HASIL CEK_60020397_C.35_(1)Penerapan Metode Static Forensics untuk Ekstraksi File Steganografi pada Bukti Digital Menggunakan Framework DFRWS

by Imam Riadi 60020397

Submission date: 27-Dec-2020 10:46PM (UTC+0700)
Submission ID: 1481489373
File name: CEK35_60020397.pdf (669.23K)
Word count: 3891
Character count: 24771

Terakreditasi SINTA Peringkat 2
Surat Keputusan Dirjen Penguatan Riset dan Pengembangan Ristek Dikti No. 10/E/KPT/2019
masa berlaku mulai Vol. 1 No. 1 tahun 2017 s.d Vol. 5 No. 3 tahun 2021

Terbit online pada laman web jurnal: **http://jurnal.iaii.or.id**

JURNAL RESTI
(Rekayasa Sistem dan Teknologi Informasi)
Vol. 4 No. 3 (2020) 576 - 583 ISSN Media Elektronik: 2580-0760

Penerapan Metode *Static Forensics* untuk Ekstraksi File Steganografi pada Bukti Digital Menggunakan *Framework* DFRWS

Sunardi[1], Imam Riadi[2], Muh. Hajar Akbar[3]
[1]Program Studi Teknik Elektro, Universitas Ahmad Dahlan
[2]Program Studi Sistem Informasi, Universitas Ahmad Dahlan
[3]Program Studi Magister Teknik Informatika, Universitas Ahmad Dahlan
[1]sunardi@mti.uad.ac.id, [2]imam.riadi@is.uad.ac.id, [3]muh1808048031@webmail.uad.ac.id

Abstract

Steganography is one of the anti-forensic techniques that allow criminals to hide information in other messages so that during the investigation, the investigator will experience problems and difficulty in getting evidence of original information on the crime. Therefore an investigator is required to have the ability to be able to find and extract (decoding) using the right tools when opening messages that have been inserted by steganography techniques. The purpose of this study is to analyze digital evidence using the static forensics method by applying the six stages to the Digital Forensics Research Workshop (DFRWS) framework and extracting steganography on files that have been compromised based on case scenarios involving digital crime. The tools used are FTK Imager, Autopsy, WinHex, Hiderman, and StegSpy. The results of extraction of 9 out of 10 files that were scanned by steganography files had 90% success and 10% of steganography files were not found, so it can be concluded that the extraction files in steganographic messages can be used as legal digital proofs according to law.

Keywords: Anti-Forensic, Steganography, DFRWS, Hiderman

Abstrak

Steganografi merupakan salah satu teknik anti forensik yang memungkinkan pelaku kejahatan untuk menyembunyikan suatu informasi kedalam pesan lainnya, sehingga pada saat pemeriksaan investigator akan mengalami permasalahan dan kesulitan untuk mendapatkan bukti informasi asli pada kejahatan tersebut. Oleh karena itu seorang investigator dituntut untuk memiliki kemampuan agar dapat menemukan serta melakukan ekstraksi (*decoding*) menggunakan *tools* yang tepat saat membuka pesan yang telah disisipi teknik steganografi. Tujuan penelitian ini adalah melakukan analisis bukti digital menggunakan metode *static forensics* dengan menerapkan enam tahapan pada *framework Digital Forensics Research Workshop* (DFRWS) serta melakukan ekstraksi steganografi pada file yang telah disusupi berdasarkan skenario kasus yang melibatkan kejahatan digital. Tools yang digunakan adalah FTK Imager, Autopsy, WinHex, Hiderman, dan StegSpy. Hasil ekstraksi terhadap 9 dari 10 file yang diskenariokan telah disusupi file steganografi memiliki keberhasilan 90% dan 10% tidak ditemukan file steganografi, sehingga dapat disimpulkan bahwa file ekstraksi pada pesan steganografi dapat dijadikan bukti digital yang sah menurut hukum.

Kata kunci: Anti Forensik, Steganografi, DFRWS, Hiderman

1. Pendahuluan

Semakin luasnya pemanfaatan komputer dalam berbagai aspek kehidupan manusia selain memberi dampak positif juga membawa dampak negatif dengan semakin banyaknya aktivitas kriminal [1]. Di Indonesia, selama tahun 2019 Direktorat Tindak Pidana Siber (Dittipidsiber) Bareskrim Polri melaporkan 4.586 kasus tindak kejahatan dengan memanfaatkan teknologi komputer [2]. Laporan tersebut menyadarkan pentingnya pemahaman serta keahlian di bidang forensik digital dalam mendukung proses investigasi dan pencarian barang bukti kasus kejahatan pada bidang komputer (*cybercrime*). Forensik digital merupakan sebuah cabang ilmu yang menerapkan teknik investigasi dan analisis pada media komputer atau media penyimpanan digital dengan cara mengidentifikasi, mengumpulkan, memeriksa, dan menyimpan bukti kasus kejahatan agar dapat dipertanggungjawabkan secara hukum [3].

Diterima Redaksi : 25-04-2020 | Selesai Revisi : 02-06-2020 | Diterbitkan Online : 20-06-2020

Barang bukti sangat penting dalam proses investigasi karena pembuktian suatu kasus bergantung pada adanya barang bukti. Keberadaan barang bukti menunjukkan bahwa betul adanya peristiwa hukum yang telah terjadi. Pada prinsipnya kasus kejahatan pasti meninggalkan barang bukti termasuk diantaranya adalah bukti elektronik maupun bukti digital [4]. Bukti elektronik adalah bukti yang secara visual yang dapat dikenali secara fisik. Oleh karena itu seorang investigator dituntut untuk mengenali dan memahami kriteria suatu barang bukti elektronik ketika sedang melakukan pencarian barang bukti di Tempat Kejadian Perkara (TKP).

Bukti digital adalah bukti yang merupakan hasil ekstrak atau *recover* menjadi bukti digital dari bukti elektronik [3]. Berdasarkan Undang-Undang Republik Indonesia No. 11 tahun 2008 tentang Informasi dan Transaksi Elektronik, barang bukti dikenal dengan istilah informasi elektronik dan dokumen elektronik. Oleh karena itu dalam rangka mengungkap kasus kejahatan berkaitan dengan bukti elektronik/digital, jenis barang bukti inilah yang harus dicari kemudian dianalisis secara teliti keterkaitan masing-masing file.

Saat melakukan tindakan *cybercrime*, pelaku sering berupaya menggunakan teknik anti forensik dengan tujuan membuat barang bukti palsu dengan harapan mengaburkan serta menghilangkan jejak kejahatan yang telah dibuat [6]. Dalam perspektif investigator digital, anti forensik dapat menghambat pengumpulan bukti, meningkatkan waktu penyelidikan, bukti menyesatkan yang dapat membahayakan penyelidikan, serta menghalangi deteksi kejahatan digital [7].

Salah satu teknik anti forensik dalam dunia digital adalah steganografi [8]. Penggunaan steganografi membutuhkan sekurang-kurangnya dua properti yaitu wadah penampung (*cover*) dan pesan atau data yang disembunyikan. Teknik ini memungkinkan pelaku untuk menyembunyikan informasi berupa teks, gambar, video ataupun audio dengan memasukkan informasi tersebut kedalam pesan lain dalam bentuk media digital, sehingga keberadaan pesan tidak diketahui [9]. Oleh karena itu, seorang investigator dituntut agar memiliki kemampuan dalam menemukan serta melakukan ekstraksi (*decoding*) pada pesan yang telah disusupi tersebut.

Permasalahan *cybercrime* sangat penting sehingga perlu adanya panduan tentang teknik investigasi sehingga menghasilkan pembuktian secara ilmiah [10]. Pemanfaatan serta penerapan *framework* atau kerangka kerja forensik dalam menangani kasus digital merupakan faktor penting untuk mendukung proses investigasi tindak kejahatan *cybercrime* agar lebih efektif dan efisien [11]. Kerangka kerja forensik yang telah banyak digunakan untuk menginvestigasi kasus digital forensik diantaranya *National Institute of Justice* (NIJ) [12], *Digital Forensics Research Workshop* (DFRWS) [13], *National Institute of Standard and Technology* (NIST), *Digital Forensics Investigation Framework* (DFIF) [14], dan *Generic Computer Forensic Investigation Model* (GCFIM) [15][16].

Pada penelitian ini dilakukan proses investigasi pada bukti digital menggunakan *framework* DFRWS dan melakukan ekstraksi file yang telah disisipi pesan steganografi. DFRWS dipilih karena memiliki kerangka forensik standar dan konsisten yang dapat memberikan kemudahan dalam penggunaan serta mudah dipahami oleh pengguna teknis ataupun non-teknis [17].

Penelitian dengan tema sejenis pernah dilakukan dengan judul Analisis Digital Forensik pada File Steganography (Studi kasus: Peredaran Narkoba) [18]. Penelitian ini membahas proses investigasi serta menemukan *digital evidence* pada file steganografi. Proses analisis steganografi menggunakan piranti lunak yaitu WinHex, InvisibleSecrets, dan FTK Imager. Metodologi atau tahapan penelitian dilakukan secara sistematis yaitu *literature review, observation & data collection, scenario case, preparation system, investigation & analysis case,* dan *report & documentation*.

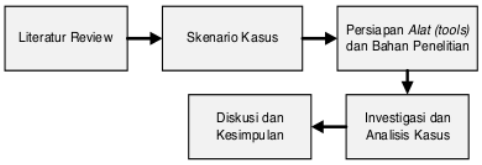
Penelitian kedua dengan tema sejenis juga dilakukan dengan judul Analisa Teknik Steganografi dan Steganalysis Pada File Multimedia Menggunakan Net Tools dan Hex Editor [19]. Penelitian ini membahas penggunaan aplikasi WinHex untuk melakukan analisis pada pesan yang disembunyikan menggunakan Net Tools kedalam citra penampung. Metode yang dipakai menggunakan metode eksperimental yaitu identifikasi masalah, studi literatur, pengujian, dan analisis.

Penelitian ketiga dengan tema yang sejenis pernah dilakukan dengan judul Analisis Digital Forensics Investigation pada Bukti Digital Steganography [20]. Penelitian ini membahas proses menemukan dan menganalisis barang bukti berupa file dengan format *.txt dan *.pdf yang disembunyikan oleh pelaku kejahatan menggunakan teknik steganografi, dan file tersebut telah di hapus oleh pelaku dari media penyimpanan digital. Pada penelitian ini menggunakan tools pada kali linux serta penggunaan StegHide dalam menemukan file yang tersembunyi. Metode penelitian yang digunakan adalah *computer forensic investigative process* yang terbagi dalam empat tahap, yaitu *acquisition, identification, evaluation,* dan *admission*.

2. Metode Penelitian

Penerapan metode yang tepat dalam mengumpulkan data forensik akan memberikan dampak keberhasilan hingga 100% [21]. Pada penelitian ini, tahapan penelitian yang dilakukan untuk pengambilan bukti digital adalah menggunakan pendekatan metodologi *static forensics* yang dapat dilihat pada Gambar 1. Metode *static forensics* merupakan teknik konvensional untuk melakukan penanganan barang bukti elektronik

yang berfokus pada pemeriksaan salinan duplikasi atau *image* [22].

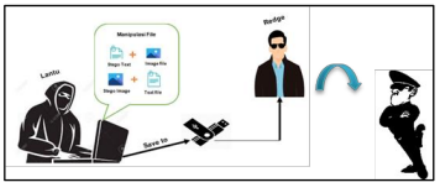


Gambar 1. Metodologi Penelitian

Berdasarkan Gambar 1, metodologi penelitian dibuat secara sistematis agar dapat menjelaskan bagaimana langkah-langkah yang dapat dijadikan pedoman untuk mengatasi permasalahan pada penelitian ini. Metodologi penelitian dimulai dari *literature review* yaitu dengan cara mengumpulkan beberapa informasi penelitian terdahulu sebagai rujukan dari berbagai sumber, selanjutnya dilakukan perancangan skenario kasus, menyiapkan alat dan bahan sebagai simulasi kasus, melakukan investigasi dan analisis kasus, dan terakhir melakukan diskusi dan memberikan kesimpulan.

2.1 Skenario Kasus

Skenario kasus bertujuan untuk memudahkan proses identifikasi saat melakukan analisis bukti digital. Barang bukti yang diamankan merupakan media penyimpanan berupa *flash disk* dalam keadaan mati atau tidak sedang aktif (*off*) di komputer. Objek penelitian sebagai bukti digital yang digunakan merupakan hasil data fiktif (tidak nyata) penemuan tindak kejahatan penyalahgunaan teknik steganografi dengan melibatkan media penyimpanan berupa sebuah *flash disk*. Berikut Gambar 2 skenario kasus pada penelitian ini.



Gambar 2. Skenario Kasus

"Seorang bandar narkoba bernama Lantu melakukan pertemuan singkat dengan seseorang yang bernama Redge untuk merencanakan proses transaksi jual beli narkoba. Redge diberikan sebuah *flash disk* yang berisi petunjuk mengenai waktu dilakukannya transaksi, lokasi transaksi, dan foto pengedar narkoba. Semua petunjuk tersebut disembunyikan dalam beberapa file. Polisi mengetahui rencana pertemuan tersebut dan kemudian melakukan penyelidikan terhadap rumah Redge. Polisi mendapati sebuah *flash disk* yang dicurigai memiliki bukti terkait transaksi yang akan dilakukan".

2.2 Persiapan Alat dan Bahan

Alat yang digunakan pada penelitian ini dapat dilihat pada Tabel 1.

Tabel 1. Alat Penelitian

No	Nama Alat	Spesifikasi	Keterangan
1	Notebook	Acer Aspire E1 - 431, 4 GB DDR 3 Memory, 500 GB HDD	Perangkat keras analisis
2	Windows 10	Windows 10 Pro	Sistem operasi
3	FTK Imager	Versi 4.2.0.13	Tool akuisisi
4	Autopsy	Versi 4.14.0	Tool analisis
5	Winhex	Versi 18.7	Tool akuisisi
6	Hiderman	-	Tool steganografi
7	StegSpy	-	Stego detect

Bahan sebagai bukti digital yang digunakan berupa *stego text* dan *stego image* yang telah dilakukan pengecekan nilai *hash* pada masing-masing file seperti ditampilkan pada Tabel 2.

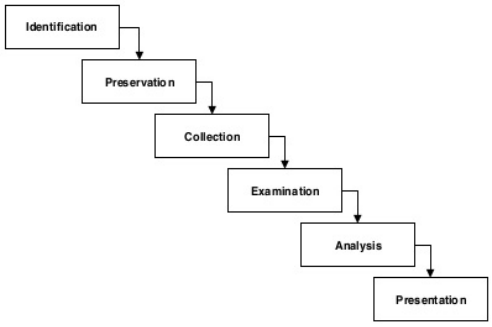
Tabel 2. Kandungan Barang Bukti *Flash Disk*

No	Nama File	Format	Nilai Hash (MD5)
1	File1	.jpg	8E4D5A1C6BFA03DCBE860943CCC86325
2	File2	.jpg	CA8BC8529A47A6777E5D201DEEC63196
3	File3	.jpg	138AAF57022D10A33837AB4D23559D79
4	File4	.jpg	6E389BEE26D14C17A19F213A935AD426
5	File5	.jpg	2F80636672A18EB7E1DB8BF392AD2418
6	File6	.pdf	88568362352A9B2407650887A532C253
7	File7	.pdf	CDB792A24BDDE9A8B4E61ADB7BD35087
8	File8	.pdf	6870FA1AA3EC6E8C08B1B9EF8B0D1A54
9	File9	.pdf	72E87BD409F64088813FD8CE7735B45C
10	File10	.pdf	44101FB802D2854E5AB88664D8BBF70E
11	Key	.txt	BF38A03F09A4772BC89388448D65017F

2.3 Investigasi dan Analisis Kasus

Investigasi dan analisis kasus dalam penelitian ini menggunakan *framework* DFRWS. *Framework* ini dapat membantu menemukan bukti serta memberikan mekanisme terpusat dalam merekam informasi yang telah dikumpulkan [21]. DFRWS dimulai dengan tahap *identification* (identifikasi), yaitu melakukan deteksi profil, monitoring sistem, dan analis audit. Selanjutnya diikuti oleh tahap *preservation* (pelestarian) dengan melakukan proses pelestarian untuk mencegah bukti-bukti yang telah didapatkan serta memastikan keaslian integritas barang bukti agar terhindar dari pihak-pihak yang tidak berhak, sehingga bukti tidak terkontaminasi dan benar-benar valid/sah. Tahap berikutnya adalah *collection* (koleksi) melalui proses pengumpulan sampel-sampel bukti yang diduga berpotensi sebagai barang bukti yang kuat. Selanjutnya terdapat dua tahap penting yaitu tahap *examination* (pemeriksaan) dan

tahap analisis. Proses pelacakan bukti, validasi bukti, dan pemulihan data tersembunyi/terenkripsi dilakukan pada tahap ini. Tahap berikutnya adalah *presentation* (presentasi) yaitu proses yang berkaitan dokumentasi, kesaksian ahli, dan sebagainya. Tahapan dalam *framework* DFRWS dapat dilihat pada Gambar 3 [13].

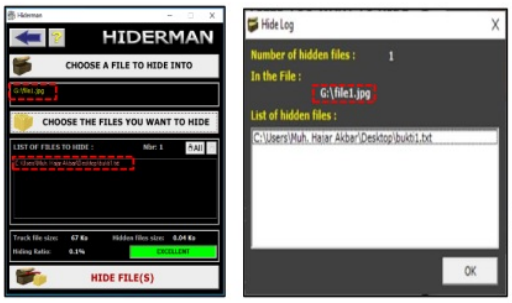


Gambar 3. Tahapan dalam *framework* DFRWS

3. Hasil dan Pembahasan

3.1 Skenario dan Implementasi

Skenario kejahatan penyalahgunaan teknik steganografi dijalankan berdasarkan pada Gambar 2. Pelaku menyembunyikan pesan rahasia mengenai proses transaksi jual beli narkoba berupa *stego text* dan *stego image* yang disisipkannya pada beberapa file dalam sebuah *flash disk*. Implementasi penyisipan pesan rahasia yang dilakukan oleh pelaku diskenariokan seperti pada Gambar 4. Pelaku kejahatan melakukan aksinya dengan menyisipkan beberapa pesan rahasia menggunakan bantuan tool Hiderman.



Gambar 4. Skenario Penyisipan Pesan

3.2 Identifikasi

Proses identifikasi barang bukti diawali dengan melakukan pengamanan TKP di kamar kos pelaku seperti pada Gambar 4(a) yang bertujuan untuk menghindari akses masuk bagi pihak-pihak yang tidak memiliki izin pada tempat tersebut. Selanjutnya dilakukan pencarian barang bukti dengan cara melihat keseluruhan TKP terhadap apa saja yang berpotensi sebagai barang bukti. Berdasarkan hasil pencarian, seperti pada Gambar 4(b) polisi menemukan sebuah barang bukti elektronik di atas meja ruang kerja pelaku.

(a) TKP (b) Barang bukti

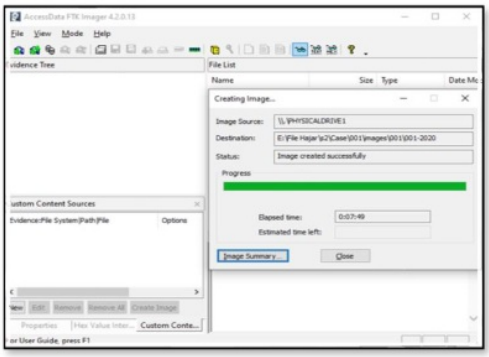
Gambar 4. Pengamanan TKP dan Penemuan Barang Bukti

Selanjutnya dilakukan proses identifikasi terhadap barang bukti yang ditemukan dari sisi jenis, merk, spesifikasi dan keterangan pendukung lainnya seperti pada Tabel 3 untuk dijadikan bukti otentik saat proses penyidikan.

Tabel 3. Dokumentasi Barang Bukti

Barang Bukti	Merk	Spesifikasi	Keterangan
Flash Disk	Kingston	Data Traveler G3, 8 GB	Barang bukti elektronik

3.3 Pelestarian

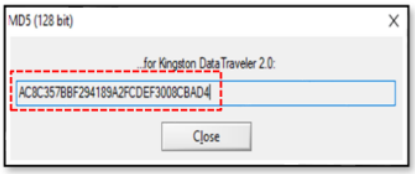


Gambar 5. Proses Akuisisi Flashdisk

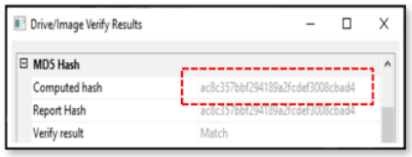
Barang bukti digital memiliki sifat mudah berubah, serta memiliki risiko hilang serta mengalami kerusakan [22]. Oleh karena itu dilakukan proses pelestarian untuk menjaga dan mengamankan keaslian barang bukti fisik yang telah didapatkan pada tahap identifikasi sehingga integritas data tetap terjaga sampai proses analisis dilakukan. Proses pelestarian dilakukan dengan cara mengakuisisi barang bukti dengan metode *static acquisition* yaitu melakukan *cloning* atau *imaging* terhadap media penyimpanan data (barang bukti fisik). Proses *cloning* dilakukan dengan *copy* data secara *bitstream image* yaitu menyalin setiap bit demi bit dari data asli, *temporary file, hidden file*, bahkan file yang ter-*overwrite* pada media baru.

Proses akuisisi data pada barang bukti fisik (*flash disk*) dilakukan menggunakan tool FTK Imager seperti yang terlihat pada Gambar 5. Waktu yang diperlukan untuk akuisisi data adalah 7 menit 49 detik.

Selanjutnya dilakukan 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. Perbandingan nilai *hash* dapat dilihat pada Gambar 6. Proses verifikasi pada Gambar 6(a) dan Gambar 6(b) keduanya menampilkan nilai *hash* identik dengan nilai yang sama yaitu "ac8c357bbf294189a2fcdef3008cbad4". Berdasarkan hasil tersebut maka dapat disimpulkan bahwa file barang bukti hasil *cloning* identik dengan barang bukti aslinya, sehingga proses investigasi dapat dilakukan ke tahap *collection*.



(a) *Hash* Barang Bukti Asli



(b) *Hash* Barang Bukti Hasil *Cloning*

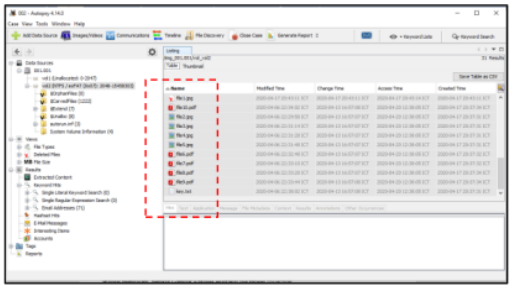
Gambar 6. Nilai *Hash* Barang Bukti

Gambar 7. Pengemasan Barang Bukti Asli

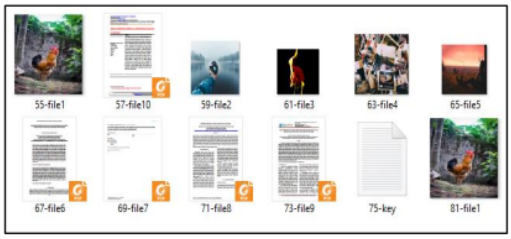
Setelah mendapatkan salinan barang bukti berupa *image*, langkah selanjutnya adalah melakukan pengemasan pada barang bukti asli dengan cara menyegel serta memberikan pelabelan untuk memastikan agar saat pemindahan, barang bukti asli tetap terjaga integritasnya. Proses pengemasan terhadap barang bukti asli ditunjukkan seperti pada Gambar 8.

3.4 Pengumpulan

Proses *collection* yaitu melakukan pengumpulan data yang diyakini memiliki keterkaitan dengan kejahatan yang dilakukan. Proses *collection* dilakukan menggunakan salinan bukti digital yang telah didapatkan pada tahap *acquisition* seperti pada Gambar 9. Proses *collection* menggunakan tool Autopsy berhasil mengumpulkan 11 file dengan nama berbeda. Selanjutnya dilakukan proses ekstraksi pada file tersebut untuk dilakukan analisis mendalam. Gambar 9 memperlihatkan proses ekstraksi file pada proses *collection*.



Gambar 8. Pengumpulan Terkait Barang Bukti



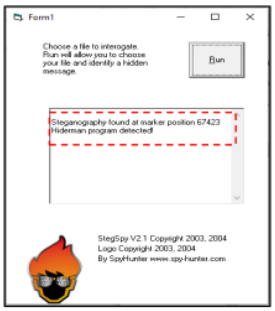
Gambar 9. Daftar File Hasil Ekstraksi

Langkah selanjutnya adalah melakukan pengecekan nilai *hash* pada tiap-tiap file. Hal ini bertujuan untuk memastikan file hasil ektraksi sesuai dengan barang bukti yang telah diskenariokan. Proses pengecekan nilai *hash* menggunakan tool hashMyFiles. Hasil dari pengecekan dapat dilihat seperti pada Tabel 4.

Tabel 4. Validasi Nilai *Hash* Menggunakan *Tool* HashMyFiles

Nama File	Hash md5	Validasi hash
55-file1	8e4d5a1c6bfa03dcbe860943ccc86325	valid
59-file2	44101fb802d2854e5ab88664d8bbf70e	valid
61-file3	ca8bc8529a47a6777e5d201deec63196	valid
63-file4	138aaf57022d10a33837ab4d23559d79	valid
65-file5	6e389bee26d14c17a19f213a935ad426	valid
67-file6	2f80636672a18eb7e1db8bf392ad2418	valid
69-file7	88568362352a9b2407650887a532c253	valid
71-file8	cdb792a24bdde9a8b4e61adb7bd35087	valid
73-file9	6870fa1aa3ec6e8c08b1b9ef8b0d1a54	Tidak valid
57-file10	72e87bd409f64088813fd8ce7735b45c	valid
75-key	.txt	no Steg found

3.5 Pengujian



Gambar 10. Pengujian Keberadaan Pesan Rahasia

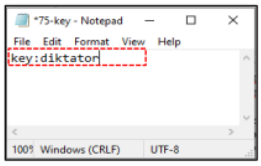
Tabel 5. Hasil Pengujian File Ekstraksi Menggunakan Tool Stegspy

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
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	-

3.6 Analisis

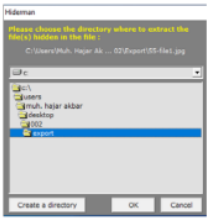
Proses analisis dilakukan untuk membuka keberadaan pesan steganografi yang telah terdeteksi pada proses *examination*. Setelah dilakukan pengamatan, terdapat satu file dengan nama file 75-key.txt yang didalamnya memuat informasi seperti pada Gambar 11.

File yang terdeteksi mengandung pesan steganografi dianalisis menggunakan tool forensik untuk melakukan dekripsi file steganografi menggunakan key "diktator". Gambar 12 menunjukkan proses ekstraksi file steganografi menggunakan tool Hiderman.

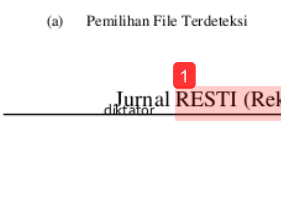


Gambar 11. Isi File 75-key.txt

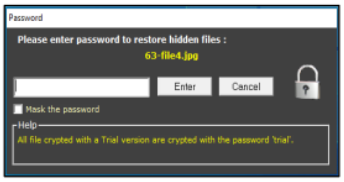
(a) Pemilihan File Terdeteksi



(b) Pemilihan Direktori Ekstrak File



(c) Proses input Key



Gambar 12. Proses Dekripsi (*Unhide Files*)

Hasil dari proses ekstraksi file steganografi dapat dilihat pada Tabel 6.

Tabel 6. Informasi Hasil Dekripsi

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	160℃0
67-file6	.pdf	Bukti6	1176845	
69-file7	.pdf	Bukti7	272361	
71-file8	.pdf	Bukti8	1555961	
73-file9	.pdf	-	-	-
57-file10	.pdf	bukti10	192119	
75-key	.txt			Key untuk dekripsi (diktator)

3.7 Presentasi

Berdasarkan hasil pada tahapan analisis, presentasi atau penyajian laporan disajikan dengan cara memberikan informasi seperti pada Tabel 7.

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 mendapatkan 9 salinan bukti digital dengan nilai *hash* identik dengan file aslinya, sehingga didapatkan 9 file yang dideteksi sebagai file steganografi. Proses ekstraksi file steganografi menggunakan Hiderman memberikan keberhasilan sebesar 90% dan 10 % tidak ditemukan file steganografi. Hal ini dibuktikan dengan berhasilnya dilakukan proses ekstraksi terhadap 9 dari 11 file yang diskenariokan telah disusupi oleh 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 serta penyempurnaan dari penelitian ini, maka dimungkinkan untuk menggunakan tool forensik yang berbeda agar mendapatkan cara lain dalam melakukan proses *preservation, collection, examination,* dan *analysis*, serta proses ekstraksi file steganografi menggunakan aplikasi selain Hiderman.

Daftar Rujukan

[1] I. Yudhana, I. Riadi, and I. Zuhriyanto, "Analisis Live Forensics Aplikasi Media Sosial Pada Browser Menggunakan Metode Digital Forensics Research Workshop (DFRWS)," vol. 20, no. 2, pp. 125–130, 2019.

[2] patrolisiber, "Statistik Jumlah Laporan Polisi yang dibuat masyarakat," *patrolisiber.id*, 2019. https://patrolisiber.id/statistic (accessed Mar. 24, 2020).

[3] M. H. Akbar, Sunardi, and I. Riadi, "Analisis Bukti Digital Pada Flash Disk Drive Menggunakan Metode Generic Computer Forensic Investigation Model (GCFIM)," in *seminar Nasional Teknologi Fakultas Teknik Universitas Krinadwipayana*, 2019, pp. 715–723.

[4] I. Riadi, R. Umar, and I. M. Nasrulloh, "Analisis Forensik Bukti Digital Pada Frozen Solid State Drive Dengan Metode National Institute of Standards and Technology (NIST)," *J. Insa. Comtech*, vol. 2, no. 2, pp. 33–40, 2017.

[5] M. N. Al-Azhar, *Digital Forensic : Panduan Praktis Investigasi Komputer*. Jakarta: Salemba Infotek, 2012.

[6] B. Rahardjo and I. P. A. E. Pratama, "Pengujian Dan Analisa Anti Komputer Forensik Menggunakan Shred Tool," *Lontar Komput. J. Ilm. Teknol. Inf.*, vol. 7, no. 2, p. 104, 2016, doi: 10.24843/lkjiti.2016.v07.i02.p04.

[7] S. Alharbi, J. Weber-Jahnke, and Traore, "The Proactive and Reactive Digital Forensics Investigation Process: A Systematic Literature Review," *Int. J. Secur. its Appl.*, vol. 5, no. 4, pp. 59–71, 2011, doi: 10.1007/978-3-642-23141-4.

[8] E. S. Wijaya and Y. Prayudi, "Integrasi Metode Steganografi DCS Pada Image Dengan Kriptografi Blowfish Sebagai Model Anti Forensik Untuk Keamanan Ganda Konten Digital," *SNATI (Seminar Nas. Apl. Teknol. Informasi)*, no. June, 2015.

[9] I. W. Ardiyasa, "Implementasi Teknik Data Hidding Untuk Pengamanan Pesan Rahasia Pada Media Digital," in *Seminar Nasional Sistem Informasi dan Teknologi Informasi 2018*, 2018, pp. 601–605.

[10] A. Fauzan, I. Riadi, and A. Fadlil, "Analisis Forensik Digital Pada Line Messenger Untuk Penanganan Cybercrime," *Annu. Res. Semin.*, vol. 2, no. 1, pp. 159–163, 2017, [Online]. Available: http://seminar.ilkom.unsri.ac.id/index.php/ars/article/view/832/752.

[11] S. Ningsih, I. Riadi, and Y. Prayudi, "Digital Forensics Workflow as A Mapping Model for People, Evidence, and Process in Digital Investigation," *Int. J. Cyber-Security Digit. Forensics*, vol. 7, no. 3, pp. 294–304, 2018, doi: 10.17781/p002463.

[12] G. Shrivastava, "Forensic Computing Models: Technical Overview," 2012, pp. 207–216, doi: 10.5121/csit.2012.2222.

[13] G. Palmer, "A road map for digital forensic research," in *Proceedings of the Digital Forensic Research Conference, DFRWS 2001 USA*, 2001, pp. iii–42.

[14] M. Martini and K. K. R. Choo, "An integrated conceptual digital forensic framework for cloud computing," *Digital Investigation*. 2012, doi: 10.1016/j.diin.2012.07.001.

[15] Y. Yusoff, R. Ismail, and Z. Hassan, "Common Phases of Computer Forensics Investigation Models," *Int. J. Comput. Sci. Inf. Technol.*, vol. 3, no. 3, pp. 17–31, 2011, doi: 10.5121/ijcsit.2011.3302.

[16] R. Umar, A. Yudhana, and M. Nur Faiz, "Analisis Kinerja Metode Live Forensics Untuk Investigasi Random Access Memory Pada Sistem Proprietary," *Pros. Konf. Nas. Ke- 4 Asos. Progr. Pascasarj. Perguru. Tinggi Muhammadiyah*, no. June 2016, pp. 207–211, 2016.

[17] R. Sudesh, "Digital Forensic Models: a Comparative Analysis," *Int. J. Manag.*, vol. 8, no. 6, pp. 432–443, 2018.

[18] A. P. Saputra, H. Mubarok, and N. Widiyasono, "Analisis Digital Forensik pada File Steganography (Studi kasus : Peredaran Narkoba)," *J. Tek. Inform. dan Sist. Inf.*, vol. 3, no. 1, pp. 179–190, 2017, doi: 10.28932/jutisi.v3i1.594.

[19] Y. B. Utomo and D. Erwanto, "Analisa Teknik Steganografi dan Steganalysis Pada File Multimedia Menggunakan Net Tools dan Hex Editor," *Gener. J.*, vol. 3, no. 1, pp. 16–22, 2019, doi: 10.29407/gj.v3i1.12698.

[20] V. A. Silalahi and I. Sembiring, "Analisis Digital Forensics Investigation pada Bukti Digital Steganography," 2013.

[21] A. Tanner and D. Dampier, "Concept mapping for digital forensic investigations," *IFIP Adv. Inf. Commun. Technol.*, vol. 306, pp. 291–300, 2009, doi: 10.1007/978-3-642-04155-6_22.

[22] A. Syauqi, I. Riadi, and Y. Prayudi, "Validasi Policy Statement pada Lemari Penyimpanan Bukti Digital (LPBD)," *J. Educ. Inform. Technol. Sci.*, vol. 1, no. 2, pp. 27–37, 2019.

HASIL CEK_60020397_C.35_(1)Penerapan Metode Static Forensics untuk Ekstraksi File Steganografi pada Bukti Digital Menggunakan Framework DFRWS

ORIGINALITY REPORT

8%	8%	3%	0%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	jurnal.iaii.or.id Internet Source	7%
2	Samuel Andi Kristyan, Suhardi, Tutun Juhana. "Design Framework Forensics Readiness as a Service for Automatic Processing", 2020 International Conference on Information Technology Systems and Innovation (ICITSI), 2020 Publication	1%
3	idoc.pub Internet Source	1%

Exclude quotes	On	Exclude matches	< 1%
Exclude bibliography	On		