PENERAPAN METODE STEGANALYSIS UNTUK PENGEMBALIAN DATA PADA HARD DRIVE

Rifki Caesar Novaldin[1], Nyimas Sopiah[2], Edi Surya Negara[3]
[1,2,3] Universitas Bina Darma
Jalan Jenderal Ahmad Yani No.3 Palembang
[1]rifkicaesarnovaldin@gmail.com, [2]nyimas_sopiah@mail.binadarma.ac.id, [3]e.s.negara@binadarma.ac.id

ABSTRACT

Steganography is the art and science of concealing information in such a way that only the sender and intended recipient. Steganography have received a great deal of attention this day. With the development of steganography technique, then the possibility of misuse will be even greater. Therefore, it is necessary to develop a counter steganography, steganalysis. There is an opinion that says "something will be scary if we can not see its physical form", maybe this term is quite similar to reason for the development of steganalysis. Steganalysis is the study of the characteristics of concealment of data on the media and how to detect even to unpack the hidden data.
Keywords: Steganography, Steganalysis.

1. PENDAHULUAN

Dulu sebelum adanya komputerisasi secanggih sekarang ini, berkas hanya memiliki bentuk fisik seperti, kertas dokumen, foto cetak dan sebagainya. Namun sekarang berkas memiliki 2 bentuk yaitu, fisik dan digital. Berkas digital sendiri memiliki berbagai macam jenis seperti dokumen, gambar, suara, video dan sebagainya. Salah satu perbedaan dari berkas fisik dan berkas digital ialah format. Format adalah informasi dasar yang mengandung data pembeda yang berada didalam suatu berkas. Contohnya adala berkas yang memiliki format .doc dan .pdf adalah dua berkas ber-format berbeda namun memiliki jenis yang sama yaitu dokumen. Pengamanan berkas digital ini penting dilakukuan untuk tetap menjaga integritas data melalui pengimplemtasian bebetap metode pengamanan computer dan jaringan (Negara, E.S 2014, Negara, E.S. 2013).

Suatu berkas digital biasanya disimpan dalam sebuah *hard drive*. *Hard drive* sendiri sering dijadikan barang bukti untuk suatu kasus digital forensik. Data dari *hard drive* yang menjadi barang bukti harus disalin ke *hard drive* ataupun media penyimpanan lainnya yang kapasitasnya sama atau lebih besar dalam bentuk image. *Hard drive* tersebut tidak boleh diperiksa langsung karena dapat menghilangkan status barang bukti benda tersebut. *Hard drive* yang menjadi barang bukti sangat jarang ditemukan dalam keadaan kosong atau telah dihapus isinya. Namun jika *hard drive* yang menjadi barang bukti dalam keadaan kosong, Hal yang dapat dilakukan terhadap *hard drive* yang telah dikosongkan tersebut adalah mengambil kembali data yang terhapus atau lebih dikenal dengan istilah *recovery data.* Untuk dapat mengembalikan data dengan utuh diperlukan suatu pendekatan yang disebut dengan ilmu forensik. Ilmu forensik adalah penerapan ilmu pengetahuan untuk menyelesaikan permasalahan hukum. Dalam forensik, hukum dan ilmu pengetahuan akan selalu menyatu. Kedua hal itu tak dapat diterapkan jika tidak menyertakan yang satunya. Barang bukti yang paling ilmiah sejagat raya sekalipun takkan berharga jika tak sesuai dengan pengadilan hukum. (Sammons, 2012). Bukan hanya subjek yang berubah dan meluas, prosesnya pun banyak mengalami perubahan. Ilmu forensik pun meluas ke bidang-bidang teknologi baru. Bahkan saat ini terdapat istilah Komputer Forensik yang mulai mencuat akhir-akhir ini. (Sulianta, 2008).

Kasus yang melibatkan *hard drive* sebagai barang bukti biasanya adalah kasus pembunuhan berencana, kasus pencabulan anak dibawah umur, dan tindak kejahatan lainnya. Pada kasus pembunuhan berencana mereka bisa menggunakan pesan yang sudah disembunyikan didalam gambar sebagai media kode mereka dan hanya merekalah yang tau tentang suatu yang ada pada gambar tersebut. Hal ini biasa disebut dengan *steganography*, *Steganography* dapat dipandang sebagai kelanjutan *cryptography*. Jika pada *cryptography*, data yang telah disandikan tetap tersedia, maka dengan *steganography* data tersebut dapat disembunyikan sehingga pihak ketiga tidak mengetahui keberadaannya. Sebaliknya, *Steganalysis* adalah ilmu untuk mendeteksi suatu pesan yang telah disembunyikan menggunakan *Steganography*. Tujuan utama dari *Steganalysis* adalah untuk mengidentifikasi paket mencurigakan, melihat apakah berkas tersebut ditutupi sesuatu dan membuka penutup pada berkas tersebut, jika memungkinkan. Oleh karena itu penulis tertarik untuk mengetahui penerapan metode *steganalysis* pada *hard drive* yang sudah sengaja dikosongkan dan didalamnya berisi berkas yang disembunyikan oleh *steganography.* Steganography adalah ilmu dalam menyisipkan pesan rahasia didalam suatu media seperti teks, gambar, suara dan video. Sama halnya dengan teknologi komunikasi modern manapun, steganography dapat disalahgunakan oleh para pelaku tindak kejahatan dalam perencanaan suatu tindak kejahatan. Dengan menyisipkan suatu pesan didalam

suatu berkas gambar dan menyebarkannya ke suatu situs publik, Dalam pengusutan komunikasi dan pencarian penerima pesan tersebut terbilang sulit. Demi mengurangi efek negatif tersebut dikembangkanlah teknik steganalysis. Steganalysis adalah suatu ilmu untuk mengungkap steganography. (Chhikara, 2013).

Adapun tujuan dari penelitian ini adalah melakukan *steganalysis* dan melewati keamanan kode *password* pada berkas yang sudah dilakukan steganography dan melakukan pengembalian berkas yang sudah dilakukan *steganography* pada *hard drive* yang sudah diformat.

2. METODOLOGI PENELITIAN

2.1 Metode Penelitian

Dalam penelitian ini metode penelitian yang digunakan adalah metode penelitian eksperimen. Penelitian eksperimen dapat dikatakan sebagai metode penelitian yang digunakan untuk mencari pengaruh perlakuan tertentu terhadap yang lain dalam kondisi yang terkendalikan.

2.2 Metode Pengumpulan Data

Metode dalam pengumpulan data yang digunakan untuk penelitian ini adalah Kajian kepustakaan (studi literatur)dimana sumber data utama dalam penelitian ini berasal dari buku, jurnal-jurnal ilmiah, artikel ilmiah, internet, laporan yang berkaitan dengan komputer forensik dan *steganalysis.* Eksperimen yang akan dilakukan pada penelitian ini adalah eksperimen penerapan metode *steganalysis* untuk pengembalian data pada *hard drive* untuk mengetahui cara kerja *steganalysis* pada data yang sudah dihapus.

3. HASIL

3.1 *Cloning* Pada *Hard Drive*

Sebelum melakukan pengembalian data, peneliti akan melakukan proses *cloning* guna menjaga status barang bukti *hard drive* yang menjadi objek penelitian. proses *cloning* yang dilakukan menggunakan *testdisk*. Proses *cloning* ini berlangsung selama 30 sampai dengan 60 menit.

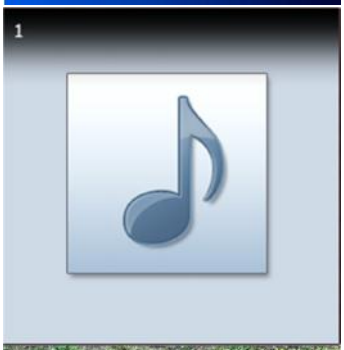
.

Gambar 1. Proses Cloning

3.2 Steganalysis

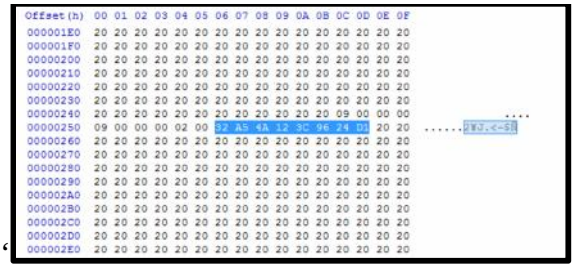
Setelah proses *cloning* dan pengembalian data selesai, barulah proses *Steganalysis* akan dilakukan pada semua berkas yang akan diteliti. Berkas-berkas yang penulis pakai disini ialah berkas-berkas yang memiliki format *.jpg,.mp3* dan *.mp4.* Proses *steganalysis* ini dilakukan dengan menggunakan program *HxD*. Untuk melakukan pencarian berkas tersembunyi pada *image hard drive*, penulis melakukan cara *copy* beberapa baris heksadesimal awal dan akhir berkas yang akan dicari, lalu melakukan perintah *find* pada *HxD* untuk mencari berkas tersebut. Lalu melihat apakah sesudah heksadesimal akhir tersebut masih memiliki data atau tidak. Jika setelah heksadesimal akhir tersebut masih tertulis suatu data, maka dapat dipastikan bahwa berkas tersebut adalah berkas yang disembunyikan.

Tabel 1. Heksadesimal Akhir dan Teks

Berkas	Hexadesimal Akhir	Teks
	Sebelum Steganography: EA D4 EB 42 9A 7B 41 0D 4C F1 A0 07 87 CF 20 67 22 BF 6F 5F FF D9	Sebelum Steganography: êÔëBš{A.Lñ .‡Ï g"¿o_ÿÙ
	Setelah Steganography: E0 42 00 00 FA 56 00 00 02 00 44 F0 18 50 79 C7 66 88	Setelah Steganography: àB..úV....Dð.PyÇfˆ
	Sebelum Steganography: C4 0C 02 40 2A AC 01 C3 00 01 45 33 2E 39 39 2E 33 55 55 55 55	Sebelum Steganography: Ä..@*¬.Ã..E3.99.3UUUU
	Setelah Steganography: FB 71 87 AB D2 01 50 4B 05 06 00 00 00 00 01 00 01 00 5F 00 00 00 AA 35	Setelah Steganography: ûq‡«Ò.PK....._...ª5
	Sebelum Steganography: 1F 41 9B 73 34 A4 C1 11 FF 00 02 A9 84 5A 7F 32 DB AD 4D 00 3B 3B 60 33 0C 51 EA 82 ED 05 C9 E3	Sebelum Steganography: .A›s4¤Á.ÿ..©„Z.2Û.M.;;‘3.Qê‚í.Éã
	Setelah Steganography: 20 20 20 74 A4 54 10 22 97 20 20 20 20 20 20 20 20 20 20 20	Setelah Steganography: t¤T."— ..

Pada gambar ubur-ubur adalah berkas yang disembunyikan menggunakan program *camouflage*. Setiap berkas yang telah disembunyikan *camouflage* akan selalu berakhiran dengan heksadesimal 74 A4 54 dan dilanjutkan serta didahului oleh beberapa heksadesimal 20. Jika data yang terletak diantara kumpulan heksadesimal akhir 20 berjumlah 10 buah maka dapat dipastikan bahwa berkas tersebut belum diberi kata sandi, namun jika data tersebut lebih dari 10 buah, itu artinya berkas tersebut sudah diberi kata sandi. pengambilan kembali berkas yang telah disembunyikan oleh *camouflage* dan tak bersandi dengan menggunakan *camouflage* itu sendiri.

Berkas baru dibuat dan di*steganography* dengan kata sandi 00000000 menggunakan *camouflage.* Tindakan selanjutnya adalah merubah heksadesimal kata sandi plainteks dan algoritma *camouflage* ke dalam biner agar dapat dilakukan enkripsi *XOR* guna mendapatkan kata sandi berkas sebelumnya.



Gambar 2. Berkas Baru Dengan Kata Sandi

Pada tabel 2, 3, dua plainteks yang harus diketahui heksadesimal dan binernya guna mendapatkan heksadesimal pada 4. Heksadesimal pada tabel 4 adalah heksa desimal yang bisa dipakai pada kata sandi *camouflage* mana pun dengan digit 8.

Tabel 2. Heksadesimal dan biner dari 2¥J.<–$Ñ

Heksadesimal	Biner	Plainteks
32 A5 4A 12 3C 96 24 D1	0011 0010 1010 0101 0100 1010 0001 0010 0011 1100 1001 0110 0010 0100 1101 0011	2¥J.<–$Ñ

Tabel 3. Heksadesimal dan biner dari 00000000

Heksadesimal	Biner	Plainteks
30 30 30 30 30 30 30 30	0011 0000 0011 0000 0011 0000 0011 0000 0011 0000 0011 0000 0011 0000 0011 0000	00000000

Tabel 4 Heksadesimal dan biner dari z"

Heksadesimal	Biner	Plainteks
02 95 7A 22 0C A6 14 E1	0000 0010 1001 0101 0111 1010 0010 0010 0000 1100 1010 0110 0001 0100 1110 0001	z"

Pada tabel 5, menggunakan heksadesimal dan biner dari kata sandi acak *caomouflage*, pada tabel 6 menggunakan heksadesimal dan biner dari hasil *XOR* sebelumnya. Dilakukanlah *XOR* pada kedua heksadesimal dan biner tersbut, diperolehlah haril plainteks dari kata sandi acak *camouflage* yaitu "Februari".

Tabel 5. Heksadesimal dan biner dari Dð.PyÇfˆ

Heksadesimal	Biner	Plainteks
44 F0 18 50 79 C7 66 88	0100 0100 1111 0000 0001 1000 0101 0000 0111 1001 1100 0111 0110 0110 1000 1000	Dð.PyÇfˆ

Tabel 6. Heksadesimal dan biner dari z"

Heksadesimal	Biner	Plainteks
02 95 7A 22 0C A6 14 E1	0000 0010 1001 0101 0111 1010 0010 0010 0000 1100 1010 0110 0001 0100 1110 0001	z"

Tabel 7. Heksadesimal dan biner dari Februari

Heksadesimal	Biner	Plainteks
46 65 62 72 75 61 72 69	01000110 01100101 01100010 01110010 01110101 01100001 01110010 01101001	Februari

4. SIMPULAN

Setelah dilakukan ujicoba dan evaluasi hasil terhadap *hard drive* yang berisi berkas *steganography* maka dapat disimpulkan :

1) Meskipun *file system* pada *hard drive* diganti, heksadesimal pada berkas yang ada pada *hard drive* tersebut akan tetap sama..

2) Pada saat proses pengembalian data, program *testdisk* dan *photorec* bekerja dengan baik, namun *photorec* melakukan perubahan terhadap nama berkas dari nama yang sebelumnya.
3) *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.
4) Teknik *steganography* dengan menggunakan *command prompt* dideteksi dengan mudah dibandingkan dengan menggunakan program aplikasi *steganography* seperti *camouflage*.

DAFTAR PUSTAKA

Chhikara, Rita, 2013. *A Review on Digital Image Steganalysis Techniques Categorised by Features Extracted*.

Dwi, Anggit, Hartanto, 2011. *Penerapan Teknik Komputer Forensik untuk Pengembalian dan Penghapusan Berkas Digital.*

Edi, S.N., 2014. Optimasi End Users Awareness of Data and System Securities Using IT Audit Methodology and Tools. In Seminar Nasional Teknologi Informasi dan Komunikasi (SNASTIKOM 2014) (Vol. 2, pp. 269-274). Sekolah Tinggi Teknik Harapan (STTH) Medan.

Grenier, Christophe, 2007. *TestDisk, Data Recovery.* (Online).(Diakses di http://www.cgsecurity.org/wiki/TestDisk, 28-11-2016).

Horz, Mael, 2009. *HxD*-Freeware Hex Editor and Disk Editor. (Online). (Diakses di https://mh-nexus.de/en/hxd, 28-11-2016).

Ibrahim, Ahmed, 2007. *Steganalysis in Computer Forensics.* (Online). (Diakses di http://ro.ecu.edu.au/cgi/viewcontent.cgi?article=1009&context=adf , 19-10-2016).

Kaur, Manveer, 2014. *Review of Various Steganalysis Techniques.* (Online). (Diakses di http://ijcsit.com/docs/Volume%205/vol5issue02/ijcsit20140502179.pdf, 24-10-2016).

M., Josua Sinambela, 2011, *Computer Forensic.* (Online). (Diakses di http://josh.rootbrain.com/seminar/Computer%20Forensic-Josua-M-Sinambela.pdf , 24-11-2016).

Munir, Rinaldi, 2004, *Kriptografi.* (Online). (Diakses di http://informatika.stei.itb.ac.id/~rinaldi.munir/Kriptografi , 22-12-2016).

Negara, E.S., 2014. Implementasi Management Network Security Pada Laboratorium CISCO Universitas Bina Darma. Jurnal Ilmiah Matrik, 16(1), pp.11-20.

Negara, E.S., Rachman, B. and Lutfi, A., 2013. Analysis and Design of Information Security Management System (ISMS) at Computer Network Infrastructure of Bina Darma University.

Sammons, John, 2012, *Basics of Digital Forensics.* (Online). (Diakses di http://store.elsevier.com/The-Basics-of-Digital-Forensics/John-Sammons/isbn-9781597496629 , 26-11-2016).

Sloan, Thomas, 2015, *Forensic Analysis of Video Steganography Tools.* (Online). (Diakses di https://peerj.com/articles/cs-7 , 19-10-2016).

Sulianta, Feri, 2008, *Komputer Forensik.* (Online). (Diakses di http://www.bukabuku.com/browses/product/9789792727715/komputer-forensik.html, 29-11-2016).