JIPI (Jurnal Ilmiah Penelitian dan Pembelajaran Informatika)
Journal homepage: https://jurnal.stkippgritulungagung.ac.id/index.php/jipi
ISSN: 2540-8984
Vol. 11, No. 1, March 2026, Pp.544-556

IMPLEMENTASI METODE STATIC FORENSICS UNTUK EKSTRAKSI FILE STEGANOGRAFI PADA BUKTI DIGITAL MENGGUNAKAN FRAMEWORK NIST

Asran*[1)], Erick Irawadi Alwi[2)], Huzain Azis[3)]
1. Teknik Informartika, Fakultas Ilmu Komputer, Universitas Muslim Indonesia, Indonesia
2. Teknik Informartika, Fakultas Ilmu Komputer, Universitas Muslim Indonesia, Indonesia
3. Teknik Informartika, Fakultas Ilmu Komputer, Universitas Muslim Indonesia, Indonesia

Article Info
Kata Kunci: Anti Forensik; InvisibleSecrets; NIST; Steganografi

Keywords: Anti-Forensic; InvisibleSecrets; NIST; Steganography

Article history:
Received 17 January 2025
Revised 28 January 2025
Accepted 8 February 2025
Available online 1 March 2026

DOI :
https://doi.org/10.29100/jipi.v11i1.7406

* Corresponding author.
Asran
E-mail address:
13020210222@umi.ac.id

ABSTRAK
Steganografi berfungsi sebagai teknik anti-forensik yang memungkinkan pelaku kejahatan menyembunyikan informasi dalam pesan lain, hal tersebut dapat menyulitkan penyelidik untuk menemukan bukti sebenarnya atas suatu kejahatan. Oleh karena itu, penyelidik harus mengenali dan memanfaatkan alat yang tepat untuk ekstraksi guna mengakses pesan yang melibatkan steganografi. Penelitian ini bertujuan untuk menganalisis bukti digital dengan menerapkan metode forensik statis berdasarkan kerangka kerja yang disiapkan oleh National Institute of Standards and Technology (NIST), penelitian ini juga berfokus pada proses ekstraksi file yang disusupi menggunakan steganografi, yang dilakukan berdasarkan skenario kejahatan. Alat yang dipakai dalam penelitian ini mencakup FTK Imager, Autopsy, HashMyFiles, USB Write Blocker, WinHex, Stegspy, serta InvisibleSecrets. Analisis proses ekstraksi menunjukkan bahwa, dari 10 file yang diperiksa sesuai dengan skenario kasus, 9 file berhasil diekstraksi dan menghasilkan tingkat keberhasilan sebesar 90%. Sebaliknya, 10% file yang tersisa tidak berisi data atau informasi tersembunyi yang relevan. Dari hasil tersebut dapat disimpulkan bahwa file steganografi yang berhasil diekstrak dapat dijadikan sebagai alat bukti materiil hukum yang sah.

ABSTRACT
Steganography serves as an anti-forensic technique that allows offenders to hide information in other messages, which might make it difficult for investigators to uncover actual evidence of a crime. Consequently, investigators must identify and employ the appropriate techniques for extraction to access messages that involve steganography. This research intends to analyze digital evidence through the application of static forensic methods derived from a framework established by the National Institute of Standards and Technology (NIST). It also emphasizes the extraction process of compromised files utilizing steganography, conducted within the context of a criminal scenario. The tools used in this research are FTK Imager, Autopsy, HashMyFiles, USB Write Blocker, WinHex, Stegspy, and InvisibleSecrets. The analysis of the extraction process revealed that, out of the 10 files assessed in accordance with the case scenario, 9 files were successfully extracted, yielding a 90% success rate. In contrast, the other 10% of files did not include any important hidden data or metadata. The results indicate that the successfully retrieved steganographic data may serve as admissible judicial evidence.

.

I. PENDAHULUAN

KEMAJUAN teknologi dan informasi yang pesat telah membawa banyak keuntungan bagi hidup manusia, tetapi di sisi lain, kemajuan tersebut juga menjadi pemicu meningkatnya tindakan kejahatan siber. Jaringan komputer atau Internet adalah salah satu teknologi utama yang digunakan dalam banyak kegiatan kriminal[1]. Berdasarkan laporan akhir tahun 2024 yang disampaikan oleh Kapolri Jenderal Listyo Sigit Prabowo di Mabes Polri, Jakarta Selatan, tercatat sebanyak 3.331 tindak pidana yang berkaitan dengan

penggunaan teknologi digital[2]. Laporan tersebut menekankan bahwa bukti memegang peranan penting dalam proses penyidikan, karena keberadaannya menentukan keberhasilan penyelesaian kasus kejahatan. Adanya bukti berfungsi sebagai petunjuk telah terjadinya suatu peristiwa hukum. Dalam kebanyakan kasus kejahatan siber, pelaku dan korban biasanya meninggalkan jejak atau sisa aktivitas mereka pada perangkat yang digunakan[3]. Terdapat dua kategori barang bukti yang diidentifikasi melalui forensik digital, yaitu bukti elektronik dan bukti digital[4]. Bukti elektronik adalah bukti yang dapat diidentifikasi secara fisik melalui pengamatan visual. Oleh karena itu, penyidik harus mampu mengidentifikasi dan memahami secara menyeluruh ciri-ciri barang bukti elektronik saat melakukan penyidikan di lokasi kejadian.

Bukti digital mengacu pada bukti digital yang diekstraksi atau dipulihkan dari bukti elektronik[5]. Berdasarkan Undang-Undang Republik Indonesia, Pasal 5 Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik ("UU ITE"), dokumen elektronik atau informasi elektronik merupakan alat bukti yang mempunyai kekuatan hukum tetap di Indonesia. Menurut Pasal 6, informasi elektronik atau dokumen elektronik dianggap sah jika dapat diakses, dapat dilihat, terjamin keasliannya, dan bisa dipertanggung jawabkan sehingga dapat menjelaskan keadaan sebenarnya[6]. Oleh karena itu, dalam menyelesaikan kasus kriminal yang melibatkan bukti elektronik atau digital, penting untuk memperhatikan dan menganalisis jenis bukti secara rinci agar dapat memahami hubungan antara satu dokumen dan dokumen yang lain.

Pelaku kejahatan siber memanfaatkan keterampilan dan kemampuan baru dengan melakukan aktivitas, teknik, dan alat anti-forensik untuk menutupi jejak mereka dan menghindari deteksi[7]. Akibatnya, serangan siber semakin canggih dan efektif. Menurut perspektif investigator digital, teknik anti-forensik bisa menghambat upaya pengumpulan bukti, memperlambat investigasi, dan menghasilkan bukti yang tidak akurat, yang berpotensi berdampak pada hasil penyelidikan serta menghalangi pengidentifikasian kejahatan digital[8].

Sebagai salah satu metode anti forensik digital, steganografi memberi kesempatan kepada para pelaku kejahatan untuk menyembunyikan informasi dalam berbagai format media digital, seperti tulisan, foto, suara, atau video, yang membuat penyelidik kesulitan dalam memperoleh bukti yang autentik mengenai informasi yang berhubungan dengan kejahatan[9]. Penggunaan steganografi biasanya membutuhkan dua komponen utama yaitu media dan data informasi yang disembunyikan di dalamnya[10]. Oleh karena itu, seorang penyelidik harus memiliki keterampilan untuk menganalisis, mengidentifikasi, dan mengekstrak informasi tersembunyi.

Cybercrime adalah masalah penting yang membutuhkan pedoman khusus untuk teknik investigasi guna memastikan pembuktian dapat dilakukan secara ilmiah[11]. Dalam memastikan bahwa investigasi kejahatan siber berjalan lebih efektif, efisien, dan terarah, penerapan dan pemanfaatan kerangka kerja atau framework digital forensik yang terstruktur sangat diperlukan[12]. Kerangka kerja forensik yang sering diterapkan dalam investigasi kasus digital forensik meliputi National Institute of Justice (NIJ)[13], National Institute of Standards and Technology (NIST), Digital Forensics Research Workshop (DFRWS)[14], Association of Chief Police Officers(ACPO)[15], Generic Computer Forensic Investigation Model (GCFIM)[16], dan Digital Forensics Investigation Framework (DFIF)[17].

Penelitian sebelumnya dengan topik sejenis telah dilakukan dengan judul "**Penerapan Metode Static Forensics untuk Ekstraksi File Steganografi pada Bukti Digital Menggunakan Framework DFRWS**[18]. Penelitian ini membahas penerapan framework DFRWS untuk melakukan investigasi pada file steganografi menggunakan perangkat lunak seperti FTK Imager, Autopsy, WinHex, Hiderman, dan StegSpy. Penelitian ini menerapkan tahapan investigasi secara sistematis, meliputi identifikasi, pelestarian, pengumpulan, pemeriksaan, analisis, dan presentasi hasil, yang bertujuan untuk menemukan bukti digital yang valid dan sah secara hukum.

Penelitian lainnya dengan topik yang sama juga telah dilakukan dengan judul "**Simulasi Investigasi pada FlashDisk dalam Mengungkap Pesan pada Kasus Perdagangan Narkoba menggunakan Metode Steganografi**[19]. Investigasi dilakukan dengan menggunakan berbagai alat seperti FTK Imager, Autopsy, dan Hex Editor Neo. Alat-alat ini membantu menemukan dan mengekstrak pesan tersembunyi dari file gambar yang tersimpan pada flashdisk. Tahapan penelitian terdiri dari *identification*, *preservation*, *collection*, *examination*, *analysis*, serta *presentation*.

Dalam penelitian ini, kerangka kerja NIST digunakan untuk melakukan forensik bukti digital dan mengekstrak file yang berisi pesan tersembunyi. Metode NIST dipilih karena *framework* ini menawarkan pedoman standar yang sistematis, fleksibel, dan terpercaya yang memastikan keaslian data, melindungi integritas bukti digital, dan meningkatkan validitas hasil analisis untuk mendukung proses hukum[20].

Selain itu, metode NIST dipilih karena kemampuannya untuk menggabungkan berbagai alat forensik, seperti FTK Imager dan InvisibleSecrets. Di sisi lain, penelitian sebelumnya, seperti yang dilakukan oleh Sunardi[18] dengan *framework* DFRWS tidak melakukan validasi hasil ekstraksi secara eksplisit melalui pengecekan nilai hash atau sertifikasi alat. Salah satu kekurangan utama dari penelitian sebelumnya adalah kemungkinan terjadinya

perubahan data saat proses pengambilan, yang dapat mempengaruhi keaslian bukti digital. Framework NIST menangani masalah tersebut dengan menggunakan mekanisme *write-blocking* dan pengecekan hash untuk memastikan integritas bukti.

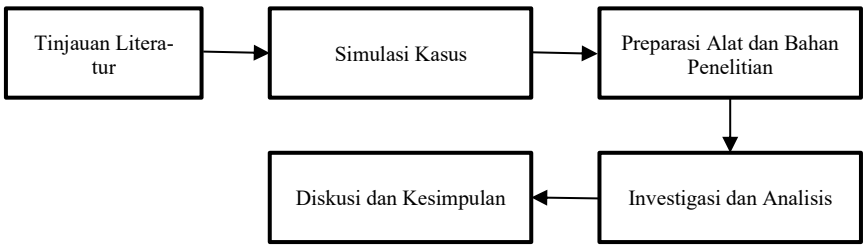
Penelitian ini bertujuan untuk mengembangkan metodologi forensik digital berbasis NIST yang terukur dan teruji dalam ekstraksi steganografi dengan mengintegrasikan alat write-blocker dan validasi hash untuk mencegah perubahan data, serta mengombinasikan penggunaan FTK Imager, Autopsy, dan InvisibleSecrets yang telah diuji kompatibilitasnya dengan standar NIST.

Pada penelitian sebelumnya[18] dan [19] yang menggunakan kerangka kerja DFRWS telah berhasil dalam mengambil file steganografi. Namun, kerangka kerja tersebut belum sepenuhnya memastikan keabsahan hukum dari bukti digital karena kurangnya standar prosedur yang diakui secara global. Selain itu, penelitian sebelumnya lebih menekankan pada penemuan steganografi tanpa memberikan perhatian yang cukup terhadap keutuhan bukti selama proses pengambilan dan analisis. Untuk mengatasi masalah ini, penelitian ini menerapkan kerangka NIST, yang memberikan panduan terstruktur untuk memastikan keaslian dan sahnya bukti digital dalam konteks hukum.

Hasil dari penelitian ini menyajikan metode yang terstandarisasi untuk menyelidiki steganografi, yang dapat digunakan oleh para penyidik dalam mengungkap kejahatan siber seperti perdagangan narkoba atau terorisme. Dengan menjamin keaslian bukti melalui kerangka kerja NIST, hasil dari ekstraksi dapat dipertanggungjawabkan di pengadilan, sehingga memperkuat posisi hukum para penyidik. Contoh praktis adalah pemanfaatan InvisibleSecrets yang sudah divalidasi oleh NIST untuk mengambil pesan yang tersembunyi di dalam file gambar, seperti petunjuk lokasi untuk transaksi narkoba.

II. METODE PENELITIAN

Dalam menjalankan sebuah penelitian, metode sangat penting untuk mencapai keberhasilan penelitian. Penggunaan teknik dan analisis forensik yang benar akan memberikan tingkat keberhasilan hampir 100% dalam mendapatkan data forensik[21]. Langkah-langkah pengumpulan bukti digital dalam penelitian ini dilakukan menggunakan pendekatan forensik statis, seperti yang ditunjukkan pada Gambar 1. Forensik Statis merupakan cara dalam forensik digital yang mengumpulkan bukti-bukti digital dengan cara ekstraksi serta analisis setelah terjadinya insiden, termasuk pemeriksaan salinan duplikat atau *disk imaging*[22].



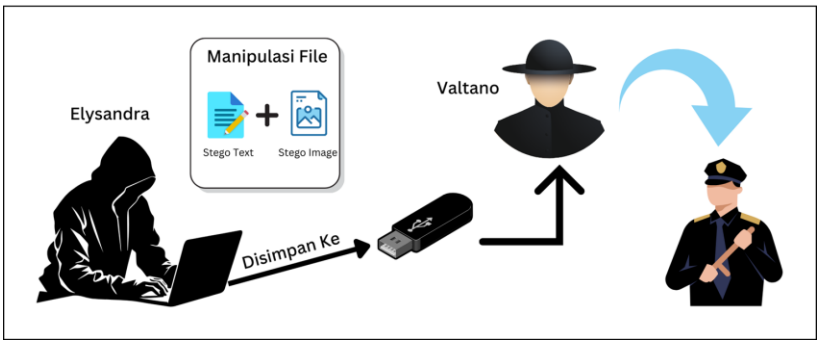
Gambar 1. Metode Penelitian

Berdasarkan pada Gambar 1, metodologi penelitian dirancang secara terstruktur untuk menunjukkan langkah-langkah yang bisa digunakan sebagai panduan untuk mengelola topik permasalahan dalam penelitian ini. Metodologi dimulai dengan studi literatur, yaitu mengumpulkan data dari penelitian yang relevan sebelumnya sebagai referensi dari berbagai sumber. Langkah berikutnya meliputi pembuatan skenario kasus, persiapan perangkat serta bahan untuk simulasi, pelaksanaan analisis dan investigasi kasus, kemudian diakhiri dengan diskusi dan penulisan kesimpulan

A. Simulasi Kasus

Simulasi kasus dirancang untuk membantu proses identifikasi saat memeriksa data digital. Perangkat penyimpanan seperti flash drive USB digunakan sebagai bukti dan dibiarkan dalam keadaan tidak aktif (dimatikan) pada perangkat komputer. Studi ini berfokus pada data digital simulasi untuk menggambarkan perilaku kriminal, terutama yang melibatkan penyalahgunaan steganografi. Metode ini memanfaatkan flashdisk sebagai penyimpanan untuk menyembunyikan informasi, sehingga memungkinkan pengujian terhadap prosedur investigasi forensik digital yang relevan. Berikut tampilan simulasi kasus dalam penelitian ini pada Gambar 2.

JIPI (Jurnal Ilmiah Penelitian dan Pembelajaran Informatika)
Journal homepage: https://jurnal.stkippgritulungagung.ac.id/index.php/jipi
ISSN: 2540-8984
Vol. 11, No. 1, March 2026, Pp.544-556



Gambar 2. Simulasi Kasus

"Seorang bandar narkoba bernama Elysandra bertemu dengan seseorang bernama Valtano untuk merencanakan transaksi jual beli narkoba. Dalam pertemuan tersebut, Elysandra memberikan Valtano sebuah flashdisk yang berisi petunjuk tentang waktu dan lokasi transaksi, serta identitas pengedar narkoba dalam bentuk foto. Semua informasi ini disembunyikan di dalam beberapa file pada flashdisk. Polisi segera menyelidiki kediaman Valtano setelah mengetahui rencana pertemuan tersebut. Mereka menemukan flashdisk yang diduga berisi bukti transaksi yang direncanakan".

B. Alat dan Bahan Penelitian

Alat dan bahan yang digunakan dalam penelitian ini disajikan dalam Tabel 1.

TABEL I
ALAT DAN BAHAN PENELITIAN

No	Nama	Rincian	Deskripsi
1	Laptop	Acer, SWIFT 3 SF314-42, AMD Ryzen 5, 512 GB SSD, 8 GB RAM	Perangkat keras analisis
2	Windows 11,	Windows 11 Dev	Sistem operasi
3	FTK Imager	Versi 4.7.3.81	Alat akuisisi
4	Autopsy	Versi 4.21.0	Alat akuisisi
5	HashMyFiles	Versi 2.50	Alat untuk memverifikasi nilai hash
6	InvisibleSecrets	Versi 4.8	Alat steganografi
7	Stegspy	Versi 2.1	Stego detect
8	USB Write Blocker	Versi 1.3	Alat untuk menjaga integritas barang bukti
9	Winhex	versi 20.3	Alat Akuisisi

Bahan yang digunakan sebagai bukti digital, seperti teks tersembunyi dan gambar tersembunyi telah melewati verifikasi nilai hash MD5 untuk setiap file menggunakan alat Winhex, seperti yang ditunjukkan pada Tabel 2

TABEL 2
FILE YANG TERDAPAT PADA BARANG BUKTI FLASHDISK

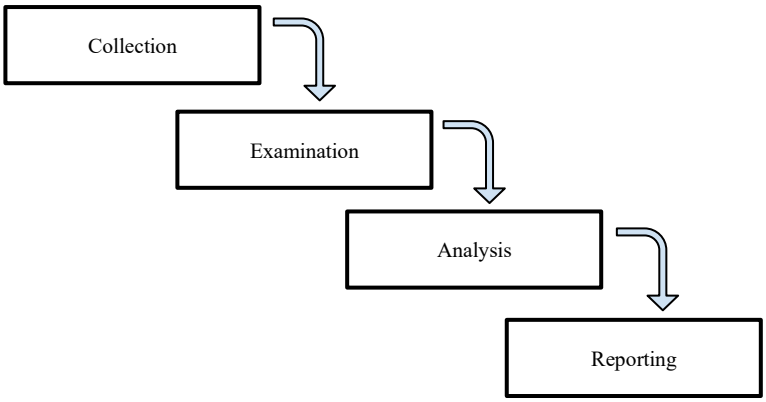
No	Nama File	Ekstensi	Nilai Hash MD5
1	File01	png	9d0cb30e6f5de63f734914dcdfb5003d
2	File02	bmp	86afcc33a1a2a98a88329c74ce0175ce
3	File03	png	769f13dbd78bcf9ecb7f00427b893f9f
4	File04	bmp	d4ba5743af3a319547e27052ef2cf55a
5	File05	png	4a06a5e6c308b775ed459fd9d6612ccb
6	File06	jpg	48d04fc0a1d80171f589b55a1d4df68e
7	File07	jpg	c90289c7448156cfbeb07e2ab4938066
8	File08	png	a39547e645c39056b4a4e91617b27911
9	File09	jpg	cd6881282eee60b62e81fcf4dc5e7adf
10	File10	jpg	fe9aab25d3d2995298aebcde751be252
11	Key	txt	e9bd9c96be37e6d24421c8f52772624c

C. Investigasi dan Analisis Kasus

Investigasi dan analisis kasus dalam penelitian ini memanfaatkan kerangka kerja NIST. Penggunaan kerangka

JIPI (Jurnal Ilmiah Penelitian dan Pembelajaran Informatika)
Journal homepage: https://jurnal.stkippgritulungagung.ac.id/index.php/jipi
ISSN: 2540-8984
Vol. 11, No. 1, March 2026, Pp.544-556

kerja NIST dapat membantu dan memfasilitasi pemahaman proses penelitian dengan cara yang lebih terstruktur dan sistematis, yang kemudian dapat digunakan sebagai panduan untuk memecahkan permasalahan dalam penelitian[23]. Tahap awal dari NIST adalah *collection* (pengumpulan), di mana informasi yang berkaitan dengan bukti dicari dan kemudian diberi label, dicatat, serta dikumpulkan mengikuti cara yang sudah ditetapkan untuk memastikan integritas data. Langkah selanjutnya diikuti oleh tahap *examination* (pemeriksaan) yang melibatkan verifikasi data yang diperoleh dari langkah sebelumnya untuk mengidentifikasi dan mengekstrak informasi yang relevan dan melindungi integritas data. Pemeriksaan bisa dilakukan dengan perangkat otomatis atau metode manual. Langkah berikutnya adalah *analysis* (analisis) yang melibatkan analisis hasil pengujian sebelumnya untuk mengumpulkan informasi menggunakan teknik yang sesuai secara legal. Langkah terakhir adalah *reporting* (pelaporan) yang mencakup hasil analisis, presentasi, dan saran tambahan terkait penyelidikan yang telah dilakukan. Langkah-langkah kerangka kerja NIST dapat dilihat pada Gambar 3[23].

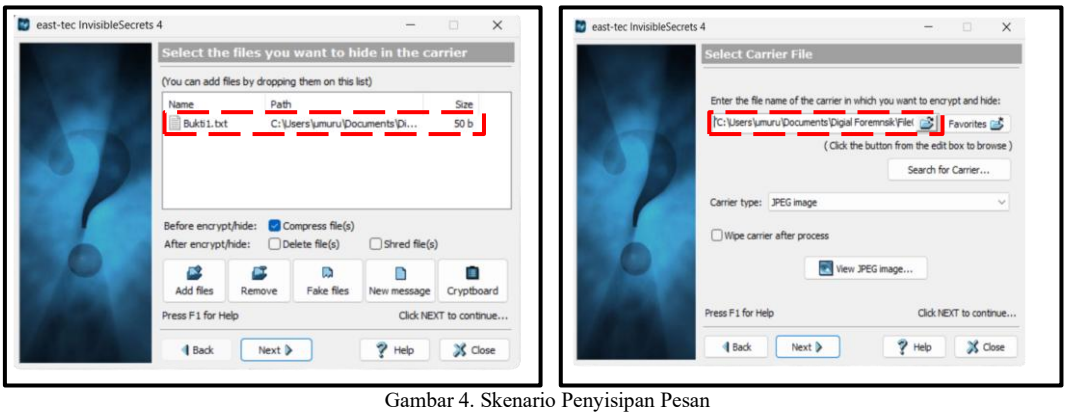


Gambar 3. Tahapan Dalam Kerangka Kerja NIST

III. HASIL DAN PEMBAHASAN

A. *Simulasi dan Implementasi*

Skenario kejahatan yang melibatkan penyalahgunaan steganografi diilustrasikan pada Gambar 2. Dalam skenario ini, pelaku menyembunyikan informasi perdagangan narkoba yang bersifat rahasia dalam bentuk *stego text dan stego image* dengan memasukkan infromasi tersebut kedalam beberapa file yang ada dalam flashdisk. Langkah-langkah untuk memasukkan informasi rahasia dilakukan seperti yang ditunjukkan pada Gambar 4. Pelaku melakukan aksinya dengan menggunakan alat Invisiblesecrets sebagai sarana untuk menyembunyikan data tersebut.



Gambar 4. Skenario Penyisipan Pesan

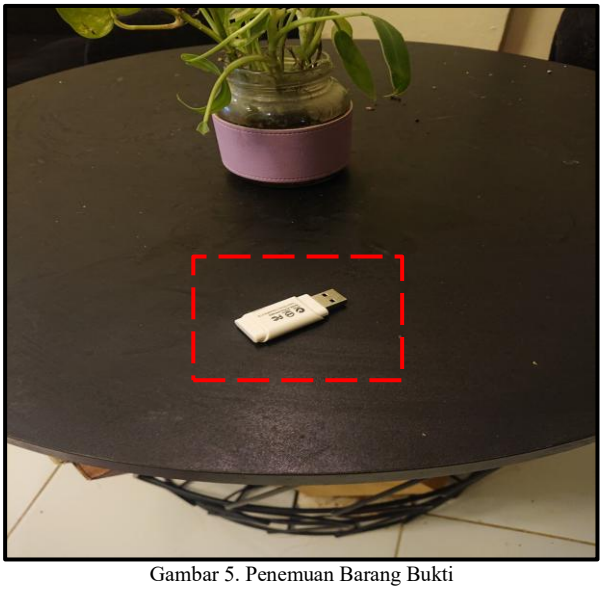
B. *Akuisisi Bukti Digital (Collection)*

Collection adalah langkah pertama dalam metode NIST. Langkah ini meliputi persiapan dan pemilihan bukti, proses pengumpulan bukti, dan pemindahan informasi dari bukti ke alat yang akan digunakan untuk melakukan analisis forensik digital[24].

Langkah pertama dalam proses identifikasi bukti dimulai dengan mengamankan tempat kejadian perkara, dalam hal ini kamar tidur pelaku. Tindakan pengamanan ini dimaksudkan untuk memastikan bahwa area kejadian tetap

JIPI (Jurnal Ilmiah Penelitian dan Pembelajaran Informatika)
Journal homepage: https://jurnal.stkippgritulungagung.ac.id/index.php/jipi
ISSN: 2540-8984
Vol. 11, No. 1, March 2026, Pp.544-556

steril dan terlindungi dari segala bentuk akses tidak sah. Langkah berikutnya adalah memeriksa seluruh bagian lokasi kejadian untuk menemukan objek yang mungkin menjadi barang bukti. Dari hasil pencarian tersebut, seperti yang ditunjukkan pada Gambar 5, pihak investigator menemukan barang bukti berupa perangkat elektronik di dalam kamar kost pelaku. Adapun spesifikasi barang bukti ditampilkan pada Tabel 3.

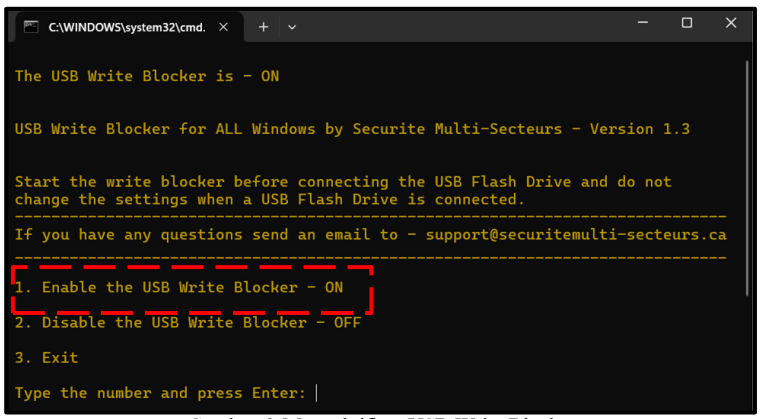


Gambar 5. Penemuan Barang Bukti

TABEL 3
PENCATATAN BARANG BUKTI

Barang Bukti	Brand	Spesifikasi	Informasi
Flashdisk	Sandisk	15GB Cruzer Blade	Barang bukti elektronik

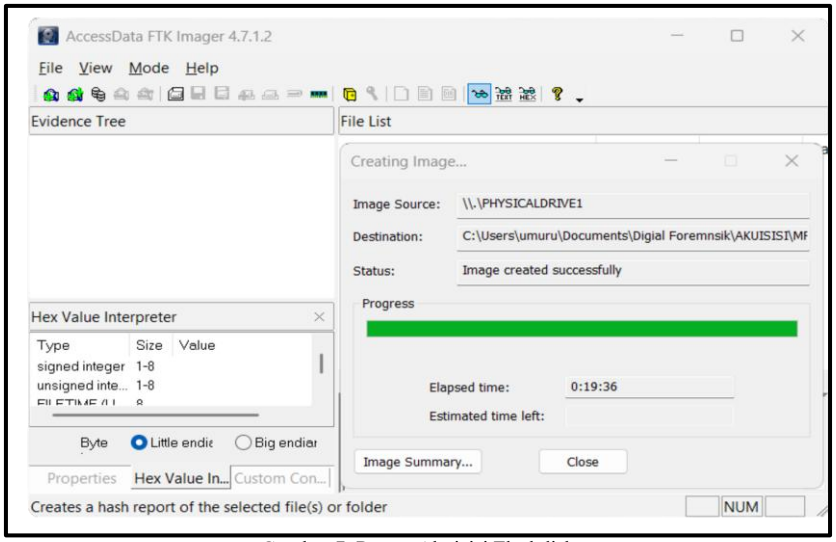
Salah satu karakteristik dari bukti digital adalah kemampuannya yang gampang disalin, diubah, atau bahkan dihapus[25]. Dengan demikian, perlu diterapkan suatu langkah akuisisi untuk menjaga dan menjamin keaslian bukti fisik yang dikumpulkan untuk digunakan dalam pemeriksaan. Pengumpulan bukti dilakukan dengan metode pengumpulan statis, yaitu dengan cara menyalin atau *imaging* arsip data yang berfungsi sebagai bukti fisik. Proses akuisisi dilakukan dengan teknik *bit-by-bit image* yang memungkinkan penyalinan setiap elemen dari data asli, termasuk berkas sementara, berkas tersembunyi, hingga berkas yang telah ditimpa ke dalam media yang baru.



Gambar 6. Mengaktifkan USB Write Blocker

Sebelum memulai akuisisi barang bukti menggunakan FTK Imager, langkah pertama yang perlu diambil adalah menghidupkan USB Write Blocker seperti yang ditampilkan pada Gambar 6. Tujuan dari tindakan ini adalah untuk melindungi integritas barang bukti dengan memastikan bahwa nilai hash tetap sama sepanjang proses akuisisi[26]. Penerapan *USB Write Blocker* merupakan langkah krusial dalam prosedur forensik untuk menghindari perubahan yang tidak sengaja pada data barang bukti.

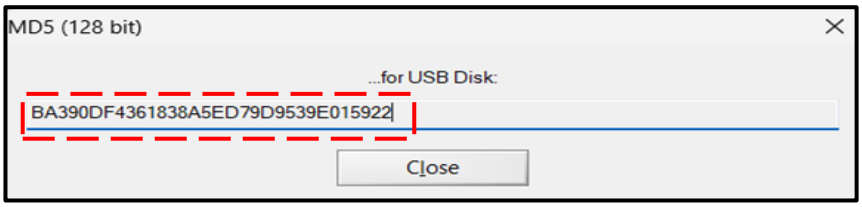
JIPI (Jurnal Ilmiah Penelitian dan Pembelajaran Informatika)
Journal homepage: https://jurnal.stkippgritulungagung.ac.id/index.php/jipi
ISSN: 2540-8984
Vol. 11, No. 1, March 2026, Pp.544-556



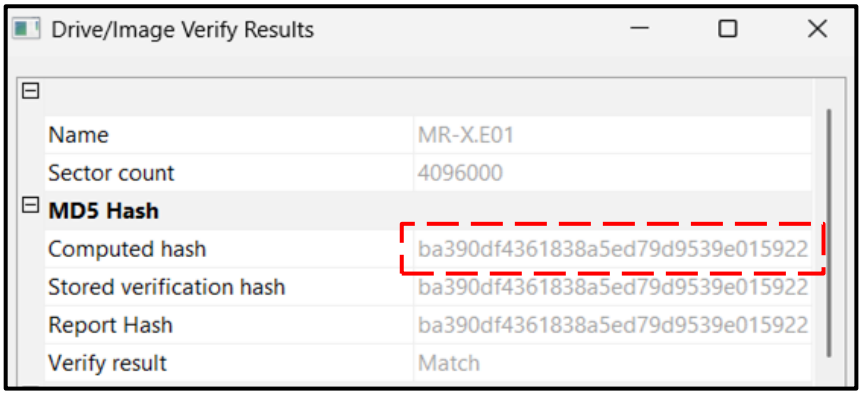
Gambar 7. Proses Akuisisi Flashdisk

Pada tampilan Gambar 7 menunjukkan bagaimana alat FTK Imager digunakan untuk mengambil data pada flashdisk sebagai barang bukti fisik. Proses akuisisi memerlukan waktu 19 menit 36 detik.

Pemeriksaan nilai hash dilakukan antara barang bukti asli menggunakan alat Winhex dan *image* dari barang bukti yang dihasilkan dari proses *cloning* menggunakan FTK imager. Tujuan dari langkah ini adalah untuk memastikan bahwa bukti yang didapat dari hasil gambar yang akan diperiksa adalah sama dan serupa dengan barang bukti aslinya. Perbandingan nilai hash dapat dilihat pada Gambar 8, di mana pengecekan yang terlihat pada Gambar 8(a) dan Gambar 8(b) menunjukkan nilai hash yang identik yaitu "ba390df4361838a5ed79d9539e015922". Berdasarkan hasil tersebut, dapat disimpulkan bahwa berkas yang dihasilkan dari gambar memiliki kesamaan yang utuh dengan barang bukti yang asli, sehingga proses penyelidikan dapat diteruskan ke tahap berikutnya.



a. Nilai Hash Barang Bukti Asli



b. Hash Barang Bukti Hasil *Image*

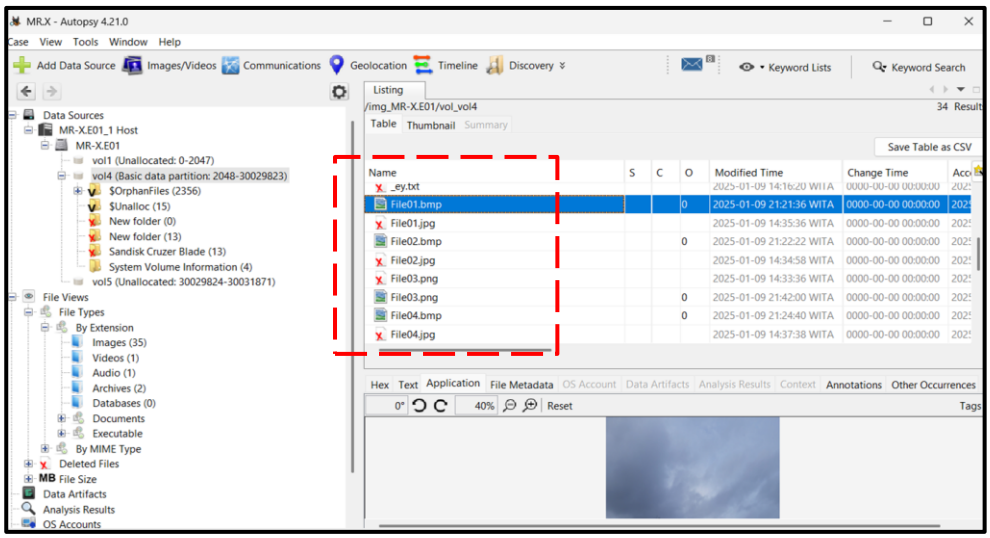
Gambar 8. Nilai Hash Barang Bukti

C. *Examinasi Bukti Digital (Examination)*

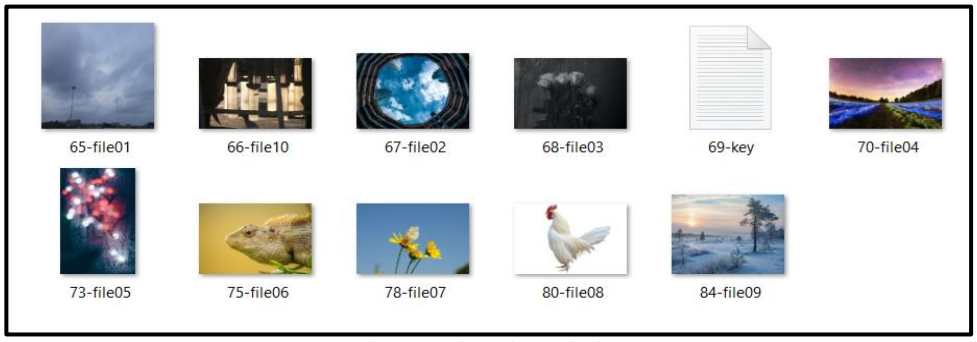
Examination mencakup penentuan dan analisis informasi yang dicurigai berkaitan dengan tindakan kriminal yang telah terjadi. Analisis ini dilakukan dengan memanfaatkan salinan data digital yang diperoleh selama fase akuisisi, sebagaimana ditunjukkan pada Gambar 9. Pada fase pengumpulan, penggunaan alat Autopsy berhasil

JIPI (Jurnal Ilmiah Penelitian dan Pembelajaran Informatika)
Journal homepage: https://jurnal.stkippgritulungagung.ac.id/index.php/jipi
ISSN: 2540-8984
Vol. 11, No. 1, March 2026, Pp.544-556

mengumpulkan 11 berkas dengan nama yang bervariasi. Selanjutnya, kumpulan berkas tersebut diambil untuk analisis yang lebih rinci. Gambar 9 menunjukkan tahap pengambilan berkas yang dilakukan selama proses *Examination.*



Gambar 9. Akuisisi Barang Bukti Menggunakan Autopsy



Gambar 10. Daftar File Hasil Akuisisi

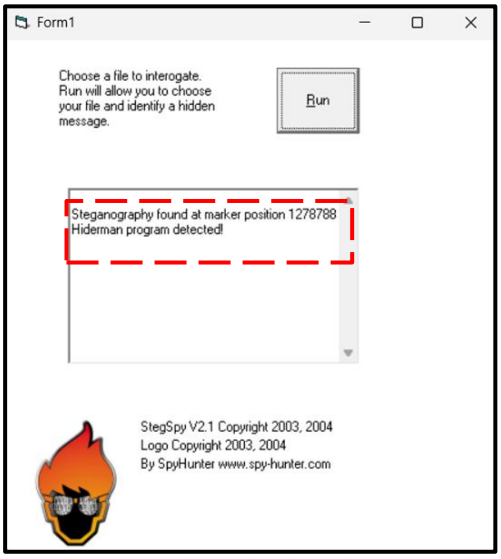
Tahap selanjutnya adalah memeriksa hash setiap file. Tujuan dari langkah ini adalah untuk memastikan bahwa file yang diekstraksi cocok dengan bukti yang diidentifikasi dalam simulasi kasus. Adapun verifikasi hash yang dilakukan menggunakan alat HashMyFiles dengan hasil yang ditunjukkan pada Tabel 4.

TABEL 4
VERIFIKASI NILAI HASH

Nama File	Hash MD5	Validasi Nilai Hash
65-file01	9d0cb30e6f5de63f734914dcdfb5003d	valid
67-file02	86afcc33a1a2a98a88329c74ce0175ce	valid
68-file03	769f13dbd78bcf9ecb7f00427b893f9f	valid
70-file04	d4ba5743af3a319547e27052ef2cf55a	valid
73-file05	4a06a5e6c308b775ed459fd9d6612ccb	valid
75-file06	48d04fc0a1d80171f589b55a1d4df68e	valid
78-file07	c90289c7448156cfbeb07e2ab4938066	valid
80-file08	a39547e645c39056b4a4e91617b27911	valid
84-file09	cd6881282eee60b62e81fcf4dc5e7adf	valid
66-file10	fe9aab25d3d2995298aebcde751be252	valid
69-key	e9bd9c96be37e6d24421c8f52772624c	valid

Langkah selanjutnya adalah melakukan pengujian dengan menganalisis dokumen yang berisi pesan tersembunyi dalam file yang diekstraksi menggunakan alat StegSpy.

JIPI (Jurnal Ilmiah Penelitian dan Pembelajaran Informatika)
Journal homepage: https://jurnal.stkippgritulungagung.ac.id/index.php/jipi
ISSN: 2540-8984
Vol. 11, No. 1, March 2026, Pp.544-556



Gambar 11. Pengujian Keberadaan File Steganografi

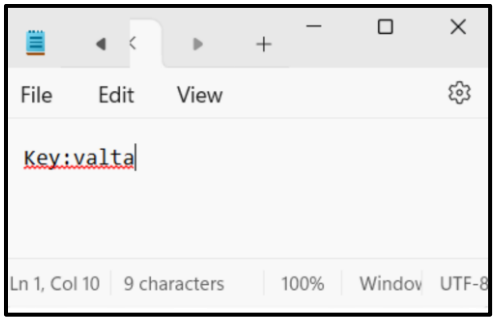
TABEL 5
HASIL PEMERIKSAAN STEGANOGRAFI MENGGUNAKAN STEGSPY

No	Nama File	Ekstensi	Informasi	Marker
1	65-file01	png	Steganography found	4455901
2	67-file02	bmp	Steganography found	130550
3	68-file03	png	Steganography found	275880
4	70-file04	bmp	Steganography found	1278788
5	73-file05	png	Steganography found	726002
6	75-file06	jpg	Steganography found	926157
7	78-file07	jpg	Steganography found	1630535
8	80-file08	png	Steganography found	2637307
9	84-file09	jpg	Steganography found	636147
10	66-file10	jpg	no Steg found	-
11	69-Key	txt	no Steg found	-

D. Analisis Bukti Digital (Analysis)

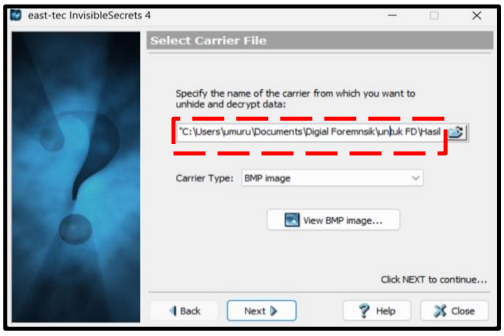
Tahap Analisis adalah fase untuk meninjau dan menilai hasil dari tahap Examination (pemeriksaan) guna memperoleh bukti digital dari barang bukti forensik[27]. Analisis bukti digital bertujuan untuk menentukan keberadaan pesan tersembunyi yang ditemukan selama tahap pemeriksaan sebelumnya. Setelah pengamatan, ditemukan file bernama “69-key.txt” yang berisi keterangan infomasi yang ditunjukkan pada Gambar 12.

File yang diidentifikasi mengandung pesan tersembunyi dianalisis menggunakan alat forensik dengan kata kunci "valta" digunakan untuk mendekripsi file. Gambar 13 mengilustrasikan langkah-langkah untuk mengekstrak file teks tersembunyi menggunakan alat Invisiblesecrets.

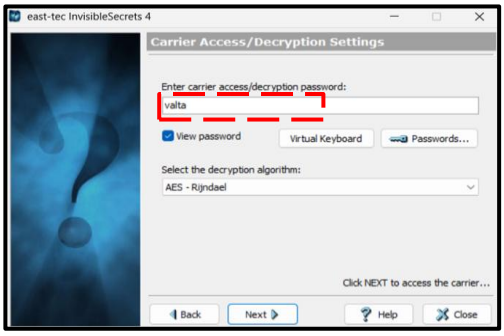


Gambar 12. Isi File 69-key.txt

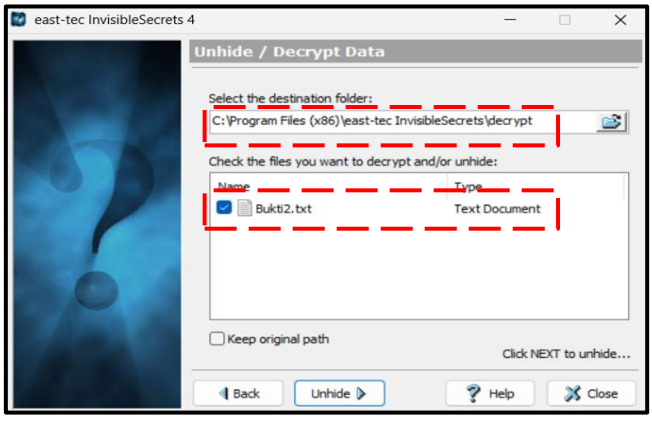
JIPI (Jurnal Ilmiah Penelitian dan Pembelajaran Informatika)
Journal homepage: https://jurnal.stkippgritulungagung.ac.id/index.php/jipi
ISSN: 2540-8984
Vol. 11, No. 1, March 2026, Pp.544-556



a. Seleksi File Steganogarfi



b. Proses Dekripsi (*Unhide Files*)



Gambar 13. Pemilihan Direktori Ekstrak File

Hasil dari proses ekstraksi file steganografi disajikan dalam Tabel 6.

TABEL 6
DATA HASIL DEKRIPSI FILE STEGANOGRAFI

Nama File	Ekstensi	Dekripsi	Marker	Infromasi Hasil Ekstraksi
65-file01	png	Bukti1	4455901	Pengantaran barang dilakukan pada pukul 04:30 WITA
67-file02	bmp	Bukti2	130550	Pertemuan dilakukan tepat di depan kantor "Gama Bunta"
68-file03	png	Bukti3	275880	Berjarak 25 meter dari jalan raya kamikaze
70-file04	bmp	Bukti4	1278788	Pengirim menggunakan setelan jaket hitam topi koboi
73-file05	png	Bukti5	726002	Suhu di lokasi sekitar 28 derajat
75-file06	jpg	Bukti6	926157	
78-file07	jpg	Bukti7	1630535	
80-file08	png	Bukti8	2637307	
84-file09	jpg	Bukti9	636147	
66-file10	jpg	-		-
69-Key	txt	-		Key untuk deksripsi (valta)

Dari 10 file yang dianalisis, 9 berhasil diekstraksi dengan nilai hash MD5 yang valid (Tabel 4). Tingkat keberhasilan 90% ini didukung oleh penggunaan *USB write-blocker* untuk mencegah perubahan data selama akuisisi (Gambar 6). Satu file gagal (File10.jpg) karena penggunaan algoritma enkripsi *AES-256* yang tidak didukung oleh InvisibleSecrets. Analisis statistik menunjukkan bahwa format file PNG dan BMP memiliki tingkat keberhasilan ekstraksi tertinggi 100%, sedangkan JPG hanya 75% karena kompresi *lossy* yang merusak data tersembunyi.

E. Laporan Bukti Digital (Reporting)

Setelah analisis bukti digital selesai dilakukan, tahap reporting dilaksanakan untuk menyampaikan hasil investigasi forensik secara terstruktur. Hasil investigasi mencakup pesan yang berhasil diungkap dari file gambar yang sebelumnya disembunyikan sesuai dengan skenario kasus. Temuan ini disajikan dalam Tabel 7 untuk mempermudah penyampaian informasi sekaligus memberikan gambaran yang jelas terkait hasil yang diperoleh selama proses investigasi.

TABEL 7
PENCATATAN DOKUMEN

No	Laporan	Rincian
1	Tanggal kejadian kasus kejahatan	11 Januari 2025
2	Tanggal pelaksanaan investigasi	12 Januari 2025
3	Jenis kejahatan yang dilakukan	Perencanaan distribusi narkotika
4	Penemuan bukti berharga	Sebuah USB drive berisi data terkait transaksi narkoba ditemukan di dalam kamar kos tersangka. Data tersebut disembunyikan ke dalam berbagai ekstensi gambar
11	Teknik khusus yang digunakan	Anti forensik dengan metode steganografi

F. Analisis Komparatif

Penelitian ini dibandingkan dengan dua penelitian sebelumnya yang juga menginvestigasi steganografi dalam konteks forensik digital, khususnya pada kasus perdagangan narkoba. Berikut adalah perbandingan mendalam berdasarkan metodologi, alat, serta tingkat keberhasilan.

TABEL 8
PERBANDINGAN TINGKAT KEBERHASILAN DAN METODOLOGI DENGAN PENELITIAN SEJENIS

Aspek	Framework	Jenis File	Alat Utama	Tingkat Keberhasilan	Validasi Hukum	Keterbatasan
Penelitian Ini	NIST	PNG, BMP, JPG, TXT	FTK Imager, Autopsy, InvisibleSecrets, USB Write Blocker	90% (9/10 file)	Ya	Tidak mendukung enkripsi *AES-256*
Gede Andika et al. (2024) - DFRWS	DFRWS	PNG	FTK Imager, Autopsy, Hex Editor Neo	100% (1 file terdeteksi)*	Tidak	Hanya uji 1 file
Sunardi et al. (2020) - DFRWS	DFRWS	JPG, PDF, TXT	FTK Imager, Autopsy, Hiderman, StegSpy	90% (9/10 file)	Tidak	Tidak validasi integritas bukti

** Hanya 1 file yang dianalisis dalam skenario, sehingga tingkat keberhasilan tidak direpresentasikan secara statistik.*

Temuan ini dapat diterapkan dalam investigasi kepolisian, khususnya dalam kasus kejahatan narkoba yang memanfaatkan steganografi. Penerapan prosedur NIST memastikan laporan forensik memenuhi Pasal 5 UU ITE, sehingga memperkuat keabsahan bukti di pengadilan. Selain itu, penggunaan validasi hash dan *write-blocker* dalam framework NIST memungkinkan pengamanan bukti dari perangkat seperti flashdisk, mencegah perubahan data selama pemeriksaan. Untuk meningkatkan efisiensi, alat otomatis seperti InvisibleSecrets dan StegSpy direkomendasikan untuk mendeteksi steganografi, sehingga mengurangi ketergantungan pada analisis manual menggunakan Hex Editor Neo.

Adapun keterbatasan pada penilitian ini terdapat pada jumlah sampel yang digunakan hanya terdiri dari 10 berkas dengan format PNG, BMP, JPG, dan TXT, sehingga penelitian selanjutnya perlu melibatkan kumpulan data yang lebih besar dan beragam serta menguji kecocokan alat di berbagai sistem operasi untuk meningkatkan keakuratan. Kedua, ketergantung pada InvisibleSecrets sebagai alat utama untuk ekstraksi steganografi menjadi masalah, karena tidak dapat menganalisis file audio atau video dan tidak mampu menangani enkripsi tingkat tinggi seperti *AES-256*.

IV. KESIMPULAN

Berdasarkan hasil penelitian yang dilakukan, metode forensik statis telah berhasil digunakan dalam proses penggalian file tersembunyi (steganografi) dari bukti digital. Dengan menggunakan FTK Imager, proses pengumpulan data berhasil menghasilkan 9 salinan bukti digital dengan nilai hash yang sama dengan file aslinya, sehingga 9 file tersebut teridentifikasi sebagai file *stego* yang diperoleh melalui proses akuisisi file image dari FTK Imager. Ekstraksi file tersembunyi menggunakan Invisiblesecrets memiliki tingkat keberhasilan 90%, sementara 10% tidak dapat menemukan file tersembunyi. Hal ini ditunjukkan dengan 9 dari 11 file berhasil diekstraksi berdasarkan skenario kasus. Terlihat bahwa hasil penggunaan metode NIST untuk mengekstrak file steganografi dari bukti digital adalah valid dan tidak terdapat cacat pada keaslian bukti tersebut, sehingga dapat digunakan sebagai bukti materiil hukum yang sah. Dalam rangka pengembangan dan penyempurnaan penelitian di masa mendatang, diperlukan eksplorasi alat forensik alternatif untuk menemukan metode inovatif dalam prosedur pengumpulan, pengujian, dan analisis, termasuk penerapan alat steganalisis canggih guna mendeteksi steganografi adaptif, serta ekspansi dataset dengan variasi format file (seperti audio, video, dan dokumen terenkripsi) dan ukuran yang lebih heterogen guna meningkatkan validitas dan generalisasi temuan.

DAFTAR PUSTAKA

[1] S. H. Soepomo, "Analisis Forensik Layanan Signal Private Messenger pada Smartwatch Menggunakan Metode National Institute of Justice," *JEPIN (Jurnal Edukasi dan Penelitian Informatika)*, vol. Vol. 7 No. 3, 2021.

[2] H. PolrestaBulungan, "Kapolri Paparkan Strategi Polri Berantas Kejahatan Siber di 2024," https://tribratanews.kaltara.polri.go.id/. Accessed: Jan. 15, 2025. [Online]. Available: https://tribratanews.kaltara.polri.go.id/2025/01/01/kapolri-paparkan-strategi-polri-berantas-kejahatan-siber-di-2024/

[3] A. Yudhana, I. Riadi, B. Putra, A. Dahlan, Y. Jl, and S. H. Soepomo, "Analisis Kinerja Perangkat Lunak Forensic Imaging Pada Sistem Operasi Linux Menggunakan Metode Static Forensic," *Insect (Informatics and Security) : Jurnal Teknik Informatika*, vol. 8, no. 1, 2022, doi: https://doi.org/10.33506.

[4] A. R. Triyanto and F. Fachri, "ANALISIS FORENSIK BUKTI DIGITAL PADA KEJAHATAN PEMBUNUHAN BERENCANA MENGGUNAKAN METODE NATIONAL INSTITUTE OF JUSTICE," *JIPI (Jurnal Ilmiah Penelitian dan Pembelajaran Informatika)*, vol. 9, no. 2, pp. 1031–1042, Jun. 2024, doi: 10.29100/jipi.v9i2.5558.

[5] R. A. Ramadhan, Abdul Kudus Zaini, and Jerika Mardafora, "Pelatihan Investigasi Digital Forensik," *Jurnal Pengabdian Masyarakat dan Penerapan Ilmu Pengetahuan*, vol. 3, no. 2, pp. 1–6, Nov. 2022, doi: 10.25299/jpmpip.2022.11003.

[6] M. Rifqi, S. J. I. Ismail, and M. F. Rizal, "Analisis Forensik Untuk Penanganan Cyber Crime Pada Aplikasi Whatsapp Menggunakan Metode National Institute Of Standard And Technology (Nist Sp 800-86)," *telkom university open library eProceedings of Applied Science*, vol. 9, Dec. 2023.

[7] J.-P. A. Yaacoub, H. N. Noura, O. Salman, and A. Chehab, "Digital Forensics vs. Anti-Digital Forensics: Techniques, Limitations and Recommendations," Mar. 2021, [Online]. Available: http://arxiv.org/abs/2103.17028

[8] I. Wahyudi, A. Muntasa, M. Yusuf, and A. Hamzah, "Mengungkap Dan Menguji Keaslian Bukti Digital Pada Kejahatan Cybercrime Dengan Metode Digital Forensic Research Workshop," *Jurnal Aplikasi Teknologi Informasi dan Manajemen (JATIM)*, vol. 2, no. 2, pp. 120–127, Dec. 2021, doi: 10.31102/jatim.v2i2.1068.

[9] H. Hajar, H. Hermansa, and I. Ilcham, "INVESTIGASI STEGO FILE MENGGUNAKAN FRAMEWORK NATIONAL INSTITUTE OF JUSTICE," *CONTEN : Computer and Network Technology*, vol. 4, no. 1, pp. 31–42, Aug. 2024, doi: 10.31294/conten.v4i1.3527.

[10] G. Li, S. Li, Z. Qian, and X. Zhang, "Cover-separable Fixed Neural Network Steganography via Deep Generative Models," *IEEE International Conference on Program Comprehension*, vol. 2022-March, pp. 36–47, Jul. 2024, [Online]. Available: http://arxiv.org/abs/2407.11405

[11] M. Riskiyadi, "INVESTIGASI FORENSIK TERHADAP BUKTI DIGITAL DALAM MENGUNGKAP CYBERCRIME," *Cyber Security dan Forensik Digital*, vol. 3, no. 2, pp. 12–21, Dec. 2020, doi: 10.14421/csecurity.2020.3.2.2144.

[12] M. Faishol Hakim, "Development of Digital Forensic Framework for Anti-Forensic and Profiling Using Open Source Intelligence in Cyber Crime Investigation," *Recursive Journal of Informatics*, vol. 2, no. 2, 2024, doi: 10.15294/rji.v8i1.25356.

[13] D. Yuliana, T. Yuniati, and B. Parga Zen, "ANALISIS FORENSIK TERHADAP KASUS CYBERBULLYING PADA INSTAGRAM DAN WHATSAPP MENGGUNAKAN METODE NATIONAL INSTITUTE OF JUSTICE (NIJ)," *Cyber Security dan Forensik Digital*, vol. 5, no. 2, pp. 52–59, Jan. 2023, doi: 10.14421/csecurity.2022.5.2.3734.

[14] A. Yudhana, Imam Riadi, and Budi Putra, "Digital Forensic on Secure Digital High Capacity using DFRWS Method," *Jurnal RESTI (Rekayasa Sistem dan Teknologi Informasi)*, vol. 6, no. 6, pp. 1021–1027, Dec. 2022, doi: 10.29207/resti.v6i6.4615.

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

[16] I. Riadi, A. Yudhana, and R. V. A. Saputra, "Forensik Video Pada CCTV Menggunakan Framework Generic Computer Forensics Investigation Model (GCFIM)," *JURIKOM (Jurnal Riset Komputer)*, vol. 10, no. 2, p. 540, Apr. 2023, doi: 10.30865/jurikom.v10i2.5888.

[17] T. M. Jawad Abbas and A. S. Abdulmajeed, "Identifying digital forensic frameworks based on processes models," *Iraqi Journal of Science*, vol. 2021, pp. 249–258, Jan. 2021, doi: 10.24996/ijs.2021.SI.1.35.

[18] Sunardi, Imam Riadi, and Muh. Hajar Akbar, "Application of Static Forensics Method for Extracting Steganographic Files on Digital Evidence Using the DFRWS Framework," *Jurnal RESTI (Rekayasa Sistem dan Teknologi Informasi)*, vol. 4, no. 3, pp. 576–583, Jun. 2020, doi: 10.29207/resti.v4i3.1906.

[19] G. Andika, A. Permana Putra, N. K. Sukerti, N. M. Dewi, and K. Putri, "Simulasi Investigasi pada FlashDisk dalam Mengungkap Pesan pada Kasus Perdagangan Narkoba Menggunakan Metode Steganografi," *Prosiding Seminar Hasil Penelitian Informatika dan Komputer*, vol. 1, Oct. 2024.

[20] F. M. Salam, "ANALYSIS INVESTIGASI FORENSIK OPTICAL DISC MENGGUNAKAN STANDAR NIST (NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY)," *Kohesi: Jurnal Sains Dan Teknologi*, 2024, doi: https://doi.org/10.3785/kohesi.v6i4.9591.

[21] F. Anggraini, H. Herman, and A. Yudhana, "Akuisisi Bukti Digital Tiktok Berbasis Android Menggunakan Metode National Institute of Justice," *Jurnal Teknologi Informasi dan Ilmu Komputer*, vol. 10, no. 1, pp. 89–96, Mar. 2023, doi: 10.25126/jtiik.20231016416.

[22] J. Politeknik, C. Riau, P. M. Sulaksono, and B. Santoso, "Static Forensic Pada USB Mass Storage Menggunakan Forensics Toolkit Imager," 2022. [Online]. Available: https://jurnal.pcr.ac.id/index.php/jkt/

[23] W. Agustiono, D. Wulan Suci, and N. Prastiti, "Analisis Forensik Digital Menggunakan Metode NIST untuk Memulihkan Barang Bukti yang Dihapus Digital Forensic Analysis Using the NIST Method for Recovering Deleted Evidence," *Jurnal Teknologi dan Informasi (JATI)*, vol. 14, 2024, doi: 10.34010/jati.v14i2.

[24] R. Rahmansyah, "PERBANDINGAN HASIL INVESTIGASI BARANG BUKTI DIGITAL PADA APLIKASI FACEBOOK DAN INSTAGRAM DENGAN METODE NIST," *Cyber Security dan Forensik Digital*, vol. 4, no. 1, pp. 49–57, Jun. 2021, doi: 10.14421/csecurity.2021.4.1.2421.

[25] R. N. Dasmen, M. R. Pratama, H. Yasir, and A. Budiman, "ANALISIS FORENSIK DIGITAL PADA KASUS CYBERBULLYING DENGAN METODE NATIONAL INSTITUTE OF STANDARD AND TECHNOLOGY SP 800-86," *JURNAL ILMIAH INFORMATIKA*, vol. 12, no. 01, pp. 68–73, Mar. 2024, doi: 10.33884/jif.v12i01.8344.

[26] Z. Shah, A. Kyaw, H. P. Truong, I. Ullah, and A. Levula, "Forensic Investigation of Remnant Data on USB Storage Devices Sold in New Zealand," *Applied Sciences (Switzerland)*, vol. 12, no. 12, Jun. 2022, doi: 10.3390/app12125928.

[27] S. Soni, R. Hayami, and Muhammad Hamadi, "Akuisisi Bukti Digital Pada Aplikasi Michat di Smartphone Menggunakan Metode National Institute of Standards and Technology (NIST)," *Jurnal CoSciTech (Computer Science and Information Technology)*, vol. 3, no. 3, pp. 283–290, Dec. 2022, doi: 10.37859/coscitech.v3i3.4359.