JISKa, Vol. 5, No. 2, SEPTEMBER, 2020, Pp. 96 – 106
ISSN : 2527 – 5836 (print) | 2528 – 0074 (online)

Steganalysis Bukti Digital pada Media *Storage* Menggunakan Metode GCFIM

Muh. Hajar Akbar [(1)], Sunardi [(2)], Imam Riadi [(3)]
Teknik Informatika, Universitas Ahmad Dahlan [(1)],
Teknik Elektro, Universitas Ahmad Dahlan [(2)],
Sistem Informasi, Universitas Ahmad Dahlan [(3)]
Jl. Prof. Dr. Soepomo, S.H., Janturan, Warungboto, Umbulharjo, Yogyakarta
e-mail : hajarakbar16@gmail.com [(1)], sunardi@mti.uad.ac.id [(2)], imam.riadi@is.uad.ac.id [(3)]

Abstract

Steganography is an anti-forensic technique that allows a criminal to hide information in other messages, so that during an examination it will be difficult to obtain evidence of the crime information. Therefore we need a technique to detect hidden messages in the data. This technique is known as steganalysis. Steganalysis is an anti-steganography science whose main purpose is to study the hiding characteristics of data on digital media and detect the existence of secret messages that are hidden using steganography techniques. The purpose of this study is to apply steganalysis techniques to detect the presence of messages that are hidden in other messages by using the forensic method, namely Generic Computer Forensic Investigation Model (GCFIM). In this study, the process of inserting steganographic messages using the Hiderman application, while the steganalysis process uses the StegSpy application. The results obtained in this study were the process of steganalysis using the help of the StegSpy application proved to be successful in detecting the presence of hidden messages in the five files that were scanned by steganographic messages.

Keywords : Steganography, Steganalysis, GCFIM, StegSpy

Abstrak

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 forensik yaitu *Generic Computer Forensic Investigation Model* (GCFIM). 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 kelima file yang diskenariokan telah disisipi pesan steganografi.

Kata Kunci : Steganografi, *Steganalysis,* GCFIM, StegSpy

1. PENDAHULUAN

Berkembangnya peradaban tidak lepas dari perkembangan teknologi dan komunikasi. Saat ini teknologi menjadi bagian paling penting dalam mengatasi permasalahan disetiap aktifitas kehidupan manusia. Sebanding dengan tingginya tingkat pemanfaatan teknologi informasi dan komunikasi, perkembangan teknologi juga memberi dampak terhadap meningkatnya kejahatan khususnya kejahatan dibidang *cybercrime* (Anwar & Riadi, 2017). Di Indonesia, selama tahun 2019 Direktorat Tindak Pidana Siber (Dittipidsiber) Bareskrim Polri mencatat terdapat 4.586 laporan kasus tindak kejahatan dengan memanfaatkan teknologi komputer (patrolisiber, 2019).

Salah satu jenis kejahatan *cybercrime* adalah penyalahgunaan teknik steganografi. Steganografi merupakan salah satu teknik yang digunakan untuk mengamankan suatu pesan

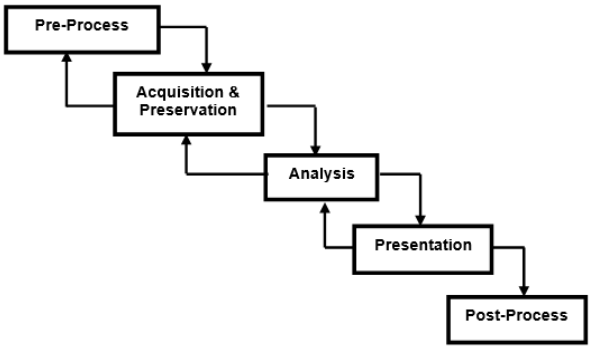
atau informasi. Kontradiksi penggunaan teknik steganografi dalam *digital forensics* adalah banyaknya pelaku kejahatan yang memanfaatkan teknik steganografi sebagai *anti forensic* dengan tujuan menutupi kejahatannya serta membuat ahli forensik kesulitan dalam melakukan investigasi (Saputra et al., 2017). Selain itu, teknik steganografi memungkinkan pelaku untuk menyembunyikan suatu informasi dengan memasukan informasi tersebut ke dalam pesan lain dalam bentuk media digital, sehingga keberadaan informasi tidak diketahui (Ardiyasa, 2018).

Kejahatan digital bermotif steganografi wajib untuk diatasi, sehingga perlu adanya panduan tentang metode dan teknik investigasi sehingga menghasilkan pembuktian secara ilmiah (Fauzan et al., 2017). Metode atau kerangka kerja forensik yang telah banyak digunakan untuk menginvestigasi kasus anti forensik diantaranya *National Institute of Justice* (NIJ) (Shrivastava, 2012), *Digital Forensics Research Workshop* (DFRWS) (Palmer, 2001), dan *Generic Computer Forensic Investigation Model* (GCFIM) (Yusoff et al., 2011). Penelitian ini menerapkan metode GCFIM. Metode GCFIM memiliki alur kerja bolak balik yang tidak dimiliki oleh metode NIJ dan DFRWS. Proses bolak-balik berarti seorang penyidik dapat kembali ketahapan sebelumnya yang disebabkan oleh situasi yang dapat berubah seperti tempat kejadian perkara (baik fisik maupun digital), alat investigasi yang digunakan, alat kejahatan yang digunakan, dan level keahlian investigator. Sehingga seorang *investigator* dimungkinkan untuk kembali ketahapan sebelumnya apabila diperlukan bukan hanya untuk memperbaiki kesalahan, tapi juga untuk mendapatkan informasi atau bukti digital yang baru. Penelitian ini memberikan gambaran terkait analisis pada bukti digital yang diduga telah disisipi pesan steganografi menggunakan metode GCFIM untuk mendapatkan bukti digital secara ilmiah sehingga dapat dipertanggungjawabkan secara hukum dalam mengungkap kasus kejahatan.

Berdasarkan studi literatur terdahulu sebagai pendukung pada penelitian ini, ditemukan penelitian dengan tema sejenis. Peneliti pertama melakukan pengujian terhadap aplikasi anti forensik agar dapat menyisipkan pesan steganografi tanpa menyebabkan pesan yang disisipkan mengalami kerusakan. Hasil penelitian yang didapat yaitu penggunaan Net Tools terbukti dapat mengamankan pesan yang akan dikirimkan melalui media internet (Utomo & Erwanto, 2019). Peneliti kedua melakukan investigasi pada aplikasi *open source* steganografi serta melakukan pengujian pada aplikasi StegExpose untuk proses steganalisis. Setelah melakukan investigasi secara komparatif, hasilnya menunjukan bahwa kemampuan dari aplikasi stegExpose sangat terbatas (Olson et al., 2017).

2. METODE PENELITIAN

Metode yang digunakan dalam penelitian ini adalah *Generic Computer Forensic Investigation Model* (GCFIM). Metode GCFIM memiliki lima langkah kerja seperti Gambar 1.



Gambar 1. Tahapan metode GCFIM

Gambar 1 merupakan tahapan metode GCFIM yang terbagi menjadi lima tahapan yaitu *pre-process, acquisition & preservation, analysis, presentation,* dan *post-process.* Secara lengkap dapat dipaparkan sebagai berikut:

Pre-process, pada tahap ini dilakukan persiapan awal sebelum dimulainya proses investigasi kasus yang berkaitan dengan barang bukti elektronik. Hal-hal yang harus dipersiapkan dan dimiliki oleh analisis *forensic* dan *investigator* adalah sebagai berikut:

1. Administrasi penyidikan berupa surat perintah penggeledahan maupun surat perintah penyitaan.
2. Nomor, skala ukur, label lembaga, serta *sticker* label kosong yang digunakan untuk memberikan penanda pada masing-masing barang bukti eletronik yg ditemukan di TKP.
3. Kamera digital yang digunakan untuk memotret TKP dan barang bukti secara *fotografi forensic* (foto umum, foto menengah dan foto *close up*).
4. Peralatan tulis yang digunakan untuk mencatat keterangan para saksi maupun spesifikasi barang bukti.
5. Formulir penerimaan barang bukti yang digunakan untuk kepentingan *chain of custody* yaitu metodologi untuk menjaga keutuhan barang bukti dimulai dari TKP.

Acquisition & preservation, pada tahap ini dilakukan pengumpulan, pengamanan, dan penyimpanan data sehingga data yang sudah di dapatkan tidak mudah dimanipulasi sehingga dapat digunakan untuk aktivitas berikutnya

Analysis, tahap ini merupakan tahapan utama dalam kegiatan penyelidikan komputer forensik. Proses yang dilakukan adalah menganalisis data yang diperoleh pada tahap sebelumnya untuk dilakukan identifikasi sumber kejahatan, motif kejahatan dan pada akhirnya menemukan pelaku tindak pidana tersebut.

Presentation, tahap ini merupakan tahap pendokumentasian dan penyampaian hasil analisis kepada pihak-pihak terkait. Tahap ini sangat penting karena hasil analisis kasus yang ditangani harus disajikan ke dalam Bahasa yang dipahami oleh pihak terkait serta harus didukung dengan bukti yang memadai dan dapat diterima. Hasil pada tahap ini berupa kesimpulan yang dapat membuktikan ataupun menyangkal suatu tindak pidana.

Post-Process, tahap ini merupakan tahapan akhir yang dilakukan oleh penyidik, yang mana bukti digital dan bukti fisik dikembalikan kepada pemiliknya yang sah dan disimpan di tempat yang aman. Pada tahap ini juga dilakukan proses *review* sebagai bahan pelajaran maupun perbaikan dimasa yang akan datang.

2.1 Alat dan Bahan

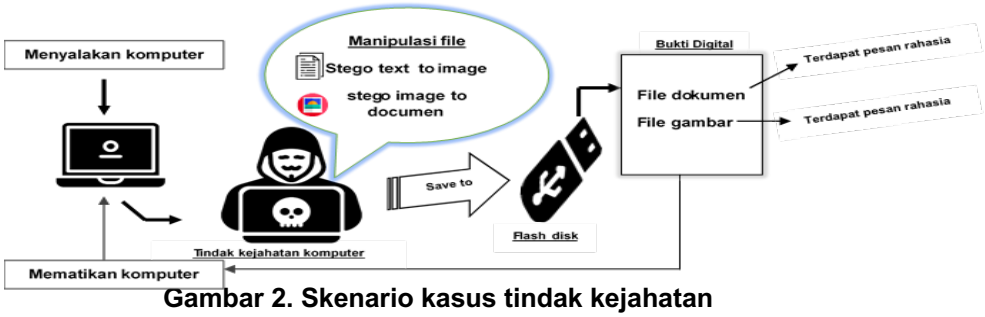
Alat dan bahan yang digunakan pada penelitian ini dapat dilihat pada Tabel 1.

Table 1. Alat dan Bahan

No	Nama Alat/Bahan	Banyak	Deskripsi/Spesifikasi	Keterangan
1	Notebook	1	* Acer Aspire E1 -431 * 4 GB DDR 3 Memory * 500 GB HDD	Perangkat keras analisis/*investigator*
2	Windows 10	1	Windows 10 Pro File sistem NTFS	Perangkat lunak sistem operasi
3	Flash Disk	1	* Kingston * Data Traveler **G3** * 8 GB	Objek penelitian/ barang bukti elektronik
3	Autopsy	-	Aplikasi berbasis Windows dan Linux yang digunakan untuk mengambil data	Perangkat lunak eksminasi
4	Winhex	-	Aplikasi berbasis Windows dan Linux yang digunakan untuk mengambil data	Perangkat lunak eksminasi
5	Hiderman	-	Aplikasi berbasis Windows yang digunakan untuk membuat pesan steganografi	*Tool* steganografi
6	Stegspy	-	Aplikasi berbasis Windows dan Linux yang digunakan untuk mengambil data yang telah di *encode* menggunakan teknik steganografi	Perangkat lunak analisis data steganografi

2.2 Skenario Kasus

Bukti digital yang digunakan pada penelitian ini merupakan hasil skenario tindak kejahatan penyembunyian pesan rahasia menggunakan teknik steganografi dengan melibatkan media penyimpanan berupa sebuah flash disk yang dapat dilihat pada Gambar 3.



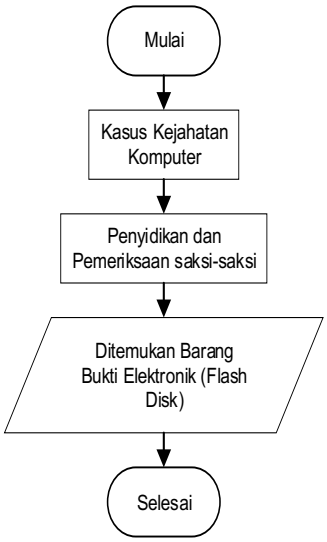
Gambar 2. Skenario kasus tindak kejahatan

Berdasarkan Gambar 2 skenario kasus pada penelitian ini dilakukan dengan cara memanipulasi beberapa *file* dengan cara menyisipkan steganografi berupa *stego text* pada *file image* serta memberikan *stego image* pada *file* dokumen. Langkah selanjutnya adalah melakukan penyimpanan beberapa kumpulan *file* tersebut dengan cara “Save as” pada flash disk yang telah dipasang pada komputer.

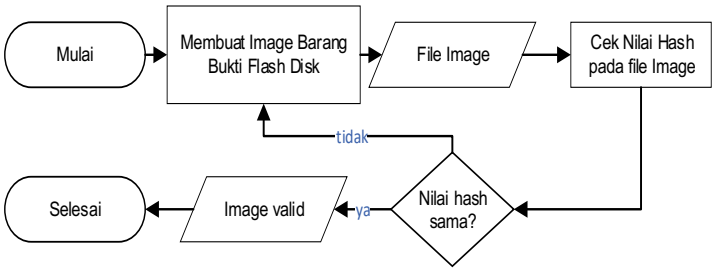
2.3 Tahap *Acquisition & Preservation*

Proses akuisisi dilakukan mengikuti rancangan skenario kasus. Barang bukti yang dijadikan objek penelitian adalah media penyimpanan berupa sebuah flash disk. Selanjutnya dilakukan *preservation* (pemeliharaan) dengan tujuan melakukan perlindungan terhadap bukti-bukti yang dapat mengalami kerusakan, perubahan maupun dilakukan penghilangan oleh pihak-pihak tertentu. Pada tahap ini proses penyelidikan tidak boleh dilakukan secara langsung pada bukti asli karena dikhawatirkan akan dapat merubah isi dan struktur *file* yang ada didalamnya. Oleh karena itu dilakukan penyalinan data secara *bitstream image* pada tempat yang yang telah ditentukan. Teknik ini umumnya diistilahkan dengan *cloning* atau *imaging* yang dilakukan

dengan cara menyalin setiap bit demi bit dari data orisinil, termasuk *file* yang ter-*defrag* (*defragmented file*), *file* temporer (*temporary file*), *file* yang tersembunyi (*hidden file*), dan *file* yang belum ter-*overwrite*. Dengan kata lain, setiap biner digit demi digit di-*copy* secara utuh dalam media baru. Data hasil *imaging* inilah yang selanjutnya dapat digunakan sebagai objek penelitian dan penyelidikan. Adapun proses *acquisition & preservation* dapat dilihat pada Gambar 3 dan Gambar 4.

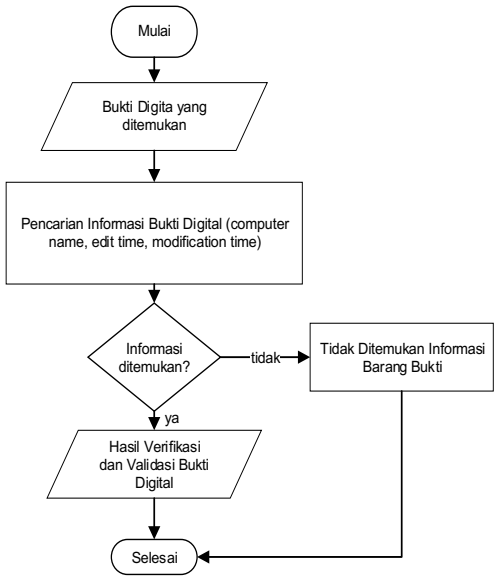


Gambar 3. Flowchart proses akuisisi barang bukti



Gambar 4. *Flowchart* tahap *preservation*

2.4 Tahap *Analysis*



Gambar 4. *Flowchart* tahap *analysis*

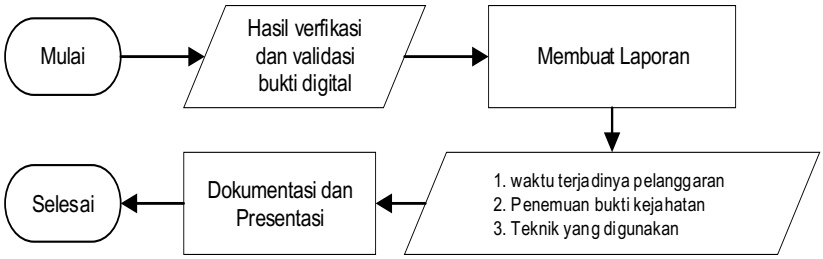
Proses *analysis* dilakukan secara mendalam berdasarkan bukti digital awal yang ditemukan, serta dilakukan analisis terhadap metadata *file* tersebut. Metadata yang berisi informasi mengenai jenis *file*, nama *file,* kapan *file* tersebut dibuat, kapan *file* tersebut dimodifikasi, dan sebagainya. Gambar 4 merupakan *flowchart* proses *analysis.*

2.5 Tahap *Presentation*

Proses *presentation* dilakukan dengan cara menyampaikan hasil analisis serta menyajikan dan menguraikan secara detail laporan penyelidikan secara mendalam dan dapat dipertanggungjawabkan kepada pihak pihak terkait. Menurut (Rosalina et al., 2015) beberapa hal penting yang perlu dicantumkan saat *presentation* yaitu sebagai berikut:

1. Tanggal dan waktu terjadinya pelanggaran.
2. Tanggal dan waktu pada saat investigasi permasalahan yang terjadi.
3. Penemuan bukti yang berharga (pada laporan akhir penemuan ini sangat ditekankan sebagai bukti penting proses penyidikan).
4. Teknik khusus yang digunakan, contoh: *password cracker*

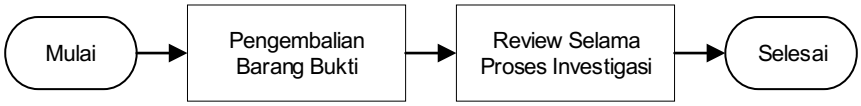
Proses *presentation* dapat dilihat berdasarkan *flowchart* pada Gambar 5.



Gambar 4. *Flowchart* tahap *presentation*

2.6 Tahap *Post-Process*

Post-process merupakan tahap akhir dalam proses investigasi. Semua barang bukti fisik dan digital dikembalikan ke pihak yang berwenCang untuk menyimpannya. *Flowchart post-process* dapat dilihat pada Gambar 5.



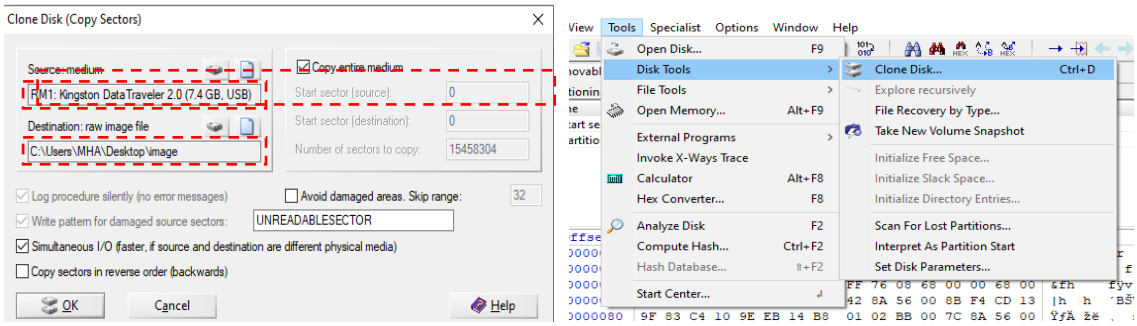
Gambar 5. *Flowchart* tahap *post-process*

3. HASIL DAN PEMBAHASAN

Hasil implementasi yang dilakukan pada penelitian ini berdasarkan skenario kasus pada Gambar 2 dengan menggunakan Flash Disk sebagai barang bukti elektronik.

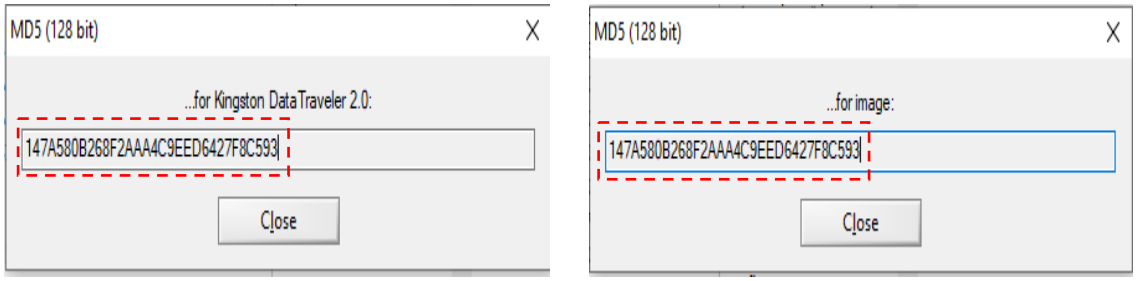
3.1 Hasil *Acquisition & Preservation*

Berdasarkan metode *statics forensics*, barang bukti fisik Flash Disk disalin dalam bentuk *image* dengan proses *bit by bit image*. Adapun alat atau aplikasi yang digunakan untuk proses *acquisition & preservation* adalah menggunakan aplikasi Winhex. Tampilan aplikasi Winhex dapat dilihat pada Gambar 6. Gambar 7 merupakan proses dimulainya *cloning* flashdisk menggunakan aplikasi WinHex. RM1:Kingston Data Traveler 2.0 (7.4 GB. USB) merupakan bukti digital asli yang akan di *cloning*, sedangkan “image” adalah *output* dari hasil *cloning* tersebut yang akan tersimpan di folder C:\users\acer\Desktop\image.



Gambar 6. Proses *clone disk*

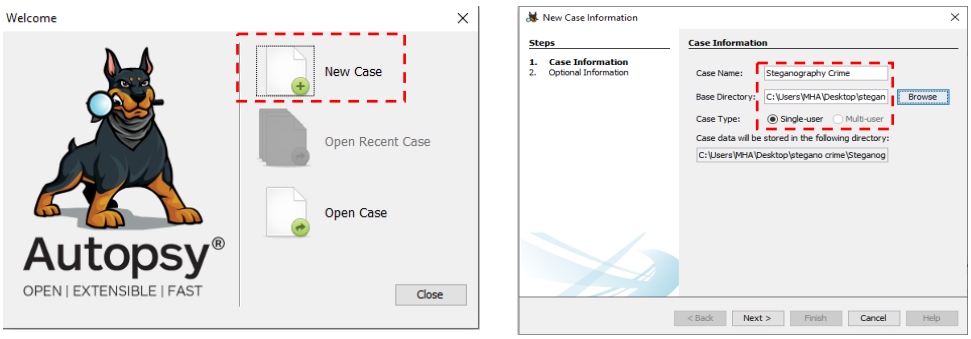
Setelah proses *imaging* dilakukan, maka selanjutnya adalah melakukan pencocokan nilai *hash* barang bukti asli (flash disk) dengan *file image* yang dibuat. Hal ini bertujuan agar barang bukti berupa Salinan (image) tidak mengalami kerusakan ataupun perubahan terhadap isi data. Gambar 7 merupakan tampilan nilai Hex dari *file* bukti asli dan hasil *imaging,* proses ini dilakukan dengan menggunakan *compute hash* MD5 (128 bit).



Gambar 7. Pencocokkan nilai *hash*

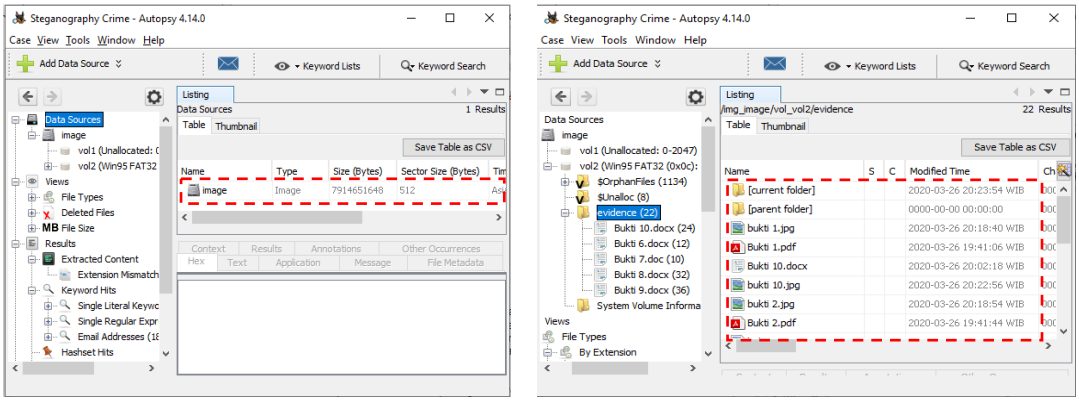
Berdasarkan Gambar 7, nilai *hash* dari *file* barang bukti asli dan *file* hasil *imaging* memiliki nilai hash yang sama yaitu “147A580B268F2AAA4C9EED6427F8C593”. Hal ini dapat disimpulkan bahwa *file image* identik dengan *file* aslinya yang kemudian dapat dipergunakan untuk tahap *analysis*. Gambar 8 merupakan proses *input* kasus (*case*) pada *tool* Autopsy.

3.2 Hasil *Analysis*



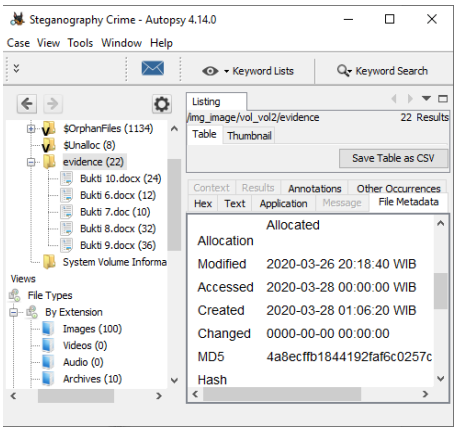
Gambar 8. Proses *input case*

Pada tahap ini dilakukan analisis terhadap *file* “image” hasil dari proses *acquisition & preservation*. Proses Analisis awal menggunakan *tool* Autopsy. Autopsy memiliki beberapa keunggulan untuk melakukan analisis dan identifikasi konten, *recovery* data maupun analisis *metadata*. Proses *input* kasus (case) pada *tool* Autopsy (Gambar 8) merupakan tahap awal dimulainya tahap analisis “image”. Gambar 9 memperlihatkan *image file* yang dibuat sebelumnya siap untuk dilakukan proses analisis.



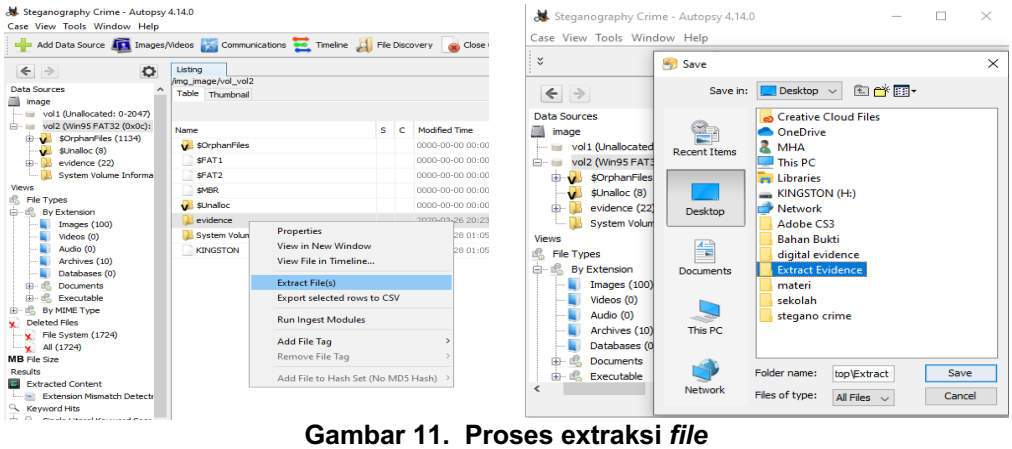
Gambar 9. *Image file* siap dianalisis

Berdasarkan Gambar 9, *tool* Autopsy dapat menampilkan *file* apa saja yang terdapat pada "image". Salah satu *file* yang dicurigai memiliki konten rahasia adalah *file* dengan nama folder "evidence". Selain itu *tool* Autopsy juga dapat menampilkan menu File Metadata yang berfungsi untuk melakukan informasi waktu terakhir data diakses, informasi waktu data tersebut dibuat, dan informasi waktu data tersebut dimodifikasi. Pada kasus ini hasil *metadata* dari folder "evidence" dapat dilihat pada Gambar 10.



Gambar 10. Informasi *metadata* folder "evidence"

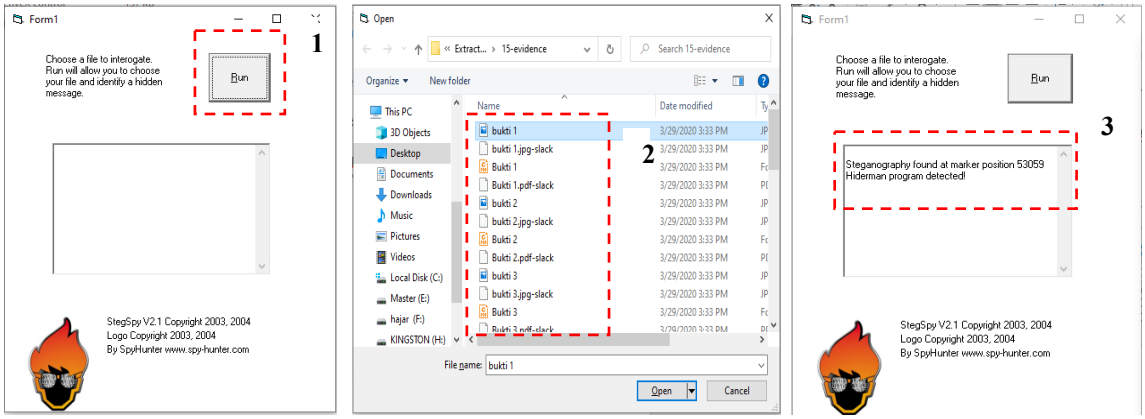
Selanjutnya dilakukan proses extraksi *file* pada folder yang dicurigai dalam hal ini folder "evidence". Proses ekstraksi bertujuan untuk mendapatkan *file* agar dilakukan analisis kembali terhadap content *file* yang dicurigai. Proses ekstraksi *file* dapat dilihat pada Gambar 11.



Gambar 11. Proses extraksi *file*

Proses selanjutnya adalah melakukan analisis mendalam pada *file* hasil ekstraksi dengan menggunakan *tool* StegSpy 2.1. *Tool* ini berfungsi untuk melakukan pengecekan keberadaan

file steganografi pada *file* bukti yang telah diekstrak pada proses analisis awal. Proses steganalisis dapat dilihat pada Gambar 12.



Gambar 12. Proses steganalisis

Berdasarkan Gambar 12, proses steganalisis berhasil mendeteksi keberadaan pesan yang disembunyikan pada setiap *file* yang dicurigai sebagai barang bukti.

3.3 Hasil *Presentation*

Pada tahap ini, dilakukan proses penyajian data dari hasil analisis, sehingga memberikan penjelasan tentang kesimpulan seperti pada Tabel 2, 3, dan 4.

Table 2. Laporan Investigasi

Tanggal Investigasi	Permasalahan	Penemuan Barang Bukti	Teknik yang Digunakan
03/29/2020	Peredaran informasi pembelian narkoba	Flash disk	Steganografi

Table 3. Laporan analisis Metadata pada file bukti yang ditemukan

No	*Type*	*Format*	*Name*	*Time*		
				Modified	***Accessed***	***Created***
1	*File System*	application/pdf	/img_image/vol_vol2/evidence/Bukti 1.pdf	2020-03-26 19:41:06 WIB	2020-03-28 00:00:00 WIB	2020-03-28 01:06:21 WIB
2	*File System*	application/vnd.openxmlformats-officedocument.document	/img_image/vol_vol2/evidence/Bukti 10.docx	2020-03-26 20:02:18 WIB	2020-03-28 00:00:00 WIB	2020-03-28 01:06:29 WIB
3	*File System*	application/pdf	/img_image/vol_vol2/evidence/Bukti 2.pdf	2020-03-26 19:41:44 WIB	2020-03-28 00:00:00 WIB	2020-03-28 01:06:29 WIB
4	*File System*	image/jpeg	/img_image/vol_vol2/evidence/bukti 4.jpg	2020-03-26 20:21:44 WIB	2020-03-28 00:00:00 WIB	2020-03-28 01:06:32 WIB
5	*File System*	image/jpeg	/img_image/vol_vol2/evidence/bukti 5.jpg	2020-03-26 20:21:56 WIB	2020-03-28 00:00:00 WIB	2020-03-28 01:06:35 WIB

Table 4. Laporan hasil steganalisis

No	Nama File	Format	Keterangan	*Marker Position*	*Stego Tools*
1	/img_image/vol_vol2/ evidence/Bukti 1.pdf	application/pdf	*Steganography found*	1512448	hiderman
2	/img_image/vol_vol2 /evidence/Bukti 10.docx	application/vnd.openxmlformats-officedocument.wordprocessingml. document	*Steganography found*	2080330	hiderman
3	/img_image/vol_vol2/ evidence/Bukti 2.pdf	application/pdf	*Steganography found*	1583902	hiderman
4	/img_image/vol_vol2/ evidence/bukti 4.jpg	image/jpeg	*Steganography found*	65194	hiderman
5	/img_image/vol_vol2/ evidence/bukti 5.jpg	image/jpeg	*Steganography found*	55867	hiderman

4. KESIMPULAN

Berdasarkan hasil penelitian dengan melakukan proses steganalisis pada barang bukti digital flash disk dengan menggunakan metode GCFIM, maka didapatkan kesimpulan sebagai berikut:

1) Analisis bukti digital pada flash disk berhasil diterapkan dengan baik menggunakan metode GCFIM. Hal ini dibuktikan dengan ditemukannya 5 jenis *file* dengan format .doc, .pdf, dan .jpg yang telah disisipi *file* steganografi.
2) Penggunaan tool Winhex berhasil diterapkan untuk mencocokkan nilai hex antara barang bukti asli dan *file image* yang telah dibuat,sehingga dapat membantu para penegak hukum dalam melengkapi persyaratan *Rules Of Evidence* dan *Chain of Chustody*.
3) Teknik steganalisis dengan menggunakan aplikasi StegSpy berhasil mendeteksi keberadaan pesan tersembunyi dalam suatu *file*. Pada penelitian ini aplikasi StegSpy sangat akurat.

Untuk pengembangan lebih lanjut serta penyempurnaan dari penelitian ini, maka saran peneliti terkait steganalisis pada bukti digital adalah sebagai berikut:

1) Penggunaan *tool* forensik yang berbeda diharapakan memberikan banyak informasi dari data hasil *acquisition & preservation*, karena tool forensik memiliki kekurangan dan keunggulan masing-masing.
2) Proses penyisipan *file* steganografi menggunakan aplikasi selain Hiderman serta proses steganalis menggunakan aplikasi selain Stegspy.

DAFTAR PUSTAKA

Anwar, N., & Riadi, I. (2017). Analisis Investigasi Forensik WhatsApp Messanger Smartphone Terhadap WhatsApp Berbasis Web. *Jurnal Ilmiah Teknik Elektro Komputer Dan Informatika*, *3*(1), 1. https://doi.org/10.26555/jiteki.v3i1.6643

Ardiyasa, I. W. (2018). Implementasi Teknik Data Hidding Untuk Pengamanan Pesan Rahasia Pada Media Digital. *Seminar Nasional Sistem Informasi Dan Teknologi Informasi 2018*, 601–605.

Fauzan, A., Riadi, I., & Fadlil, A. (2017). Analisis Forensik Digital Pada Line Messenger Untuk Penanganan Cybercrime. *Annual Research Seminar (ARS)*, *2*(1), 159–163. http://seminar.ilkom.unsri.ac.id/index.php/ars/article/view/832/752

Olson, E., Carter, L., & Liu, Q. (2017). A Comparison Study Using StegExpose for Steganalysis. *International Journal of Knowledge Engineering*, *3*(1), 8–12. https://doi.org/10.18178/ijke.2017.3.1.079

Palmer, G. (2001). A road map for digital forensic research. *Proceedings of the Digital Forensic Research Conference, DFRWS 2001 USA*, iii–42.

patrolisiber. (2019). *Statistik Jumlah Laporan Polisi yang dibuat masyarakat*. Patrolisiber.Id. https://patrolisiber.id/statistic

Rosalina, V., Herli, D., Informasi, F. T., Raya, U. S., Informasi, F. T., Raya, U. S., Forensik, D., Model, P., Framework, Z., & Clark, J. G. (2015). *Pengembangan Model Tahapan Digital Forensic Untuk Mendukung*. 0–5.

Saputra, A. P., Mubarok, H., & Widiyasono, N. (2017). Analisis Digital Forensik pada File Steganography (Studi kasus : Peredaran Narkoba). *Jurnal Teknik Informatika Dan Sistem Informasi*, *3*(1), 179–190. https://doi.org/10.28932/jutisi.v3i1.594

Shrivastava, G. (2012). *Forensic Computing Models: Technical Overview*. 207–216. https://doi.org/10.5121/csit.2012.2222

Utomo, Y. B., & Erwanto, D. (2019). Analisa Teknik Steganografi dan Steganalysis Pada File Multimedia Menggunakan Net Tools dan Hex Editor. *Generation Journal*, *3*(1), 16–22. https://doi.org/10.29407/gj.v3i1.12698

Yusoff, Y., Ismail, R., & Hassan, Z. (2011). Common Phases of Computer Forensics Investigation Models. *International Journal of Computer Science and Information Technology*, *3*(3), 17–31. https://doi.org/10.5121/ijcsit.2011.3302