Terbit *online* pada laman : https://teknosi.fti.unand.ac.id/

Jurnal Nasional Teknologi dan Sistem Informasi

| ISSN (Print) 2460-3465 | ISSN (Online) 2476-8812 |

Artikel Penelitian

Steganalisis Bukti Digital pada Media Penyimpanan Menggunakan Metode *Static Forensics*

*Sunardi [a], Imam Riadi [b], Muh. Hajar Akbar [c] **

[a] *Program Studi Teknik Elektro Universitas Ahmad Dahlan, Jalan Prof. Dr. Soepomo, S.H., Janturan, Warungboto, Umbulharjo, Yogyakarta, Indonesia*
[b] *Program Studi Sistem Informasi Universitas Ahmad Dahlan, Jalan Prof. Dr. Soepomo, S.H., Janturan, Warungboto, Umbulharjo, Yogyakarta, Indonesia*
[c] *Program Studi Teknik Informatika, Universitas Ahmad Dahlan, Jalan Prof. Dr. Soepomo, S.H., Janturan, Warungboto, Umbulharjo, Yogyakarta, Indonesia*

INFORMASI ARTIKEL

Sejarah Artikel:
Diterima Redaksi: 14 November 2020
Revisi Akhir: 23 Mei 2020
Diterbitkan *Online*: 30 Mei 2020

KATA KUNCI

Steganalisis,
StegSpy,
Static Forensics

KORESPONDENSI

E-mail: hajarakbar16@gmail.com

A B S T R A C T

Steganografi merupakan salah satu teknik anti forensik yang memungkinkan pelaku kejahatan untuk menyembunyikan suatu informasi kedalam pesan lainnya, sehingga pada saat pemeriksaan akan sulit untuk didapatkan bukti informasi kejahatan tersebut. Oleh karena itu diperlukan teknik untuk mendeteksi pesan tersembunyi di dalam suatu data. Teknik tersebut dikenal dengan istilah steganalisis. Steganalisis merupakan suatu ilmu anti-steganografi yang tujuan utamanya adalah mempelajari karakteristik penyembunyian suatu data pada media digital serta mendeteksi keberadaan pesan rahasia yang disembunyikan menggunakan teknik steganografi. Tujuan pada penelitian ini adalah menerapkan teknik steganalisis untuk mendeteksi keberadaan pesan yang disembunyikan dalam pesan lain dengan menggunakan metode *static forensics.* Pada penelitian ini, proses penyisipan *pesan* steganografi menggunakan aplikasi Hiderman, sedangkan proses steganalisis menggunakan aplikasi StegSpy. Hasil yang didapat pada penelitian ini adalah proses steganalisis dengan menggunakan bantuan aplikasi StegSpy terbukti berhasil mendeteksi keberadaan pesan tersembunyi pada keempat file yang diskenariokan telah disisipi pesan steganografi. Hal ini membuktikan bahwa hasil steganalisis pada media penyimpanan flash disk dengan menggunakan aplikasi StegSpy dapat dijadikan bukti digital yang sah menurut hukum.

1. PENDAHULUAN

Berbagai aksi kejahatan yang memanfaatkan teknologi komputer sebagai medianya pada akhir-akhir ini menunjukan angka yang signifikan, baik dari segi kuantitas maupun dari segi kualitasnya. Di Indonesia, [1] melaporkan bahwa sepanjang tahun 2018, Badan Siber dan Sandi Negara (BSSN) mencatat terdapat 225,9 kejahatan dengan menggunakan teknologi komputer sehingga merugikan ekonomi Indonesia hingga 400 Triliun Rupiah. Untuk melawan dan menangani kasus kejahatan komputer tidak hanya dari Polri saja, akan tetapi dibutuhkan juga kesadaran dan pengetahuan dari masyarakat mengenai bagaimana cara membuktikan suatu kejahatan yang memanfaatkan teknologi komputer secara ilmiah [2].

Sebagai langkah untuk menutupi kejahatan serta menghindarkan diri dari *IT Forensics*, menurut [3] pelaku menggunakan teknik anti forensik dengan tujuan menurunkan kualitas bukti digital sehingga menyulitkan ahli forensik dalam melakukan proses investigasi. Salah satu teknik anti forensik adalah steganografi. Teknik ini memungkinkan pelaku untuk menyembunyikan informasi dengan memasukan informasi tersebut ke dalam pesan lain dalam bentuk media digital, sehingga keberadaan pesan tersebut tidak diketahui [4].

Untuk mendeteksi serta menanggulangi teknik steganografi, munculah disiplin ilmu yang dinamakan steganalisis. Steganalisis adalah suatu teknik untuk mendeteksi serta membongkar keberadaan pesan rahasia yang dicurigai dalam media digital [5]. Selain itu menurut [6], steganalisis dapat dijadikan pedoman untuk mengetahui dan mengevaluasi kelemahan teknik steganografi

https://doi.org/10.25077/ TEKNOSI.v6i1.2020.1-8

sehingga dapat dilakukan proses penyisipan pesan yang lebih aman. Pada kehidupan nyata teknik steganalisis diterapkan untuk melakukan pelacakan terhadap tindakan kriminalitas atau komputer forensik maupun dalam serangan *cyber warfare*.

Berdasarkan studi literatur terdahulu sebagai pendukung penelitian ini, ditemukan penelitian dengan tema sejenis. Penelitian pertama dengan judul "Analisa Teknik Steganografi dan *Steganalysis* Pada *File* Multimedia Menggunakan Net Tools dan Hex Editor". Tujuan dari penelitian ini adalah penggunaan aplikasi Net Tools untuk melakukan penyisipan pesan ke dalam wadah penampung serta penggunaan aplikasi Hex Editor untuk menganalisis pesan tersebut tanpa menyebabkan pesan yang telah disisipkan mengalami kerusakan sehingga kerahasiaan pesan yang dikirimkan lebih terjaga. Adapun hasil dari penelitian tersebut adalah Aplikasi Net Tools dapat mengamankan suatu pesan yang akan dikirimkan melalui media internet dan menghindarkan dari pihak yang ingin memanipulasi isi pesan tersebut [7].

Penelitian kedua oleh [8] dengan judul "*A Comparison Study Using StegExpose for Steganalysis*", penelitian ini bertujuan untuk melakukan investigasi pada aplikasi *open source* steganografi/steganalisis serta melakukan pengujian pada aplikasi StegExpose untuk proses steganalisis. Setelah melakukan investigasi secara komparatif, hasilnya menunjukan bahwa kemampuan dari aplikasi stegExpose sangat terbatas.

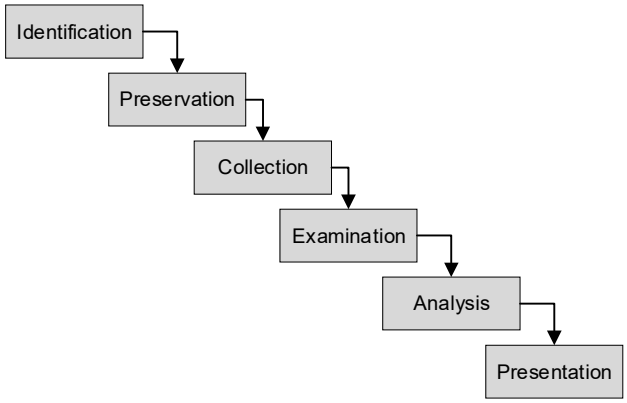
Peneliti ketiga oleh [9] dengan judul "Penerapan Metode *Steganalysis* untuk Pengembalian Data pada *Hard Drive*". Penelitian ini bertujuan untuk melakukan *steganalysis* dan melewati kode keamanan *password* pada berkas yang sudah dilakukan steganografi dan melakukan pengembalian berkas yang sudah dilakukan steganografi pada *hard drive* yang sudah di format. Setelah melakukan pengujian, maka hasil yang didapatkan adalah meskipun *file system* pada *hard drive* diganti, heksadesimal pada berkas yang ada pada hard drive tersebut akan tetap sama, Testdisk dan photorec bekerja dengan baik dalam mengembalikan seluruh berkas, namun tidak sempurna karena berkas yang telah disembunyikan didalam berkas lainnya tidak ikut terbaca dan harus dilakukan pencarian secara manual, Teknik *steganography* dengan menggunakan command prompt dideteksi dengan mudah dibandingkan dengan menggunakan program aplikasi steganografi seperti camouflage.

Penelitian keempat oleh [10] dengan judul "Investigasi Email Spoofing dengan Metode *Digital Forensics Research Workshop* (DFRWS)" juga menjadi acuan dalam penelitian ini. Penelitian tersebut membahas tentang identifikasi *email spoofing* dengan melakukan analisis pada header email yang diterima dengan menggunakan metode DFRWS. Adapun hasil dari penelitian tersebut adalah proses identifikasi dilakukan dengan cara mengidentifikasi pesan yang dicurigai memiliki keanehan. Keanehan dapat berupa adanya sebuah tautan berupa teks atau gambar yang akan mengarahkan ke halaman *web phishing*. Setelah analisis dilakukan, maka langkah selanjutnya adalah melakukan identifikasi dengan cara mencermati secara rinci pada *header email* agar lebih meyakinkan bahwa *email spoofing* benar-benar ada atau tidak.

2. METODE

Menurut [11], penerapan metode yang tepat dalam mengumpulkan data akan memberikan dampak keberhasilan hingga 100%. Pada penelitian ini, metode yang digunakan untuk pengambilan bukti digital adalah metode *static forensics*. Metode *static forensics* merupakan teknik konvensional untuk melakukan penanganan barang bukti elektronik yang berfokus pada pemeriksaan salinan duplikasi atau *image* [12]. Pada penelitian ini barang bukti yang diambil merupakan media penyimpanan berupa *flash disk* dalam keadaan mati atau tidak sedang aktif di komputer dengan menerapkan langkah kerja (*framework*) *Digital Forensics Research Workshop* (DFRWS).

Framework DFRWS memiliki enam tahapan yaitu *identification, preservation, collection, examination, analysis,* dan *presentation*. *framework* DFRWS. *Framework* ini dapat membantu menemukan bukti serta memberikan mekanisme terpusat dalam merekam informasi yang telah dikumpulkan [13] Tahapn Framework DFRWS dapat dilihat pada Gambar 1.



Gambar 1. Tahapan *Framework* DFRWS

Menurut [14], tahapan pada metode DFRWS dapat dijelaskan sebagai berikut:

1. *Identification* (Identifikasi)
   Pada tahap ini dilakukan proses identifikasi tentang kebutuhan-kebutuhan apa saja yang harus dipersiapkan dalam melakukan penyelidikan dan pencarian bukti digital.

2. *Preservation* (Pemeliharaan)
   Pada tahap ini dilakukan proses pemeliharaan untuk menjaga bukti-bukti yang telah didapatkan dan memastikan keaslian atau integritas barang bukti agar terhindar dari pihak-pihak yang tidak berkenan, sehingga bukti tidak terkontaminasi dan benar-benar valid/sah.

3. *Collection* (Pengumpulan)

https://doi.org/10.25077/ TEKNOSI.v6i1.2020.1-8

Pada tahap ini dilakukan proses pengumpulan sampel-sampel bukti yang diduga berpotensi sebagai barang bukti yang kuat.

4. *Examination* (Pemeriksaan)
   Pada tahap ini dilakukan analisis serta filterisasi data pada bagian tertentu dari sumber data, filterisasi dilakukan dengan syarat tidak mengubah keaslian data.

5. *Analysis* (Analisis)
   pada tahap ini dilakukan penentuan tentang asal-usul sumber data, siapa yang menciptakan data tersebut, lokasi data tersebut dihasilkan, bagaimana data tersebut dihasilkan dan alasan mengapa data tersebut dihasilkan.

6. *Presentation* (Presentasi)
   Tahap ini merupakan tahap terakhir dengan melaporkan serta mempresentasikan hasil analisis sehingga dapat dipahami oleh publik.

2.1. Steganografi

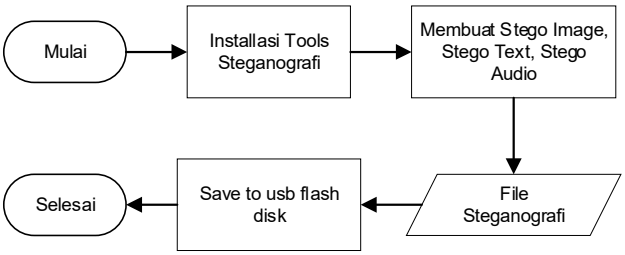
Steganografi berasal dari Bahasa Yunani yang terdiri atas dua kata yaitu "steganos" dan "graptos". Steganos berarti menyembunyikan, sedangkan graptos artinya tulisan. Jadi steganografi adalah tulisan yang disembunyikan. Teknik steganografi bertujuan untuk merahasiakan atau menyembunyikan keberadaan suatu pesan rahasia ke dalam *file* penampung. Pada umumnya, kebanyakan pesan disembunyikan dengan cara menyisipkan pesan tersebut pada data digital lain yang tidak akan menarik perhatian. Steganografi membutuhkan dua property, yaitu data dan wadah penampung. Adapun format digital yang dapat digunakan untuk menyembunyikan suatu pesan yaitu teks, *image, audio*, maupun video [15]. Teknik steganografi pada era modern menjadi sangat populer setelah terjadinya peristiwa pemboman gedung WTC di Amerika Serikat. Dilaporkan bahwa teroris saat itu menyembunyikan kegiatan terornya seperti perintah untuk aktivitas teroris pada bulletin boards porno dan website, foto-foto target, dan menyembunyikan peta-peta lokasi target dalam media penampung seperti *image, video* ataupun *audio* [16].

2.2. Steganalisis

Steganalisis merupakan seni dan ilmu untuk mendeteksi bahkan menemukan informasi tersembunyi dalam suatu objek steganografi. Tujuan dari steganalisis adalah untuk mengidentifikasi apakah suatu media yang dicurigai mempunyai pesan tersembunyi atau tidak dan jika memungkinkan, akan dilakukan proses ekstraksi pada data yang disembunyikan.

2.3. Skenario Kasus

Pada penelitian ini, sampel bukti digital yang digunakan merupakan hasil skenario layaknya kasus kejahatan komputer pada kejadian yang sebenarnya. Alur skenario pembuatan barang bukti dapat dilihat pada Gambar 2.



Gambar 2. Tahapan Skenario Pembuatan *File* Barang Bukti

2.4. Implementasi *Skenario Kasus*

Berdasarkan tahapan skenario kasus sesuai Gambar 2, pada tahap ini dilakukan implementasi penyembunyian pesan pada beberapa format *file* dengan menggunakan bantuan aplikasi anti forensik yaitu aplikasi Hiderman. Tampilan aplikasi Hiderman seperti pada Gambar 3. Untuk mengaktifkan proses penyembunyian pesan yaitu dengan cara memilih tombol Hide Files.

Gambar 3. Tampilan Aplikasi Hiderman

Implementasi yang dilakukan terhadap fungsi Hide Files pada aplikasi Hiderman dibuat dengan tujuan menyisipkan beberapa pesan tersembunyi ke dalam beberapa format *file* seperti teks, gambar, *audio* yang kemudian *file-file* tersebut disimpan pada sebuah *flash disk*.

3. HASIL DAN PEMBAHASAN

Sesuai dengan metode yang diterapkan, maka tahap investigasi untuk melakukan proses staganalisis yaitu sebagai berikut:

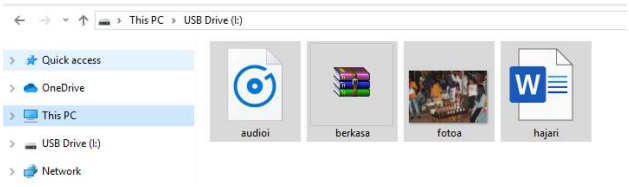
3.1. Tahap Identification

Proses identifikasi pertama kali dilakukan pada barang bukti yang didapat. Barang bukti yang didapat adalah berupa sebuah *flash disk* yang didalamnya terdapat beberapa *file* dengan format yang berbeda. Adapun spesifikasi barang bukti dapat dilihat pada Tabel

1. Sedangkan isi *file* pada *flash disk*/barang bukti dapat dilihat pada Gambar 4.

Tabel 1. Spesifikasi Barang Bukti

Gambar	Nama	Jenis	Kapasitas	*Tranfer speed*
	Kingston	*Data Traveler* ***G3***	8GB	Read: Up to 18 MB/s ** Write: Up to 5 MB/s **



Gambar 4. Daftar *File* Pada Barang Bukti *Flash Disk*

Proses identifikasi selanjutnya adalah mempersiapkan aplikasi yang akan digunakan untuk proses steganalisis. Adapun aplikasi yang akan digunakan dapat dilihat pada Gambar 5.

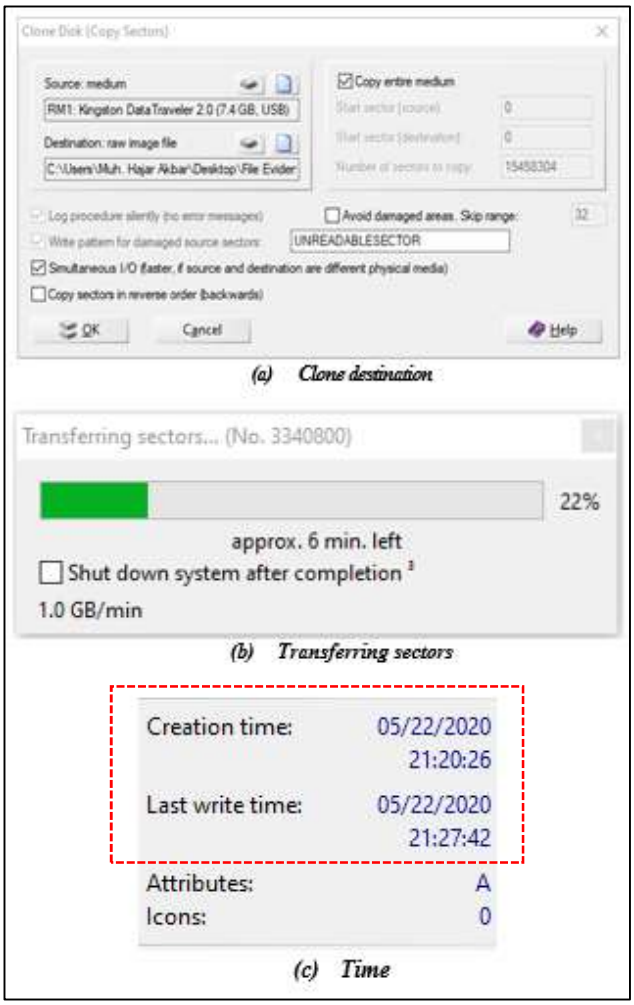
Gambar 5. Aplikasi Stegspy

Berdasarkan Gambar 5 pada aplikasi StegSpy terdapat tombol Run yang berfungsi untuk memilih *file* sekaligus melakukan deteksi dan *cracking* terhadap *file* steganografi.

3.2. Tahap Preservation

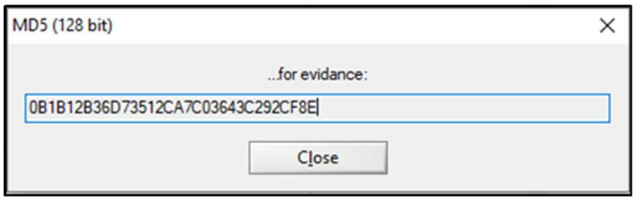
Menurut [17], barang bukti digital jika tidak ditangani dengan benar maka akan mudah terkontaminasi atau mengalami kerusakan, karena barang bukti digital bersifat rapuh,. Agar bukti yang didapat terjaga keasliannya, maka langkah selanjutnya adalah melakukan proses *cloning* pada barang bukti. Adapun alat atau aplikasi yang digunakan untuk proses *cloning* adalah menggunakan aplikasi Winhex.

Gambar 6 merupakan dimulainya proses cloning barang bukti flashdisk menggunakan aplikasi winhex. RM1:Kingston Data Traveler 2.0 (7.4 GB. USB) merupakan bukti digital asli yang akan di *cloning*, sedangkan file evidance adalah output dari hasil *cloning* tersebut yang akan tersimpan di folder C:\users\acer\Desktop. Waktu yang diperlukan untuk proses *cloning* data adalah 7 menit 42 detik.



Gambar 6. Proses *Cloning* Barang Bukti

Setelah didapatkannya file *Image*, langkah selanjutnya adalah melakukan pengecekan terhadap nilai *hash*. Gambar 7 merupakan perbandingkan nilai *hash* pada barang bukti asli dengan barang bukti hasil *cloning*.



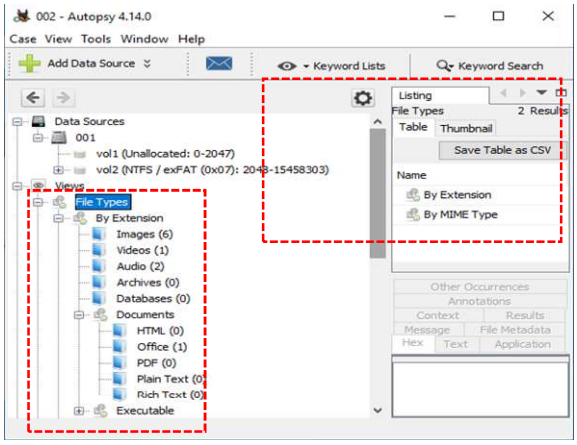
Gambar 7. Perbandingan Nilai *Hash*

https://doi.org/10.25077/ TEKNOSI.v6i1.2020.1-8

Berdasarkan Gambar 7, menunjukan bahwa nilai *hash* sebelum dilakukan *cloning* dan setelah dilakukan *cloning* adalah sama yaitu "0B1B12B36D73512CA7C03643C292CF8E". Hal ini membuktikan bahwa duplikat *file* dari hasil *cloning* identik dengan barang bukti asli.

3.3 Tahap Collection

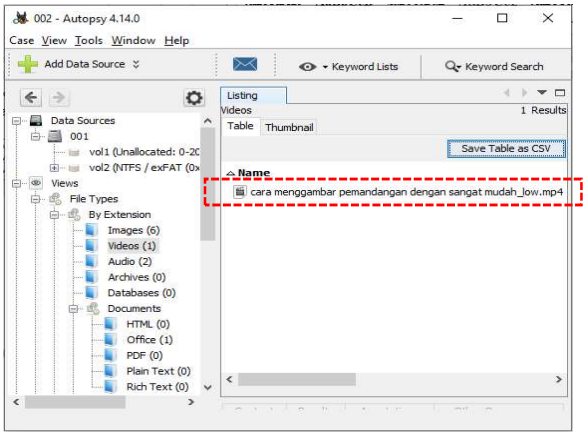
Proses selanjutnya adalah melakukan tahap pengumpulan *file-file* apa saja yang terdapat pada duplikat *file image*. Tahap pengumpulan menggunakan aplikasi Autopsy, dengan menggunakan aplikasi Autopsi investigator dapat melihat *file* apa saja yang terdapat pada *file image* hasil duplikat. Gambar 8 merupakan tampilan menu Views pada aplikasi Autopsi.



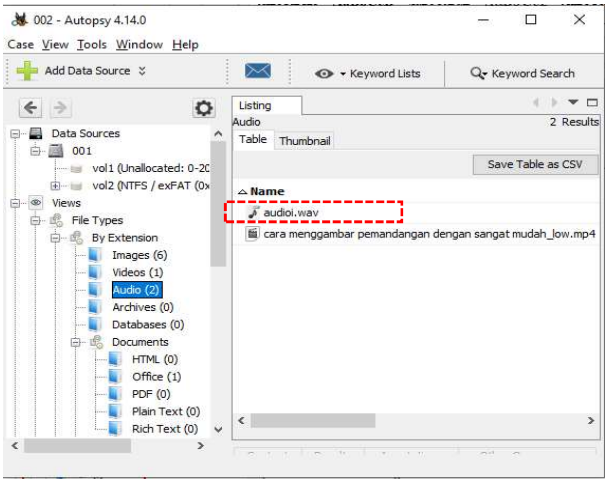
Gambar 8. Tampilan Menu Views Pada Aplikasi Autopsi

Pada menu views, investigator dapat mengetahui *file-file* apa saja yang terdapat pada salinan barang bukti. Berdasarkan informasi *file* yang terdapat pada menu views, ada beberapa format *file* yang mencurigakan yaitu *Images, Audio, Videos, dan Office*.

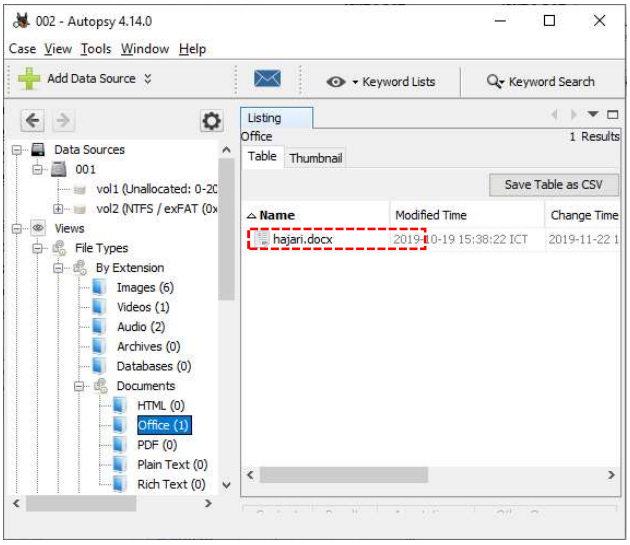
Langkah selanjutnya adalah mengekstrak ketiga *file* yang ditemukan kedalam folder yang telah ditentukan. Hal ini dilakukan untuk mengumpulkan *file* yang nantinya dilakukan proses pemeriksaan dan analisis. Gambar 9 adalah proses ektraksi *file* data yang ditemukan.



(a) File Video



(b) File Audio



(c) File document

Gambar 9. Proses Ekstraksi *File video, audio,* dan *document*

Tabel 2. *Meta Data* Daftar *File* Pada Menu Views

No	*Type*	Format	*Name*	Waktu		
				Modified	*Accessed*	*Created*
1	*File system*	*Images*	/img_evidance/vol_vol2/fotoa.JPG	2019-10-19 15:41:20 ICT	2019-10-19 15:50:07 ICT	2019-10-19 15:50:04 ICT
2	*File system*	*Videos*	/img_evidance/vol_vol2/cara menggambar	2019-10-19 16:39:53 ICT	2019-10-19 16:42:03 ICT	2019-10-19 16:41:57 ICT
3	*File system*	*Audio*	/img_evidance/vol_vol2/audioi.wav	2019-10-19 15:17:23 ICT	2019-10-19 16:41:55 ICT	2019-10-19 15:50:00 ICT
4	*File system*	*Office*	/img_evidance/vol_vol2/hajari.docx	2019-10-19 15:38:22 ICT	2019-10-19 16:41:55 ICT	2019-10-19 15:50:07 ICT

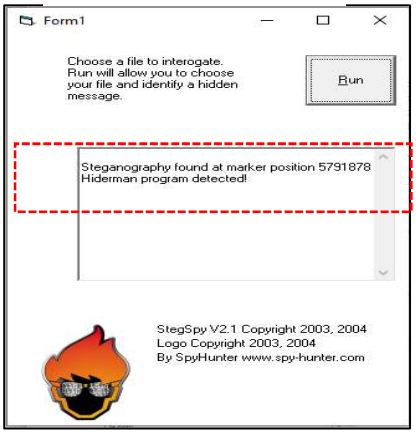
4. Examination

Pada tahap ini dilakukan pencatatan informasi *meta data* terhadap *file* bukti yang didapatkan dengan menggunakan aplikasi Autopsy. Tabel 2 menampilkan *meta data* dari *file* yang telah didapatkan.

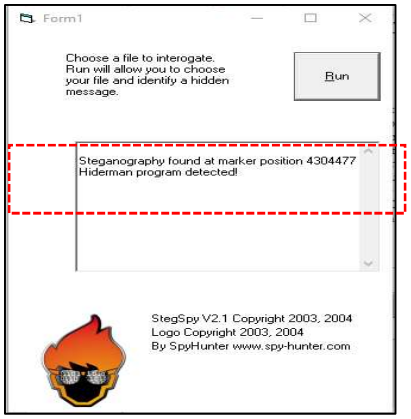
5. *Analysis*

Pada tahap ini dilakukan proses analisis terhadap data yang telah didapatkan pada tahap pengumpulan dan tahap pemeriksaan. Tahap analisis dilakukan untuk mencari informasi penting pada saat pemeriksaan, dengan cara melakukan analisis terhadap *file* bukti yang didapatkan apakah mengandung pesan rahasia yang tersembunyi di dalamnya. Pada tahap ini dilakukan proses steganalisis terhadap masing-masing *file evidance* yang telah didapatkan menggunakan aplikasi StegSpy. Gambar 10 merupakan hasil steganalisis masing-masing *file* menggunakan aplikasi StegSpy.

(a) Steganalysis File images

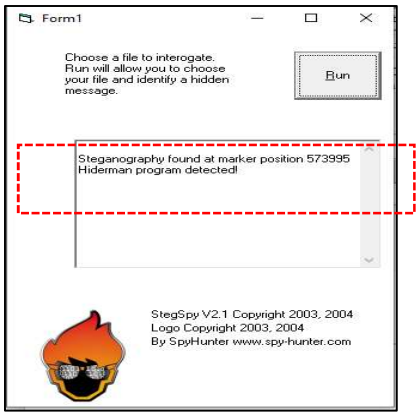


(b) Steganalysis File Video



(c) Steganalysis File Audio

(d) Steganalysis File Document



Gambar 10. Proses Steganalisis pada *File images, video, audio* dan *document*

https://doi.org/10.25077/ TEKNOSI.v6i1.2020.1-8

Berdasarkan Gambar 10, hasil analisis menggunakan tool StegSpy dengan melakukan proses *steganalysis* terhadap empat *file* yang dicurigai dengan format yang berbeda, ditemukan atau dideteksi *file* steganografi pada masing-masing file dengan *position marker* yang berbeda.

6. *Presentation*

Pada tahap ini, dilakukan proses penyajian dari hasil *steganalysis*, sehingga memberikan penjelasan tentang kesimpulan seperti pada Tabel 3.

Tabel 3. Dokumentasi Hasil *Steganalysis*

No	Nama *file*	Format *file*	Keterangan	*Marker position*	*Stego tools*
1	fotoa	.JPG	*Stego found*	5791878	Hiderman
2	cara menggambar	.mp4	*Stego found*	4304477	Hiderman
3	Audioi	.wav	*Stego found*	7135572	Hiderman
4	hajari	.docx	*Stego found*	573995	Hiderman

Berdasarkan *steganalysis* yang telah dilakukan, aplikasi StegSpy berhasil mendeteksi keberadaan pesan steganografi pada keempat *file* yang telah diberikan pesan steganografi sesui dengan skenario di awal.

7. KESIMPULAN

Berdasarkan hasil steganalisis bukti digital menggunakan metode *static forensics* yang telah peneliti lakukan, maka dapat ditarik kesimpulan yaitu file steganografi yang telah dihasilkan menggunakan *tool* Hiderman, dapat di deteksi dengan baik menggunakan *tool* StegSpy seperti yang telah ditunjukkan pada Tabel 3. Hal ini membuktikan bahwa hasil steganalisis pada media penyimpanan flash disk dengan menggunakan aplikasi StegSpy dapat dijadikan bukti digital yang sah menurut hukum. Untuk pengembangan lebih lanjut serta penyempurnaan dari penelitian ini, maka disarankan agar penelitian selanjutnya menggunakan metode yang berbeda yaitu *live forensics* dan penggunaan *tool forensics* yang berbeda pula.

DAFTAR PUSTAKA

[1] H. Aco, "Cyber Crime Tinggi, Indonesia Diminta Tingkatkan Cyber Security," *www.tribunnews.com*, 2019. https://www.tribunnews.com/techno/2019/09/14/cyber-crime-tinggi-indonesia-diminta-tingkatkan-cyber-security?page=all (accessed Sep. 14, 2019).

[2] 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.

[3] 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.

[4] 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.

[5] P. P. Amritha, M. Sethumadhavan, R. Krishnan, and S. K. Pal, "Anti-forensic approach to remove stego content from images and videos," *J. Cyber Secur. Mobil.*, vol. 8, no. 3, pp. 295–320, 2019, doi: 10.13052/jcsm2245-1439.831.

[6] F. G. Pamungkas, B. Hidayat, and N. Andini, "Implementasi Teknik Steganalisis Menggunakan Metode Improvement Difference Image Histogram Pada Steganografi LSB," in *Seminar Nasional Inovasi Dan Aplikasi Teknologi Di Industri 2017*, 2017.

[7] 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.

[8] E. Olson, L. Carter, and Q. Liu, "A Comparison Study Using StegExpose for Steganalysis," *Int. J. Knowl. Eng.*, vol. 3, no. 1, pp. 8–12, 2017, doi: 10.18178/ijke.2017.3.1.079.

[9] R. C. Novaldin, N. Sopiah, and E. S. Negara, "Penerapan Metode Steganalysis untuk Pengembalian Data pada Hard Drive," *SENTIKOM*, 2017.

[10] A. L. Suryana, R. El Akbar, and N. Widiyasono, "Investigasi Email Spoofing dengan Metode Digital Forensics Research Workshop (DFRWS)," *J. Edukasi dan Penelit. Inform.*, vol. 2, no. 2, pp. 111–117, 2016, doi: 10.26418/jp.v2i2.16821.

[11] R. A. Putra, A. Fadlil, and I. Riadi, "Forensik Mobile pada Smartwatch Berbasis Android," *JURTI*, vol. 1, pp. 41–47, 2017.

[12] 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.

[13] 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.

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

[15] A. Hafiz, "Steganografi Berbasis Citra Digital Untuk Menyembunyikan Data Menggunakan Metode Least Significant Bit (Lsb)," *J. Cendikia*, vol. 17, no. 1 April, pp. 194–198, 2019.

[16] P. S. Bin Saju, "16 Tahun Serangan '9/11': WTC Runtuh Bukan karena Tabrakan Pesawat?," *www.internasional.kompas.com*, 2017. https://internasional.kompas.com/read/2017/09/12/09575401/16-tahun-serangan-911-wtc-runtuh-bukan-karena-tabrakan-pesawat?page=all (accessed Nov. 14, 2019).

[17] A. Yudhana, R. Umar, and A. Ahmadi, "Digital Evidence Identification on Google Drive in Android Device Using NIST Mobile Forensic Method," vol. 6, no. 1, pp. 54–63, 2019.

BIODATA PENULIS

Sunardi. Lahir di Sragen, 21 Mei 1974. Penulis menyelesaikan pendidikan Strata 1 di Jurusan Teknik Elektro Universitas Gadjah Mada pada tahun 1999. Kemudian menyelesaikan pendidikan Strata 2 di Jurusan Teknik Elektro Institut Teknologi Bandung pada tahun 2003. Kemudian menyelesaikan pendidikan Strata 3 di Jurusan Teknik Elektro Universiti Teknologi Malaysia pada tahun 2011. Saat ini penulis bekerja sebagai dosen di Jurusan Magister Teknik Informatika, Universitas Ahmad Dahlan.

Imam Riadi. Lahir di Kudus pada tanggal 10 Agustus 1980. Penulis menyelesaikan pendidikan Strata 1 di Jurusan Teknik Elektro Universitas Negeri Yogyakarta pada tahun 2001. Kemudian menyelesaikan pendidikan Strata 2 di Jurusan Ilmu Komputer Universitas Gadjah Mada pada tahun 2013. Dan pada tahun 2014 kembali menyelesaikan pendidikan Strata 3 di Jurusan Ilmu Komputer Universitas Gadjah Mada. Saat ini penulis bekerja sebagai dosen di Jurusan Magister Teknik Informatika Universitas Ahmad Dahlan.

Muh. Hajar Akbar. Lahir di Latugho pada tanggal 16 Maret 1996. Penulis memperoleh gelar S.T., dalam bidang Teknik Informatika pada tahun 2017. Kemudian melanjutkan proses pendidikan Strata 2 pada Program Studi Magister Teknik Informatika di Universitas Ahmad Dahlan Yogyakarta pada tahun 2018. Saat ini penulis sedang menempuh semester II, penulis memfokuskan untuk mengkaji bidang Digital Forensik.