penyimpangan internal BD1 dan diketahui bahwa "mmcblk0" merupakan lokasi yang menyimpan seluruh data dan partisi dari BD1. Hasil dari proses *imaging* "mmcblk0" berupa *disk image* yang diberi nama "android.dd" dengan ukuran 30 Gigabyte. Tabel 3 menunjukkan informasi detail dari hasil akuisisi disertasi dengan nilai *hash* untuk verifikasi integrasi datanya dengan tiga algoritma yaitu SHA1, MD5, dan SHA256. Nilai *hash* ini menjadi penting untuk memastikan *disk image* yang diperiksa dan dianalisis tidak mengalami perubahan sebagaimana bukti digital yang diakuisisi [23].

Tabel 3. *Disk image* hasil akuisisi perangkat BD1

Rincian	Informasi
Nama *File*	android.dd
Ukuran *File*	30 GB
Durasi Akuisisi	01:47:22
Nilai SHA1	69098E01DE9280B94AC7F95697785F00CB0FA147
Nilai MD5	E142A23BF7F96B80E76A924937E44959
Nilai SHA256	F4AD60E998AE2B9B59A9841726A4017F0D9F0035 EA15B105CAA41239A31D98B3

3.4. Pemeriksaan

Hasil dari tahap pemeriksaan yaitu informasi jumlah objek, entitas, dan struktur artefak yang terdapat di dalam *disk image* "android.dd*"*. Dengan memasukkan "android.dd" pada *tools* Autopsy

diperoleh bahwa ”android.dd” mengandung 22 kategori dengan total 142.892 artefak. Selain itu, diperoleh 40 partisi dengan dengan total 96.158 objek di dalamnya.

Hasil identifikasi juga menunjukkan dari 40 partisi terdapat satu partisi yaitu “Vol41” memiliki jumlah objek yang paling banyak di antara partisi yang lainnya dan diektahui bahwa partisi tersebut tersimpan banyak informasi pertukaran data dan *log* aktivitas yang dilakukan oleh pengguna, termasuk penyimpanan data dari skenario yang dijalankan. Informasi seluruh objek tersebut diekspor ke “file-report.txt” kemudian dikonversi menjadi “file-report.csv” untuk kemudahan pengolahan data pada Model DEO.

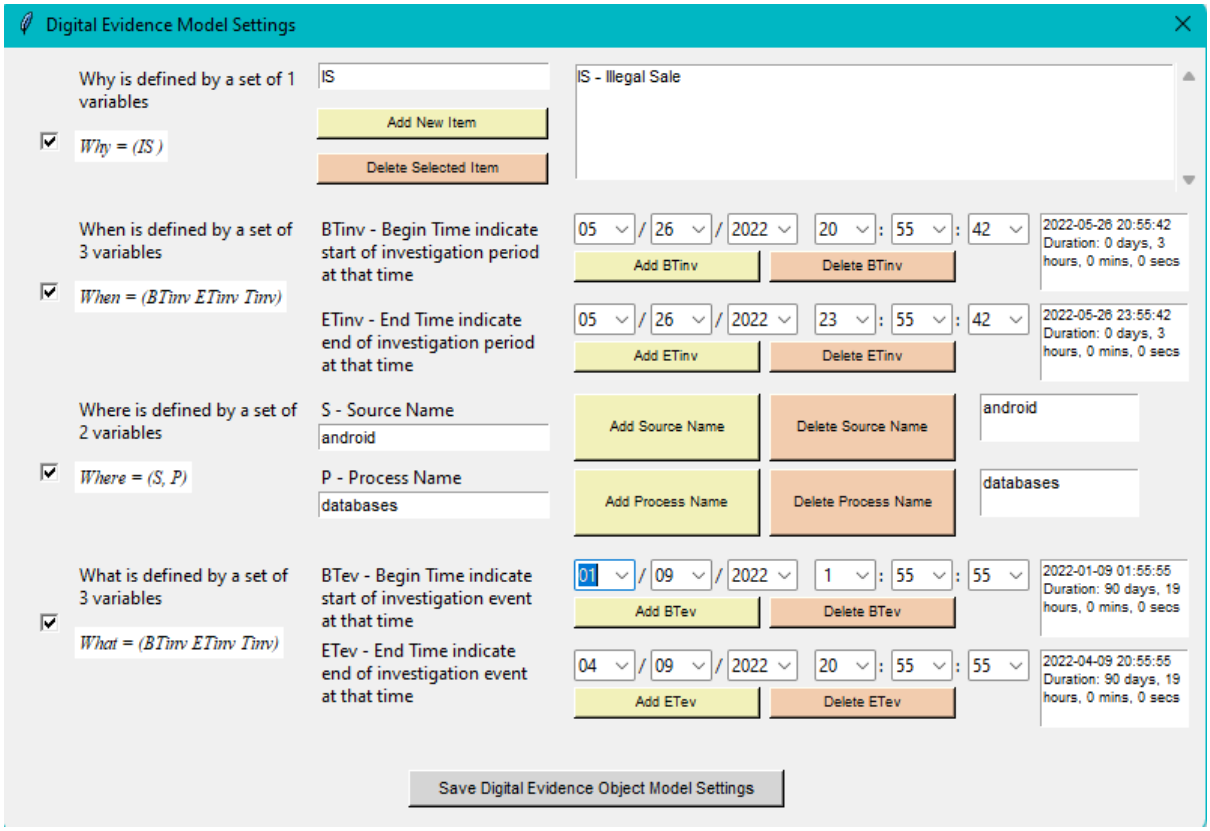
3.4.1. Reduksi Data dengan DEO

Tahap reduksi menggunakan tool DEO berbasis Python dengan input file “file-report.csv” hasil dari pemeriksaan menggunakan Autopsy. Selanjutnya Model DEO tersebut didefinisikan dengan lima variabel, yaitu DEO = (*Why, When, Where, What, Who*) dengan penyesuaian berdasarkan *case* yang dianalisis sesuai skenario sehingga pada masing-masing *tuple* disesuaikan sebagai berikut:

1. W_{hy} = {IS}
   IS adalah *Illegal Sale* dengan variabel IS = {mmssms, messages, telegram, instagram, telephony, barang, sabu}. Parameter yang ada di dalam variabel IS ditentukan berdasarkan data yang terdapat pada *internal storage* dan disesuaikan dengan skenario yang dijalankan, yaitu pertukaran pesan pada media sosial. *Illegal Sale* dipilih berdasarkan skenario yang telah diterapkan sebelumnya dan penyesuaian variabel yang dilakukan berdasarkan skenario yang diterapkan.
2. W_{hen} = {BT_{inv}, ET_{inv}, ΔT_{inv}}
   BT_{inv} adalah *Begin Time* yang mengindikasikan awal dari waktu investigasi menggunakan *timestamp* Unix, ET_{inv} adalah *End Time* yang mengindikasikan akhir dari waktu investigasi menggunakan *timestamp* Unix, dan Δ_{inv} adalah *Time Duration* yang mengindikasikan durasi waktu antara nilai waktu berturut-turut dari periode investigasi. Pada kasus yang dianalisis terjadi selama 3 jam yaitu antara 27-05-2022 20:55:42 hingga 27-05-2022 23:55:42.
3. W_{here} = {S, P}
   S melambangkan *Source of Investigation* dan P melambangkan *Place of Investigation. Source Name* pada *tuple Where* dipilih berdasarkan *data source* pada *disk image* “android.dd” yang berasal dari sistem operasi android. *Process name* dipilih berdasarkan file “databases” yang dihasilkan dari *tools* Autopsy setelah menganalisis *disk image* “android.dd” yang kemduain dikonversi kedalam format *comma separated value* (csv).
4. W_{hat} = {BT_{inv}, ET_{inv}, ΔT_{inv}}
   BT_{inv} adalah *Begin Time* yang mengindikasikan awal dari peristiwa yang diinvestigasi menggunakan *timestamp* Unix, ET_{inv} adalah *End Time* yang mengindikasikan akhir dari peristiwa yang diinvestigasi menggunakan *timestamp* Unix, dan Δ_{inv} adalah *Time Duration* yang mengindikasikan durasi waktu antara nilai waktu berturut-turut dari periode peristiwa yang diinvestigasi.
5. W_{ho} = {U, E}
   U adalah Orang yang melakukan aktivitas kriminal (+6281297384239, +62895413948655, dan +62895413948647) yang diketahui setelah melakukan analisis pada hasil reduksi data dan E adalah *Entity* (*process, file, directory, registry* atau entri sistem, dan lain-lain).

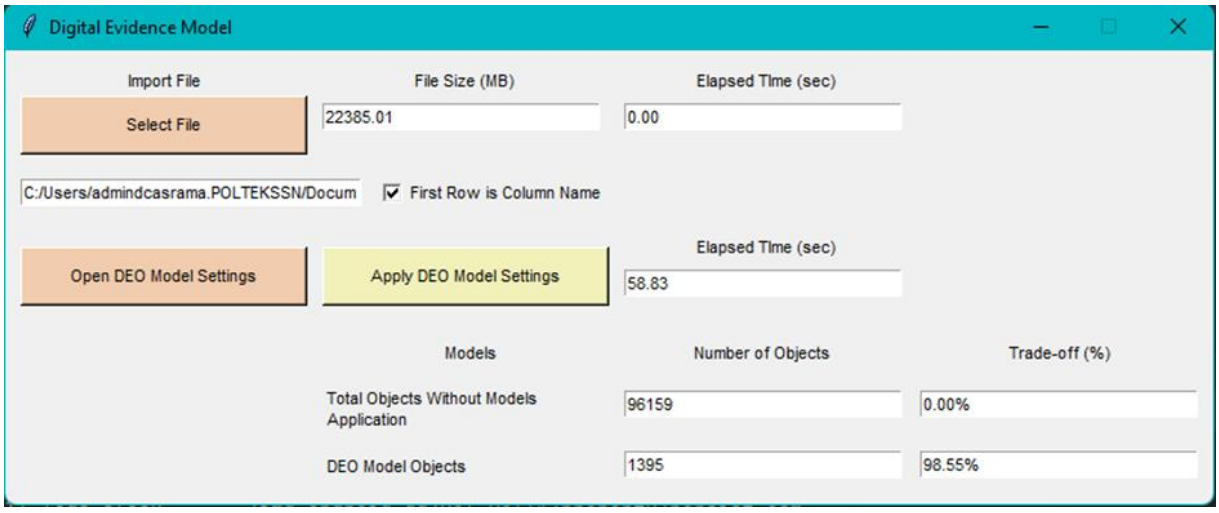
Gambar 8 menunjukkan DEO *settings* pada *tools* dengan tuple disesuaikan skenario kasus yang sedang dianalisis.

Jurnal Teknik Informatika (JUTIF)
P-ISSN: 2723-3863
E-ISSN: 2723-3871
Vol. 6, No. 4, August 2025, Page. 2707-2722
https://jutif.if.unsoed.ac.id
DOI: https://doi.org/10.52436/1.jutif.2025.6.4.4999



Gambar 8. Pengaturan kategori sesuai skenario pada *tools* DEO

Gambar 9 menunjukkan *main user interface* dari *tools* DEO yang dibuat dengan pemrograman Python. Selain itu pada gambar tersebut juga dapat dilihat ukuran file input, *path* dari file tersebut, waktu proses DEO, dan hasil reduksi dari sejumlah 96159 objek menjadi 1395 objek dengan persentase reduksi sebesar 98,55%.



Gambar 9. Hasil Reduksi Data menggunakan DEO

3.4.2. Repetisi Reduksi Data

Tahap reduksi bukti digital dilakukan sebanyak empat kali hingga mendapatkan jumlah artifak yang paling relevan dengan kasus yang sedang dianalisis. Proses reduksi sebanyak empat kali dilakukan

Vol. 6, No. 4, August 2025, Page. 2707-2722
https://jutif.if.unsoed.ac.id
DOI: https://doi.org/10.52436/1.jutif.2025.6.4.4999

berdasarkan rentang waktu yang dipersempit. Oleh karena itu, parameter yang diubah hanya *tuple When* pada masing-masing reduksinya. *Tuple When* diatur hingga mendekati waktu skenario dijalankan. Pada reduksi pertama, file "file-report.csv" dipilih dengan jumlah 96.158 objek dan mereduksi bukti digital sebanyak 98,55% hingga menghasilkan 1.395 objek pada file "deoModel2.csv". Hasil dari reduksi bukti digital setelah empat kali reduksi dijelaskan pada Tabel 4.

Tabel 4. Jumlah objek hasil reduksi dari repetisi yang dilakukan

Repetisi ke-	Nama File	Jumlah Objek Sebelum Reduksi	Jumlah Objek Setelah Reduksi	Total Reduksi	Presentase Reduksi
1	file-report.csv	96158	1395	94763	98,55%
2	deoModel1.csv	1395	1345	50	3,58%
3	deoModel2.csv	1345	1324	21	1,56%
4	deoModel3.csv	1324	74	1250	94,4%
Total Reduksi				96084	

Hasil percobaan pada reduksi kelima memperoleh hasil yang sama dengan reduksi keempat sehingga data dari reduksi kelima tidak dicantumkan. Selain itu, percobaan reduksi keenam tidak dilakukan karena hasil dari percobaan reduksi kelima sama dengan reduksi keempat. Dengan demikian, reduksi keempat merupakan hasil reduksi yang paling optimal pada kasus ini.

3.5. Analisis

Analisis dilakukan terhadap 74 objek hasil reduksi data dengan metode penelusuran path dan menganalisis konten dari setiap objek. Hasil yang diperoleh berupa empat objek yang terindikasi menyimpan bukti yang relevan sebagaimana ditunjukkan pada Tabel 5. Selanjutnya, dari kempat objek setelah dianalisis ditemukan bahwa objek ke-4 terdapat artefak yang berisikan pertukaran pesan teks pada BD1. File tersebut kemudian diekspor ke dalam format csv untuk analisis lebih lanjut dengan melihat artefak apa saja yang terdapat di dalamnya. File yang diekspor menghasilkan file dengan nama "Messages_20220515085604.csv" yang di dalamnya berisi 63 artefak pesan teks.

Tabel 5. Objek hasil analisis

No	Objek	Jumlah Artefak Pesan Teks
1	/img_android.dd/vol_vol41/user_de/0/com.android.providers.telephony/databases/mmssms.db-wal-slack	0
2	/img_android.dd/vol_vol41/user_de/0/com.android.providers.telephony/databases/mmssms.db-wal	0
3	/img_android.dd/vol_vol41/user_de/0/com.android.providers.telephony/databases/mmssms.db-shm	0
4	/img_android.dd/vol_vol41/user_de/0/com.android.providers.telephony/databases/mmssms.db	63

Tabel 6. Contoh hasil analisis berupa pesan disertai *timeline*

Timeline	Nomor kontak	Konten Pesan	Peristiwa
2022-04-09 14:07:44 ICT	+62895413948647	"Sabu sabu 4 kantong masing2 4 gram bang, nnt w ambil kesana"	Pengedar menyampaikan pesanannya kepada bandar
2022-04-09 14:08:25 ICT	+62895413948655	"sekarang ini? gas ke tempat w ya, yang di depok y Ato"	
2022-04-09 14:08:34 ICT	+62895413948647	"Oke bang"	

Artefak yang tersebut kemudian dianalisis dengan mencari keterkaitan antara pesan teks yang dikirim dan pesan teks yang diterima serta yang memiliki keterkaitan dengan skenario yang diterapkan. Berdasarkan hasil analisis, disusun *timeline* peristiwa sebagaimana contoh salah satu pesan yang terungkap pada tahap analisis ditunjukkan pada Tabel 6.

3.6. Perbandingan kinerja pemeriksaan *exhaustive search* dengan Model DEO

Pemeriksaan artefak dalam jumlah besar yang diekstraksi dari bukti digital membutuhkan waktu dan tenaga yang lebih besar jika dilakukan secara manual dengan mencari informasi kunci satu per satu (*exhaustive search*). Untuk itu Model DEO ditujukan untuk mereduksi data sehingga membantu analis forensik tidak menghabiskan waktu untuk menganalisis artefak yang tidak relevan dengan kasus yang sedang dianalisis. Perbandingan efisiensi antara metode *exhaustive search* dengan Model DEO dapat dihitung menggunakan persentase reduksi data sebagai berikut:

$$Persentase = \frac{Jumlah\ objek\ yang\ ter{-}reduksi}{Jumlah\ objek\ sebelum\ direduksi}\ x\ 100\% = \frac{96.804}{96.158}\ x\ 100\% = 99{,}92\% \quad (2)$$

Dari perhitungan (2) dapat dilihat bahwa Model DEO mampu mereduksi objek yang tidak relevan dengan skenario kasus sebanyak 99,92% yang berarti objek-objek yang dianalisis merupakan objek yang memiliki relevansi tinggi dengan skenario yang diterapkan, sehingga objek tersebut dapat dijadikan sebagai bukti untuk membuktikan adanya tindak kejahatan yang terjadi melalui perangkat *smartphone*.

3.7. Tingkat akurasi objek hasil reduksi data dengan Model DEO

Reduksi data yang dilakukan dengan Model DEO menunjukkan efisiensi yang signifikan, namun hasil reduksi juga harus dipastikan mencapai tingkat akurasi yang tinggi sehingga memberikan objek tereduksi yang relevan. Pada artikel ini tingkat akurasi Model DEO diukur dengan nilai *False Positive Rate* (FPR) yang digunakan untuk mengetahui *error* pendeteksi objek yang direduksi oleh *tools* DEO yang dikembangkan.

$$FPR = \frac{C}{C+D} = \frac{C}{C+D} = \frac{70}{70+96.084} = 0{,}00072 \quad (3)$$

Keterangan:
C = jumlah objek tidak relevan yang dipulihkan
D = jumlah objek tidak relevan yang tidak dipulihkan

Dari perhitungan (3) dapat dilihat bahwa nilai FPR yang diperoleh sebesar 0,00072 mengindikasikan bahwa *tools* DEO yang dikembangkan memiliki rasio *error* yang sangat kecil. Dengan demikian, *tools* DEO mampu mereduksi objek yang benar-benar tidak relevan dengan kasus yang sedang dianalisis, sehingga objek yang dipertahankan (tidak direduksi) memiliki relevansi yang tinggi dengan kasus yang sedang dianalisis.

4. DISCUSSIONS

Berdasarkan hasil yang diperoleh, pembahasan difokuskan kepada dua aspek yaitu tingkat efisiensi dan tingkat akurasi hasil reduksi data menggunakan Model DEO yang diimplementasikan. Tingkat efisiensi diukur dengan persentase objek yang direduksi dibandingkan dengan seluruh objek yang diekstrasi tanpa proses reduksi[24]. Dampak dari reduksi yang dilakukan dibandingkan dengan pemeriksaan satu per satu (*exhaustive search*). Selanjutnya, tingkat akurasi diukur dengan *False Positive Rate* (FPR) [25] yang digunakan untuk mengetahui *error* pendeteksi objek yang direduksi oleh *tools* DEO yang dikembangkan. Semakin besar nilai FPR maka semakin rendah tingkat akurasi *tools* DEO dan berlaku sebaliknya.

4.1. Validasi hasil Pemeriksaan dan Analisis dengan skenario yang diterapkan

Validasi hasil yang diperoleh pada tahap Pemeriksaan dan Analisis dilakukan dengan memastikan bahwa hasil yang diperoleh sesuai dengan skenario kasus yang telah dirancang dan diterapkan di awal. Teknik validasi ini disebut juga validasi simulasi. Dari simulasi yang dilakukan, metode DEO pada tahap pemeriksaan mampu mereduksi secara signifikan objek yang dianalisis, sehingga mengarahkan proses analisis hanya kepada objek yang relevan dengan kasus yang diperiksa. Seluruh komunikasi SMS pada Gambar 7 berhasil ditemukan dan dikupas pada tahap Analisis.

Hal ini menunjukkan bahwa meskipun reduksi dilakukan secara signifikan, namun objek yang relevan dengan kasus tetap terjaga tanpa terkena reduksi. Dengan demikian, reduksi yang dilakukan tidak menghilangkan objek yang relevan dengan kasus, sehingga tetap memberikan hasil yang valid. Contoh pesan yang berhasil dianalisis sebagaimana disajikan pada Tabel 6 sesuai dengan pesan pada skenario komunikasi SMS pada tahap penerapan skenario. Adapun bilamana pada kasus tertentu, proses analisis dari hasil reduksi data tidak mengupas komunikasi secara utuh, *forensic examiner* masih mempunyai data awal sebelum reduksi dan dapat mencari objek yang hilang dari data tersebut dengan pencarian yang lebih cepat karena sudah memperoleh metadata dari objek yang relevan hasil analisis data tereduksi. Pendekatan tersebut sangat membantu *forensic examiner* dalam mengupas seluruh objek yang relevan dengan kasus yang sedang diinvestigasi.

4.2. Pengembangan Lanjutan

Pengembangan lanjutan dapat berupa pengembangan Model berbasis DEO yang mampu melakukan reduksi data pada proses *mobile forensic* dengan artefak yang terenkripsi. Meskipun konten artefak terenkripsi namun pendekatan DEO dengan mengorelasikan berbagai *metadata* pada konfigurasi memungkinkan untuk mendeteksi relevansi file terenkripsi tersebut dengan kasus yang sedang dianalisis. Selain itu, perlu dikaji potensi pendekatan DEO pada platform lain yaitu IoT *forensic* dan *cloud forensic*, yang penggunaan platform tersebut semakin berkembang.

5. CONCLUSION

Pada artikel ini dilakukan investigasi forensik terhadap penyimpanan internal *smartphone* berbasis Android OS dengan proses reduksi bukti digital menggunakan Model DEO yang implementasikan pada *tools* berbasis *python.* Berdasarkan hasil dan pembahasan dapat disimpulkan bahwa Model DEO yang diterapkan mampu mereduksi jumlah objek yang diperoleh dari tahap akuisisi secara signifikan, dengan total reduksi sebanyak 96.084 objek yang dicapai dalam empat repetisi. Dari hasil tersebut, Model DEO telah mereduksi objek sebanyak 99,92% dan menghasilkan 74 objek untuk dianalisis sehingga diperoleh objek akurat yang merupakan lokasi penyimpanan dari skenario yang dijalankan. Selain itu, penerapan Model DEO berbasis *python* pada proses *mobile forensic* mampu mengefisiensi proses investigasi forensik tanpa perlu menganalisis seluruh objek dan bukti digital yang diperoleh. Dengan menganalisis jumlah objek yang sedikit, penerapan Model DEO sangat membantu analis forensik dalam mengefisiensi waktu investigasi dan pengambilan keputusan di waktu yang kritikal. Lebih lanjut, Model DEO yang dikembangkan mampu memberikan hasil reduksi dengan perhitungan FPR yang sangat rendah yaitu 0,00072 yang berarti semua objek melalui proses analisis dan reduksi sesuai dengan parameter yang ditetapkan pada pengaturan Model DEO. Hal ini didukung dengan objek-objek yang dianalisis memiliki keutuhan informasi dan relevansi dengan skenario yang ditetapkan sehingga hasil analisis dapat dijadikan sebagai bukti yang sah dan akurat.

CONFLICT OF INTEREST

The authors declares that there is no conflict of interest between the authors or with research object in this paper.

ACKNOWLEDGEMENT

Acknowledgement is only addressed to funders or donors and object of research. Acknowledgement can also be expressed to those who helped carry out the research.

REFERENCES

[1] D. Kim and S. Lee, "Study of identifying and managing the potential evidence for effective Android forensics," *Forensic Sci. Int. Digit. Investig.*, vol. 33, p. 200897, Jun. 2020, doi: 10.1016/j.fsidi.2019.200897.

[2] H. Alatawi, K. Alenazi, S. Alshehri, S. Alshamakhi, M. Mustafa, and A. Aljaedi, "Mobile forensics: A review," presented at the 2020 International Conference on Computing and Information Technology (ICCIT-1441), IEEE, 2020, pp. 1–6.

[3] C. M. da Silveira *et al.*, "Methodology for forensics data reconstruction on mobile devices with android operating system applying in-system programming and combination firmware," *Appl. Sci.*, vol. 10, no. 12, p. 4231, 2020.

[4] C. Anglano, M. Canonico, and M. Guazzone, "The android forensics automator (anfora): A tool for the automated forensic analysis of android applications," *Comput. Secur.*, vol. 88, p. 101650, 2020.

[5] X. Zhao, "Survey: The Evolution and Future of Android Software Development," vol. 1, no. 1, 2024, doi: 10.71080/dlpr.v1i1.64.

[6] C. Vaishali, V. Thirumalaiswamy, and M. Thillaichidambaram, "Introduction to Digital Forensics," in *AI and Emerging Technologies*, CRC Press, 2025, pp. 27–35.

[7] M. Moreb, S. Salah, and B. Amro, "A novel framework for mobile forensics investigation process," *Int. J. Comput. Digit. Syst.*, vol. 16, no. 1, pp. 125–136, 2024.

[8] T. Sutikno, "Mobile forensics *tools* and techniques for digital crime investigation: a comprehensive review," *Int. J. Inform. Commun. Technol.*, vol. 13, no. 2, p. 321, 2024, doi: 10.11591/ijict.v13i2.pp321-332.

[9] M. Al-Fayoumi, M. Al-Fawa'reh, Q. A. Al-Haija, and A. Alakailah, "Towards Detecting Digital Criminal Activities Using File System Analysis," in *Proceedings of Data Analytics and Management*, A. Swaroop, Z. Polkowski, S. D. Correia, and B. Virdee, Eds., Singapore: Springer Nature Singapore, 2024, pp. 531–550.

[10] A. Almuqren, H. Alsuwaelim, M. H. Rahman, and A. A. Ibrahim, "A Systematic Literature Review on Digital Forensic Investigation on Android Devices," *Procedia Comput. Sci.*, vol. 235, pp. 1332–1352, 2024.

[11] R. Ayers, W. Jansen, and S. Brothers, "Guidelines on mobile device forensics (NIST Special Publication 800-101 Revision 1)," *NIST Spec Publ*, vol. 1, no. 1, p. 85, 2014.

[12] M. R. Setyawan, "Perbandingan *Tools* Forensik Dalam Analisis Bukti Digital Pada Aplikasi Skype Menggunakan Framework NIST," *J. Mahajana Inf.*, vol. 8, no. 2, pp. 80–88, 2023, doi: 10.51544/jurnalmi.v8i2.4580.

[13] S. Grigaliunas, J. Toldinas, A. Venckauskas, N. Morkevicius, and R. Damaševičius, "Digital evidence object Model for situation awareness and decision making in digital forensics investigation," *IEEE Intell. Syst.*, vol. 36, no. 5, pp. 39–48, 2020.

[14] Š. Grigaliūnas and J. Toldinas, "Habits attribution and digital evidence object Models based tool for cybercrime investigation," *Balt. J. Mod. Comput.*, vol. 8, no. 2, pp. 275–292, 2020.

[15] A. M. Wazarkar, "Python: A Quintessential approach towards Data Science," *Int. J. Res. Appl. Sci. Eng. Technol.*, vol. 9, pp. 3018–3024, 2021, doi: 10.22214/IJRASET.2021.35683.

[16] M. A. Kabir and M. Ahmed, "Python for Data Analytics: A Systematic Literature Review of *Tools*, Techniques, and Applications," *Acad. J. Sci. Technol. Eng. Math. Educ.*, vol. 4, no. 04, pp. 10–69593, 2024.

[17] N. Kishore and P. Raina, "Digital Forensics in Mobile Phones: An Overview of Data Acquisition Techniques and its Challenges," pp. 108–125, 2024, doi: 10.2174/9789815238990124010010.

[18] H. H. Lwin, W. P. Aung, and K. K. Lin, "Comparative Analysis of Android Mobile Forensics *Tools*," 2020, doi: 10.1109/ICCA49400.2020.9022838.

Vol. 6, No. 4, August 2025, Page. 2707-2722
https://jutif.if.unsoed.ac.id
DOI: https://doi.org/10.52436/1.jutif.2025.6.4.4999

[19] J. Fonseca-Bustos, K. A. Ramírez-Gutiérrez, and C. Feregrino-Uribe, "A robust self-supervised image hashing method for content identification with forensic detection of content-preserving manipulations.," *Neural Netw.*, vol. 177, p. 106357, 2024, doi: 10.1016/j.neunet.2024.106357.

[20] M. Farnan, J. Pratt, and M. Shakiba, "Digital Forensic *Tools*: Comparison of Autopsy TSK and Forensic Explorer," pp. 1–5, 2024, doi: 10.1109/iciteics61368.2024.10625076.

[21] A. K. Singh and O. P. Rai, "Exploring the role of forensic science in modern law enforcement: Challenges and opportunities," *Int. J. Crim. Common Statut. Law*, vol. 4, no. 1, pp. 122–126, 2024, doi: 10.22271/27899497.2024.v4.i1b.75.

[22] J. Mau, "Category theory for structural characterization," pp. 15–44, 2024, doi: 10.1515/9783111341996-003.

[23] K. A. Lakshmi, P. B. Honnavali, and S. Rajashree, "Ensure the Validity of Forensic Evidence by Using a Hash Function," Springer, Singapore, 2021, pp. 341–346. doi: 10.1007/978-981-15-7345-3_28.

[24] A. Harika, P. Sharma, K. Aravinda, A. Nagpal, Praveen, and A. Albawi, "Efficient Data Sampling and Reduction Methods in Large-Scale Forensic Analysis," pp. 1–7, 2024, doi: 10.1109/otcon60325.2024.10687910.

[25] N. Richetelli, L. Hammer, and J. A. Speir, "Forensic Footwear Reliability: Part III-Positive Predictive Value, Error Rates, and Inter-Rater Reliability.," *J. Forensic Sci.*, vol. 65, no. 6, pp. 1883–1893, 2020, doi: 10.1111/1556-4029.14552.