CONTEN : Computer and Network Technology
Vol. 4, No. 1, Juni 2024, hlm. 31-42

e-ISSN: 2797-5274
p-ISSN: 2809-9788

Investigasi *Stego File* Menggunakan *Framework National Institute of Justice*

Muh. Hajar Akbar[*1], Hermansa[2], Ilcham[3]

[1]Universitas Sembilanbelas November Kolaka
[2]Universitas Werisar
[3]Universitas Muhammadiyah Kendari
Email: [1]mhajarakbar@usn.ac.id, [2]hermansa@unsar.ac.id, [3]ilcham@umkendari.ac.id
***korespondensi**

Abstrak

Steganografi merupakan salah satu teknik anti-forensik yang memungkinkan pelaku kejahatan untuk menyembunyikan informasi ke dalam pesan lain, sehingga investigator akan menghadapi kesulitan dalam mendapatkan bukti informasi asli pada kejahatan tersebut. Oleh karena itu, seorang investigator dituntut untuk memiliki kemampuan menemukan serta melakukan ekstraksi dengan menggunakan alat yang tepat saat membuka pesan yang telah disisipi teknik steganografi. Penelitian ini menganalisis bukti digital menggunakan metode static forensics dengan menerapkan lima tahapan pada framework National Institute of Justice (NIJ) serta melakukan ekstraksi steganografi pada file yang telah disusupi berdasarkan skenario kasus yang melibatkan kejahatan digital. Alat yang digunakan meliputi FTK Imager, Autopsy, WinHex, Hiderman, dan StegSpy. Hasil ekstraksi menunjukkan bahwa dari 10 file yang diskenariokan telah disusupi steganografi. Dapat disimpulkan bahwa file hasil ekstraksi dari pesan steganografi dapat dijadikan bukti digital yang sah menurut hukum.

Kata kunci: *Anti forensik, steganografi, NIJ, Hiderman*

Abstract

Steganography is an anti-forensic technique that allows criminals to hide information within other messages, making it difficult for investigators to obtain the original information as evidence in criminal cases. Therefore, an investigator must have the skills to discover and extract hidden messages using appropriate tools. This study analyzes digital evidence using static forensics by applying the five stages of the National Institute of Justice (NIJ) framework and performing steganography extraction on files embedded with hidden messages based on a digital crime scenario. The tools used include FTK Imager, Autopsy, WinHex, Hiderman, and StegSpy. The extraction results show that out of 10 files embedded with steganography. It can be concluded that the extracted files from steganographic messages can be used as legitimate digital evidence in court.

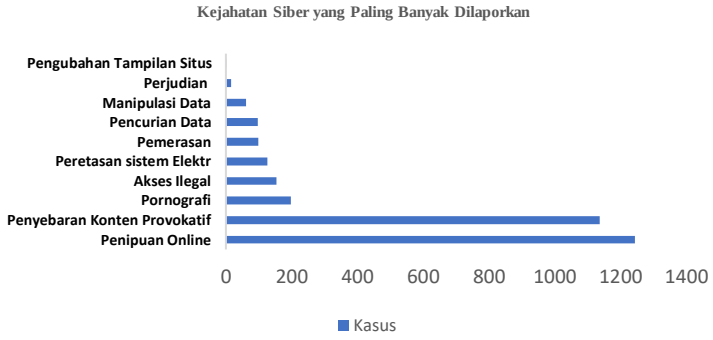
Keywords: *Anti-forensic, steganography, NIJ, Hiderman*

1. PENDAHULUAN

Kemajuan teknologi dan industri, yang merupakan hasil dari budaya manusia, selain membawa dampak positif yang dapat dimanfaatkan untuk kepentingan umat manusia, juga dapat membawa dampak negatif terhadap perkembangan dan peradaban itu sendiri [1]. Berbagai persoalan hukum yang muncul saat ini telah menyadarkan kita akan pentingnya keahlian dalam bidang forensik digital untuk mendukung investigasi dan pencarian barang bukti dalam kasus kejahatan, khususnya kejahatan di bidang komputer (*cybercrime*) [2]. Forensik digital adalah ilmu yang diterapkan untuk mengidentifikasi, mengekstraksi, menganalisis, dan menyajikan bukti digital yang tersimpan pada perangkat digital [3]. Di Indonesia,

e-ISSN: 2797-5274
p-ISSN: 2809-9788

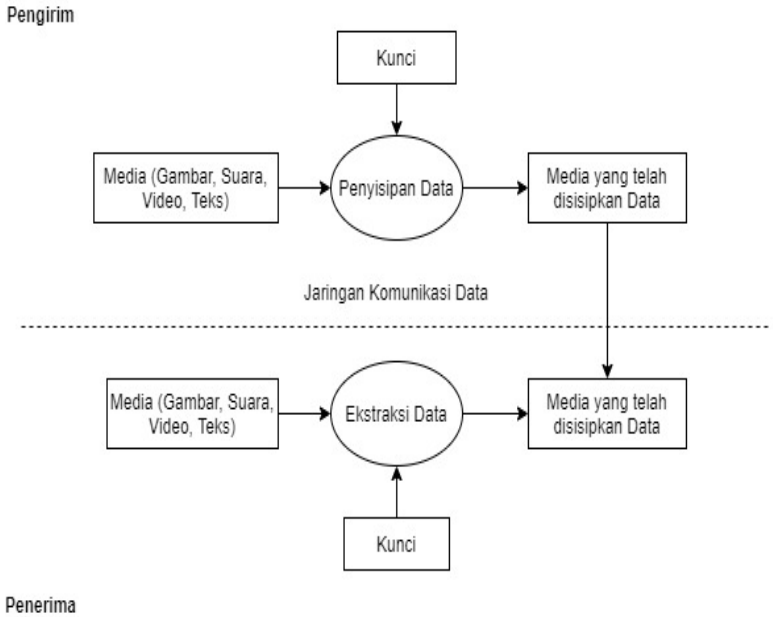
sepanjang tahun 2019, Direktorat Tindak Pidana Siber (Dittipidsiber) Bareskrim Polri menerima 3.130 kasus tindak kejahatan yang memanfaatkan teknologi komputer. Gambar 1 menunjukkan berbagai kejahatan yang paling banyak terjadi.



Gambar 1. Laporan Kasus Kejahatan Siber

Gambar 1 menunjukkan data statistik mengenai jenis-jenis kejahatan siber yang paling banyak dilaporkan. Penipuan *online* menduduki peringkat tertinggi dengan jumlah kasus mencapai sekitar 1.300. Ini diikuti oleh penyebaran konten provokatif yang mencapai hampir 600 kasus. Jenis kejahatan lainnya seperti pornografi, akses ilegal, dan peretasan sistem elektronik memiliki jumlah kasus yang lebih rendah, masing-masing berkisar antara 100 hingga 200. Jenis kejahatan seperti pemerasan, pencurian data, manipulasi data, perjudian, dan pengubahan tampilan situs menunjukkan jumlah kasus yang relatif lebih kecil, masing-masing di bawah 100 kasus. Gambar ini memberikan gambaran bahwa penipuan online dan penyebaran konten provokatif merupakan dua masalah utama dalam kejahatan siber di Indonesia pada periode tersebut.

Sebagai langkah untuk menutupi kejahatan dan menghindari deteksi oleh forensik TI, pelaku sering menggunakan teknik anti forensik yang bertujuan untuk menurunkan kualitas bukti digital sehingga menyulitkan ahli forensik dalam melakukan investigasi [4]. Salah satu teknik anti forensik yang digunakan adalah steganografi [5]. Teknik ini memungkinkan pelaku untuk menyembunyikan informasi dengan memasukkan informasi tersebut ke dalam pesan lain dalam bentuk media digital seperti teks, gambar, audio, atau video [6] sehingga keberadaan pesan tidak terdeteksi [7][8]. Gambar 2 menunjukkan proses steganografi

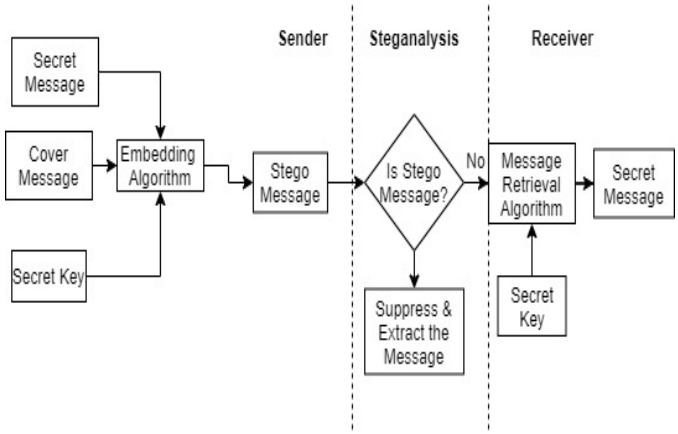


Gambar 2. Proses steganografi

e-ISSN: 2797-5274
p-ISSN: 2809-9788

Gambar 2 menunjukkan alur proses steganografi dan steganalisis. Pada bagian pengirim, proses dimulai dengan penyisipan data rahasia ke dalam media digital seperti gambar, suara, video, atau teks menggunakan kunci enkripsi. Media yang telah disisipi data tersebut kemudian dikirim melalui jaringan komunikasi data. Di sisi penerima, media yang telah disisipi data diterima dan proses ekstraksi dilakukan untuk mengeluarkan informasi rahasia dari media tersebut. Proses ekstraksi juga menggunakan kunci enkripsi yang sama atau terkait dengan kunci yang digunakan oleh pengirim. Alur ini menggambarkan bagaimana data rahasia dapat disisipkan dan diekstraksi dari media digital dalam proses steganografi dan steganalisis. Berdasarkan Gambar 2, pelaku (pengirim pesan) mengirim media yang telah disisipi informasi rahasia tersebut melalui jalur komunikasi publik, hingga dapat diterima oleh si penerima. Penerima pesan dapat mengekstraksi informasi yang ada di dalamnya [9].

Proses deteksi steganografi menjadi sangat penting dilakukan oleh investigator forensik digital untuk menanggulangi teknik steganografi [10]. Hal ini melahirkan disiplin ilmu yang disebut steganalisis [11]. Steganalisis adalah teknik untuk mendeteksi serta mengungkap keberadaan pesan rahasia yang dicurigai ada dalam media digital [12]. Selain itu, menurut [13], steganalisis dapat dijadikan pedoman untuk mengetahui dan mengevaluasi kelemahan teknik steganografi, sehingga memungkinkan proses penyisipan pesan yang lebih aman. Dalam kehidupan nyata, teknik steganalisis diterapkan untuk melacak tindakan kriminalitas, forensik komputer, maupun dalam serangan perang siber (*cyber warfare*) [14]. Gambar 3 menunjukkan cara kerja steganalisis.



Gambar 3. Blok diagram steganalisis

Gambar 3 mengilustrasikan cara kerja steganalisis dalam mendeteksi dan mengekstraksi pesan rahasia yang disisipkan dalam media digital. Proses dimulai dari sisi pengirim, di mana pesan rahasia (*Secret Message*) dimasukkan ke dalam pesan sampul (*Cover Message*) menggunakan algoritma penyisipan (*Embedding Algorithm*) dan kunci rahasia (*Secret Key*), menghasilkan pesan yang telah disisipkan (*Stego Message*). Pada tahap steganalisis, pesan yang telah disisipkan diperiksa untuk menentukan apakah pesan tersebut mengandung informasi rahasia. Jika ditemukan bahwa pesan tersebut merupakan stego message, maka pesan akan ditekan dan diekstraksi (*Suppress & Extract the Message*). Di sisi penerima, algoritma pengambilan pesan (*Message Retrieval Algorithm*) digunakan bersama dengan kunci rahasia untuk mengekstraksi pesan rahasia dari pesan yang telah disisipkan. Hasil akhir dari proses ini adalah pesan rahasia yang berhasil diekstraksi. Alur ini menunjukkan pentingnya steganalisis dalam mengidentifikasi dan memulihkan pesan rahasia dari media digital.

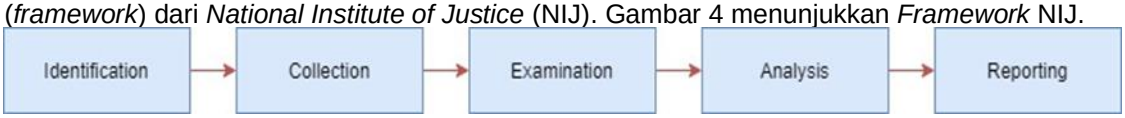
Berdasarkan latar belakang masalah tersebut, penelitian ini dilakukan dengan tujuan untuk menginvestigasi bukti digital serta mengekstraksi file yang telah disisipi pesan steganografi dengan menerapkan langkah kerja dari *National Institute of Justice* (NIJ). NIJ dipilih karena memiliki kerangka kerja forensik yang standar dan konsisten, sehingga langkah-langkah penelitian dapat diketahui secara sistematis dan dapat dijadikan pedoman dalam menyelesaikan permasalahan yang ada.

2. METODE PENELITIAN

Menurut [20], penerapan metode yang tepat dalam mengumpulkan data dapat memberikan dampak keberhasilan hingga 100%. Pada penelitian ini, metode yang digunakan untuk pengambilan bukti digital

e-ISSN: 2797-5274
p-ISSN: 2809-9788

adalah metode *static forensics*. *Static forensics* adalah teknik konvensional untuk menangani barang bukti elektronik yang berfokus pada pemeriksaan salinan duplikasi atau *image* [15]. Karena bukti digital sangat rentan terhadap perubahan data, penanganan yang ekstra hati-hati diperlukan untuk menjaga keutuhan barang bukti digital [16]. Barang bukti yang digunakan dalam penelitian ini adalah media penyimpanan berupa *flash disk* dalam keadaan mati atau tidak sedang aktif di komputer, dengan menerapkan langkah kerja (*framework*) dari *National Institute of Justice* (NIJ). Gambar 4 menunjukkan *Framework* NIJ.



Gambar 4. *Framework National Institute of Justice* (NIJ)

Langkah kerja NIJ ini terbagi menjadi lima tahapan, yaitu identifikasi, pengumpulan, Pemeriksaan, analisis, dan pelaporan [17], yang secara lengkap dipaparkan sebagai berikut:

Tahap identifikasi merupakan kegiatan pemilahan barang bukti kejahatan digital dan data-data untuk mendukung proses penyidikan dalam rangka pencarian barang bukti tersebut. Pada tahap ini, terdapat proses identifikasi, pelabelan, dan perekaman untuk menjaga keutuhan barang bukti.

Tahap pengumpulan merupakan serangkaian kegiatan untuk mengumpulkan data-data yang mendukung proses penyidikan dalam rangka pencarian barang bukti kejahatan digital. Pada tahap ini, proses pengambilan data dari sumber yang relevan dilakukan dengan menjaga integritas barang bukti dari perubahan.

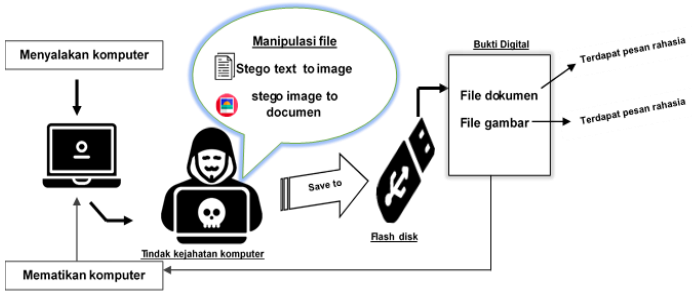
Tahap pemeriksaan merupakan tahap di mana data yang dikumpulkan diperiksa secara forensik, baik secara otomatis maupun manual, untuk memastikan bahwa data tersebut asli sesuai dengan yang ditemukan di tempat kejadian kejahatan komputer. Pada file digital, perlu dilakukan identifikasi dan validasi file dengan teknik *hash*ing.

Tahap analisis dilakukan setelah mendapatkan file atau data digital yang diinginkan dari proses pemeriksaan sebelumnya. Data tersebut kemudian dianalisis secara detail dan komprehensif dengan metode yang diakui secara teknis dan hukum untuk membuktikan keabsahannya. Hasil analisis terhadap data digital kemudian digunakan sebagai barang bukti digital yang dapat dipertanggungjawabkan secara ilmiah dan hukum.

Tahap pelaporan dilakukan setelah barang bukti digital diperoleh dari proses pemeriksaan dan analisis. Pada tahap ini, hasil analisis dilaporkan dengan mencakup penggambaran tindakan yang dilakukan, penjelasan mengenai alat dan metode yang digunakan, penentuan tindakan pendukung yang dilakukan, serta memberikan rekomendasi untuk perbaikan kebijakan, metode, alat, atau aspek pendukung lainnya dalam proses forensik digital.

2.1. PERANCANGAN SISTEM

Dalam penelitian ini, bukti digital yang digunakan tidak diperoleh dari lingkungan yang sebenarnya atau dari hasil tindak kejahatan komputer yang sebenarnya, melainkan bukti digital dibuat dan diperoleh dari hasil skenario pada tahap implementasi dan pengujian yang akan dibahas pada sub-bab tersendiri. Gambar 5 menunjukkan tahap implementasi dan pengujian forensik bukti digital ditunjukkan pada alur.



Gambar 5. Skenario Kasus Penyisipan Pesan

e-ISSN: 2797-5274
p-ISSN: 2809-9788

Kasus yang diskenariokan dalam penelitian ini adalah kasus penyisipan file berupa *stego file*, di mana investigator menemukan barang bukti berupa media penyimpanan *flash disk*. Gambar 6 menunjukkan tahapan implementasi skenario penelitian.

Gambar 6. Tahapan Skenario Kasus Penyisipan Pesan

Gambar 6 menunjukkan alur proses implementasi skenario penyisipan file steganografi pada media penyimpanan *flash disk*. Tahapan dimulai dengan menyiapkan dan menyalakan komputer. Selanjutnya, dilakukan proses penyisipan file stego menggunakan *tool* steganografi, yang kemudian disimpan pada *flash disk*. Setelah file stego disimpan, komputer dimatikan sesuai standar prosedur. Langkah terakhir adalah melepaskan *flash disk* dan melakukan proses *imaging* menggunakan komputer investigator untuk menganalisis dan memverifikasi file yang telah disisipkan. Alur ini berakhir dengan tahapan selesai, menandakan akhir dari proses implementasi skenario.

2.2. PERSIAPAN ALAT DAN BAHAN

Tabel 1 menunjukkan alat-alat yang digunakan dalam penelitian.

Tabel 1. Spesifikasi peralatan

No	Nama Alat	Spesifikasi	Keterangan
1	notebook	Acer Aspire E1-431, 4 GB DDR 3 Memory, 500 GB HDD	Perangkat keras untuk analisis bukti digital
2	Windows 10	Windows 10 Pro	System operasi
3	FTK Imager	Versi 4.2.0.13	Akuisisi tool
4	Autopsy	Versi 4.14.0	Akuisisi tool
5	Winhex	Versi 18.7	Akuisisi tool
6	Hiderman	-	Akuisisi tool
7	Stegspy	-	Steganalysis tool

Tabel 2 menunjukkan bukti digital yang digunakan berupa stego teks dan stego gambar yang telah dilakukan pengecekan nilai *hash* pada masing-masing file.

e-ISSN: 2797-5274
p-ISSN: 2809-9788

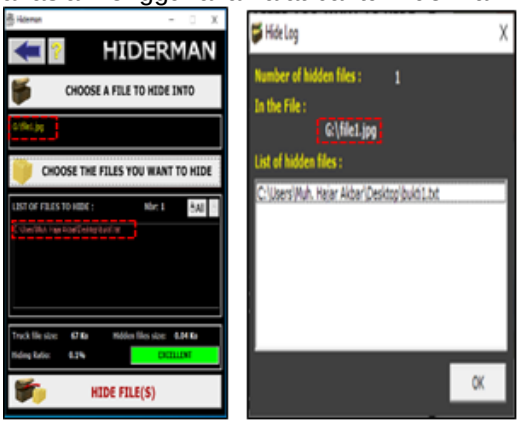
Tabel 2. Kandungan barang bukti

No	Nama File	Format	Hash
1	File1	.jpg	8e4d5a1c6bfa03dcbe860943ccc86325
2	File2	.jpg	ca8bc8529a47a6777e5d2 01deec63196
3	File3	.jpg	1Hw91XA9c1CuLKp9PhAt1ujZ963ZsagEBf
4	File4	.pdf	88568362352a9b2407650887a532c253
5	File5	.pdf	cdb792a24bdde9a8b4e61adb7bd35087
6	key	.txt	bf38a03f09a4772bc89388448d65017f

3. HASIL DAN PEMBAHASAN

3.1. Skenario dan Implementasi

Skenario kejahatan penyalahgunaan teknik steganografi dijalankan berdasarkan Gambar 2. Pelaku menyembunyikan pesan rahasia terkait transaksi jual beli narkoba dalam bentuk stego teks dan stego gambar yang disisipkan pada beberapa file dalam sebuah flash disk. Gambar 7 menunjukkan Implementasi penyisipan pesan rahasia oleh pelaku. Pelaku kejahatan melakukan aksinya dengan menyisipkan beberapa pesan rahasia menggunakan alat bantu Hiderman.



Gambar 7. Skenario penyisipan pesan

3.2. Identifikasi

Gambar 8 menunjukkan proses identifikasi barang bukti diawali dengan pengamanan TKP di kamar kos pelaku. Tujuannya adalah untuk menghindari akses masuk bagi pihak-pihak yang tidak berwenang ke tempat tersebut.

Gambar 8. Proses pengamanan TKP

Pencarian barang bukti selanjutnya dilakukan dengan memeriksa keseluruhan TKP untuk menemukan segala sesuatu yang berpotensi sebagai barang bukti. Berdasarkan hasil pencarian, pada Gambar 9, ditemukan sebuah barang bukti elektronik di atas meja ruang kerja pelaku.

e-ISSN: 2797-5274
p-ISSN: 2809-9788

Gambar 9. Penemuan barang bukti

Tabel 3 menunjukkan proses identifikasi terhadap barang bukti yang ditemukan, mencakup jenis, merk, spesifikasi, dan keterangan pendukung lainnya untuk dijadikan bukti otentik dalam proses penyidikan.

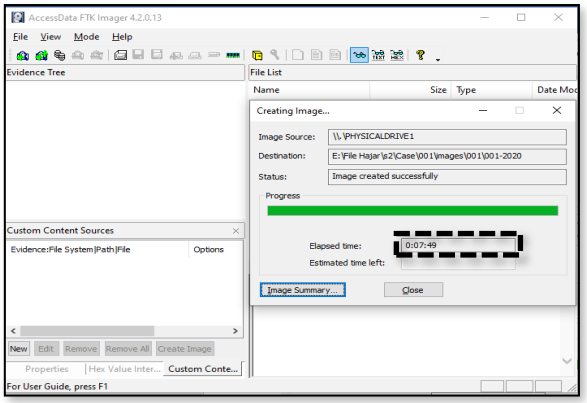
Tabel 3. Kandungan barang bukti

Barang Bukti	Merk	Spesifikasi	Keterangan
Flas disk	kingston	Data Traveler G3, 8 GB	Barang bukti elektronik

3.3. Pengumpulan

Barang bukti digital memiliki sifat mudah berubah serta berisiko hilang dan mengalami kerusakan [24]. Oleh karena itu, dilakukan proses pelestarian untuk menjaga dan mengamankan keaslian barang bukti fisik yang telah diperoleh pada tahap identifikasi, sehingga integritas data tetap terjaga sampai proses analisis dilakukan. Proses pelestarian dilakukan dengan metode *static acquisition*, yaitu melakukan *cloning* atau *imaging* terhadap media penyimpanan data (barang bukti fisik). Proses *cloning* dilakukan dengan cara *copy* data secara *bitstream image*, yaitu menyalin setiap bit dari data asli, *temporary file*, *hidden file*, bahkan file yang ter-*overwrite* pada media baru.

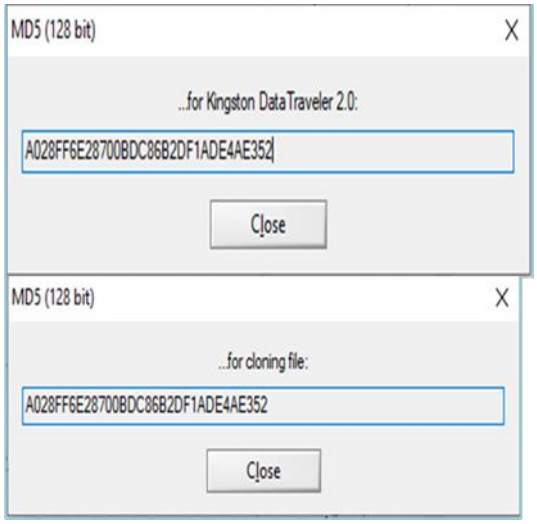
Gambar 10 menunjukkan proses pengumpulan data pada barang bukti fisik (*flash disk*) dilakukan menggunakan alat FTK Imager. Waktu yang diperlukan untuk pengumpulan data adalah 7 menit 49 detik.



Gambar 10. Proses akuisisi flash disk

Langkah selanjutnya adalah melakukan verifikasi nilai *hash* antara barang bukti asli dengan *image* barang bukti hasil dari proses *cloning*. Hal ini bertujuan untuk memastikan bahwa barang bukti hasil *cloning* yang akan diperiksa sama dan identik dengan barang bukti asli. Gambar 11 menunjukkan Perbandingan nilai *hash*. Proses verifikasi pada Gambar 8(a) dan Gambar 8(b) menunjukkan nilai *hash* identik dengan nilai yang sama, yaitu “A028FF6E28700BDC86B2DF1ADE4AE352”. Berdasarkan hasil tersebut, dapat disimpulkan bahwa file barang bukti hasil *cloning* identik dengan barang bukti aslinya, sehingga proses investigasi dapat dilanjutkan ke tahap pengumpulan.

e-ISSN: 2797-5274
p-ISSN: 2809-9788

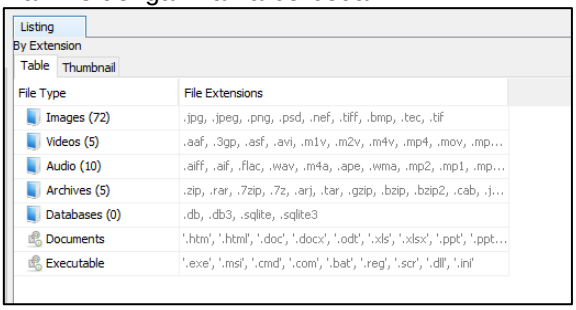


Gambar 11. Perbandingan nilai *hash*

Setelah mendapatkan salinan barang bukti berupa *image*, langkah selanjutnya adalah melakukan pengemasan terhadap barang bukti asli dengan cara menyegel serta memberikan pelabelan untuk memastikan integritasnya tetap terjaga selama pemindahan. Gambar 12 menunjukkan proses pengemasan barang bukti asli.

Gambar 12. Pengemasan barang bukti asli

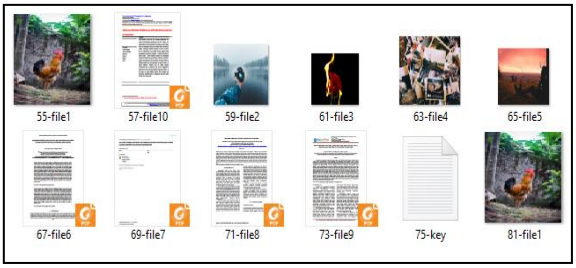
Langkah berikutnya adalah mengumpulkan data yang diyakini memiliki keterkaitan dengan kejahatan yang dilakukan. Gambar 13 menunjukkan proses pengumpulan ini dilakukan menggunakan salinan bukti digital yang telah diperoleh pada tahap akuisisi. Pengumpulan data menggunakan *tool* Autopsy berhasil mengumpulkan file dengan nama berbeda.



Gambar 13. Proses pengumpulan

Selanjutnya, dilakukan proses ekstraksi pada file tersebut untuk analisis mendalam. Gambar 14 memperlihatkan proses ekstraksi file dalam tahap pengumpulan.

e-ISSN: 2797-5274
p-ISSN: 2809-9788



Gambar 14. Proses ekstraksi

Dalam proses ini, pengumpulan data yang diyakini memiliki keterkaitan dengan kejahatan dilakukan menggunakan salinan bukti digital dari tahap akuisisi, seperti terlihat pada Gambar 10. Pengumpulan data menggunakan tool Autopsy berhasil mengumpulkan 11 file dengan nama berbeda. Selanjutnya, dilakukan proses ekstraksi pada file tersebut untuk analisis mendalam. Gambar 14 memperlihatkan proses ekstraksi file pada tahap pengumpulan. Langkah selanjutnya adalah melakukan pengecekan nilai *hash* pada setiap file. Hal ini bertujuan untuk memastikan bahwa file hasil ekstraksi sesuai dengan barang bukti yang telah diskenariokan. Proses pengecekan nilai *hash* dilakukan menggunakan *tool* hashMyFiles. Tabel 4 menunjukkan hasil pengecekan nilai *hash*.

Tabel 4. Validasi Nilai *Hash* Menggunakan *Tool Hash* my files

Nama file	Hash md5	Validasi *hash*
55-file1	8e4d5a1c6bfa03dcbe860943ccc86325	valid
59-file2	44101fb802d2854e5ab88664d8bbf70e	valid
61-file3	ca8bc8529a47a6777e5d201deec63196	valid
63-file4	1Hw91XA9c1CuLKp9PhAt1ujZ963ZsagEBf	valid
65-file5	6e389bee26d14c17a19f213a935ad426	valid
75-key	2f80636672a18eb7e1db8bf392ad2418	valid

3.4. Pemeriksaan

Proses pemeriksaan dilakukan pada file hasil ekstraksi dari proses pengumpulan untuk mengidentifikasi apakah file-file tersebut mengandung pesan rahasia yang telah disisipkan. Gambar 15 menunjukkan proses pemeriksaan. Pemeriksaan dilakukan menggunakan *tool* StegSpy pada setiap file hasil ekstraksi.

Gambar 15. Pengujian keberadaan pesan rahasia

Hasil pengujian ditampilkan pada Tabel 5. Berdasarkan hasil pengujian, ditemukan bahwa 9 file teridentifikasi mengandung pesan steganografi, sedangkan dua file lainnya tidak terdeteksi mengandung pesan steganografi.

Tabel 5. Hasil pengujian

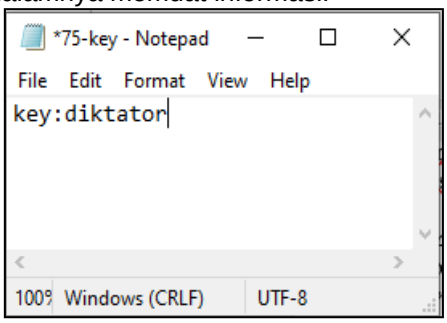
No	Nama File	Format	Keterangan	Marker
1	55-file1	.jpg	*Steganography found*	67423
2	59-file2	.jpg	*Steganography found*	22222
3	61-file3	.jpg	*Steganography found*	13481
4	63-file4	.jpg	*Steganography found*	63133
5	65-file5	.jpg	*Steganography found*	23861

e-ISSN: 2797-5274
p-ISSN: 2809-9788

6	67-file6	.pdf	*Steganography found*	1176845
7	69-file7	.pdf	*Steganography found*	272361
8	71-file8	.pdf	*Steganography found*	1555961
9	73-file9	.pdf	*no Steg found*	-
10	57-file10	.pdf	*Steganography found*	192119
11	75-key	.txt	*no Steg found*	-

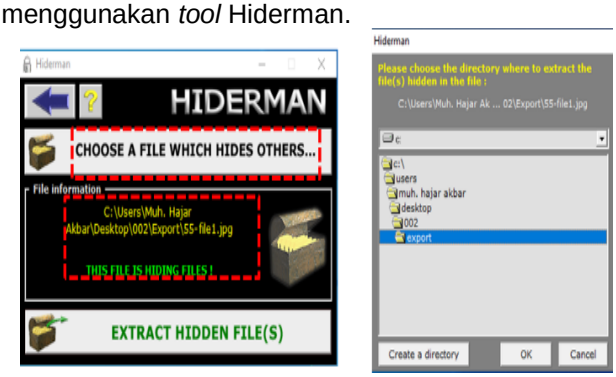
3.5. Analisis

Proses analisis dilakukan untuk mengungkap keberadaan pesan steganografi yang telah terdeteksi pada tahap pemeriksaan. Setelah dilakukan pengamatan, Gambar 15 meperlihatkan ditemukan satu file dengan nama 75-key.txt yang di dalamnya memuat informasi.



Gambar 16. Isi file 75-key.txt

File yang terdeteksi mengandung pesan steganografi dianalisis menggunakan *tool* forensik untuk mendekripsi file steganografi dengan menggunakan kunci "diktator". Gambar 17 menunjukkan proses ekstraksi file steganografi menggunakan *tool* Hiderman.



Gambar 17. Proses dekripsi (*Unhide Files*)

Berdasarkan hasil pada tahap analisis, Tabel 6 menunjukkan laporan yang disajikan dengan memberikan informasi.

Tabel 6. Hasil pengujian

Nama	Format	Dekripsi	Format	Keterangan
55-file1	.jpg	bukti1	67423	Pengantaran barang dilakukan pukul 02:30
59-file2	.jpg	Bukti2	22222	bertemu di depan kantor Maju Bersama
61-file3	.jpg	Bukti3	13481	30 meter dari jalan utaãa
63-file4	.jpg	Bukti4	63133	pengirim memakai kacamata hitam
65-file5	.jpg	Bukti5	23861	160ºC0
67-file6	.pdf	Bukti6	1176845	
69-file7	.pdf	Bukti7	272361	
71-file8	.pdf	Bukti8	1555961	
73-file9	.pdf	-	-	-

e-ISSN: 2797-5274
p-ISSN: 2809-9788

57-file10	.pdf	bukti10	192119	
75-key	.txt			Key untuk dekripsi (diktator)

3.6. Laporan

Berdasarkan hasil pada tahapan analisis, Tabel 7 menunjukkan penyajian laporan dengan cara memberikan informasi.

Tabel 7. Penyajian laporan

No	Informasi	Keterangan
1	Waktu terjadinya kasus kejahatan	19 April 2020
2	Waktu proses investigasi dilakukan	20 April 2020
3	Kejahatan yang dilakukan	Perencanaan transaksi jual beli narkoba
4	Penemuan bukti yang berharga	Flash disk Informasi mengenai transaksi jual beli narkoba yang disembunyikan pada file biasa
5	Teknik khusus yang digunakan	Anti forensik (steganografi)

4. KESIMPULAN

Berdasarkan hasil penelitian yang telah dilakukan, proses ekstraksi file steganografi pada bukti digital berhasil diterapkan dengan baik menggunakan metode *static forensics*. Proses akuisisi data menggunakan FTK Imager berhasil memperoleh 9 salinan bukti digital dengan nilai *hash* identik dengan file aslinya, sehingga ditemukan 9 file yang dideteksi sebagai file steganografi. Proses ekstraksi file steganografi menggunakan Hiderman menunjukkan tingkat keberhasilan sebesar 90%, dengan 10% tidak ditemukan file steganografi. Hal ini dibuktikan dengan berhasilnya proses ekstraksi terhadap 9 dari 11 file yang diskenariokan telah disusupi pesan rahasia. Oleh karena itu, dapat disimpulkan bahwa hasil ekstraksi file steganografi pada bukti digital dapat dijadikan bukti yang sah menurut hukum. Untuk pengembangan lebih lanjut dan penyempurnaan penelitian ini, dimungkinkan untuk menggunakan alat forensik yang berbeda agar mendapatkan metode alternatif dalam proses identifikasi, pengumpulan, pemeriksaan, dan pelaporan, serta dalam proses ekstraksi file steganografi menggunakan aplikasi selain Hiderman.

REFERENSI

[1] Fediro, B., & Tata Sutabri. (2023). RANCANG BANGUN SISTEM PELAPORAN INSIDEN KEJAHATAN SIBER. Jurnal Informatika Teknologi Dan Sains (Jinteks), 5(1), 38-43. https://doi.org/10.51401/jinteks.v5i1.2210 Geiger, M. A. and S. M. Ogilby. 2000. The First Course in Accounting: Students Perceptions and their Effect on the Decision to Major in Accounting. *Journal of Accounting Education*, 18, 63-78.

[2] Subektiningsih, S., & Hariyadi, D. (2022). The Role of Digital Forensic Experts in Cybercrime Investigations in Indonesia Based on The Scopus Research Index. Building of Informatics, Technology and Science (BITS), 4(3), 1665−1670. https://doi.org/10.47065/bits.v4i3.2638

[3] Alghamdi, M. (2021). digital forensics in cyber security—recent trends, threats, and opportunities.. https://doi.org/10.5772/intechopen.94452

[4] Baskoro, A., Cahyani, N., & Putrada, A. (2020). Analysis of voice changes in anti forensic activities case study: voice changer with telephone effect. International Journal on Information and Communication Technology (Ijoict), 6(2), 64-77. https://doi.org/10.21108/ijoict.v6i2.508

[5] Akbar, M. and Riadi, I. (2020). Analysis of steganographic on digital evidence using general computer forensic investigation model framework. International Journal of Advanced Computer Science and Applications, 11(11). https://doi.org/10.14569/ijacsa.2020.0111141

[6] Azizan, N. (2022). File hiding web application (fhwa) using image steganography.. https://doi.org/10.15405/epms.2022.10.56

[7] Pevnev, V. and Voikov, Y. (2020). Research and prototyping methods of steganography using mosaic. Advanced Information Systems, 4(2), 137-141. https://doi.org/10.20998/2522-9052.2020.2.20

[8] Sulong, G. and Wimmer, M. (2023). Image hiding by using spatial domain steganography. Wasit Journal of Computer and Mathematics Science, 2(1), 25-29. https://doi.org/10.31185/wjcm.110

[9] Fateh, M., Rezvani, M., & Irani, Y. (2021). A new method of coding for steganography based on lsb matching revisited. Security and Communication Networks, 2021, 1-15. https://doi.org/10.1155/2021/6610678

e-ISSN: 2797-5274
p-ISSN: 2809-9788

[10] Lwowski, J., Corley, I., & Hoffman, J. (2020). Neural steganalysis with spatial rich models for image steganography detection.. https://doi.org/10.36227/techrxiv.11949762
[11] Lokman, S., Ismail, A., & Din, R. (2020). Analysis review on linguistic steganalysis. Indonesian Journal of Electrical Engineering and Computer Science, 17(2), 950. https://doi.org/10.11591/ijeecs.v17.i2.pp950-956
[12] Hidayasari, N., Riadi, I., & Prayudi, Y. (2020). steganalysis using yedrodj-net net's convolutional neural networks (cnn) method on steganography tools. Proceeding International Conference on Science and Engineering, 3, 207-211. https://doi.org/10.14421/icse.v3.499
[13] Bunzel, N., Steinebach, M., & Liu, H. (2021). Cover-aware steganalysis. Journal of Cyber Security and Mobility. https://doi.org/10.13052/jcsm2245-1439.1011
[14] Shi, H., Sun, T., Jiang, X., Dong, Y., & Xu, K. (2021). A hevc video steganalysis against dct/dst-based steganography. International Journal of Digital crime and Forensics, 13(3), 19-33. https://doi.org/10.4018/ijdcf.20210501.oa2
[15] Badillah, R. (2023). Digital forensic evidence analysis in revealing defamation on social media (twitter) using the static forensics method. Ceddi Journal of Information System and Technology (Jst), 2(2), 22-33. https://doi.org/10.56134/jst.v2i2.45
[16] Mualfah, D. and Ramadhan, R. (2020). Analisis forensik metadata kamera cctv sebagai alat bukti digital. digital Zone Jurnal Teknologi Informasi Dan Komunikasi, 11(2), 257-267. https://doi.org/10.31849/digitalzone.v11i2.5174
[17] Anshori, I., Putri, K., & Ghoni, U. (2020). Analisis barang bukti digital aplikasi facebook messenger pada smartphone android menggunakan metode nij. It Journal Research and Development, 5(2), 118-134. https://doi.org/10.25299/itjrd.2021.vol5(2).4664