DATA HIDING DAN DATA DESTRUCTION PADA ANTI FORENSIK KOMPUTER

Naikson Fandier Saragih

Program Studi Teknik Informatika, Fakultas Ilmu Komputer,
Universitas Methodist Indonesia
Jl. Hang Tuah No. 8 Medan, 20152

saragihnaikson@gmail.com

ABSTRAK

Anti Forensik dibutuhkan untuk mengamankan suatu bukti digital pada saat orang yang tidak berhak berusaha mendapatkan data digital. Metode *Data hiding* dan *data destruction* dapat digunakan untuk melakukannya. Penelitian ini menganalisis dan mengimplementasikan kedua metode tersebut dengan menggunakan Teknik steganografi, kriftografi, penyembunyian partisi, pemecahan file dan, penghapusan file pada media hardisk/flashdisk. Analisis pada aspek file system dan Pengujian menggunakan tools anti forensic dan pengujian kekuatan menggunakan tools forensik

Kata Kunci: *Data Hiding, Data Destruction, steganografi, kriftografi, tools forensic dan anti forensic*

1. PENDAHULUAN

Data digital milik perusahaan dalam kondisi tertentu perlu diamankan dalam beberapa situasi. Situasi pertama dimana data tidak diperlukan lagi, tetapi data diinginkan tidak menjadi konsumsi di luar perusahaan misalkan laptop perusahaan yang akan dilelang, data pada hardisk perlu dikosongkan dalam kondisi aman. Untuk situasi ini dapat diadopsi teknik anti forensic data destruction. Situasi kedua dimana data masih diperlukan dan masih digunakan, tetapi data dinginkan tidak menjadi konsumsi orang yang tidak berhak misalnya data yang akan dikirimkan ke orang lain melalui jalur internet yang tidak aman, data pada flashdisk atau hardisk, dan lain-lain.Untuk situasi ini dapat diadopsi teknik anti forensic data hiding. Hardisk dan flashdisk hingga saat ini secara umum masih digunakan sebagai media penyimpanan data digital saat ini yang menjadi target anti forensic sehingga bagaimana melakukan ujicoba anti forensic untuk penyembunyian (*hiding*) dan penghapusan (*destruction*) file pada media hardisk dan flashdisk dan menguji efektivitaasnya menggunakan tools anti forensik. Adapun tujuan penelitian ini adalah mencari parameter-parameter penting dalam melakukan ujicoba anti forensik secara benar dan mengimplementasikan anti forensik : *data hiding* dan *data destruction* serta melakukan pengujian efektivitas anti forensik yang dilakukan

ANTI FORENSIC

Anti Forensic merupakan sebuah studi tentang teknik dan tools dengan tujuan menghalangi tools computer forensic, investigator dan proses forensic lainnya dengan cara menyembunyikan (*hiding*) atau menghancukan (destroying) data dan meta data[1]. anti-forensik adalah *"sebuah tindakan negatif yang dilakukan untuk mempengaruhi keberadaan, jumlah, dan atau kualitas barang bukti yang ada di lokasi kejadian, atau membuat pemeriksaan terhadap barang bukti tersebut menjadi sulit bahkan hingga tidak mungkin untuk dilakukan"*.

*Antiforensics is more than technology. It is an approach to criminal hacking that can be summed up like this: Make it hard for them to find you and impossible for them to prove they found yo*u.Anti Forensic adalah pendekatan terhadap hacking kriminal dengan moto "Buatlah sulit bagi mereka untuk menemukan Anda dan tidak mungkin mereka membuktikan bahwa mereka menemukan Anda" [2].

anti-forensics methods which in sense is how information obfuscation is affecting digital forensic investigation. Anti Forensic yang dalam arti adalah bagaimana merubah data (information obfuscation) sehingga menyulitkan penyelidikan forensik digital [3]

Tujuan Anti Forensik

Ada empat tujuan Anti forensic secara umum :

1. Menghindari deteksi bahwa beberapa hal telah terjadi
2. Mengacaukan (*Disrupting*) usaha mendapatkan /mengumpulan informasi
3. Membuat waktu lebih lama bagi pemeriksa (examiner) dalam melakukan pelacakan
4. Memunculkan keraguan pada laporan forensic atau testimoni [3]

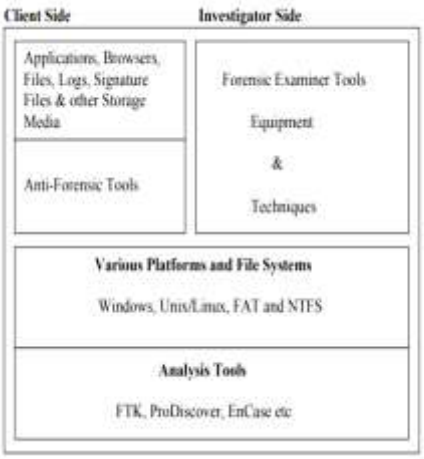
Teknik Anti Forensik

Teknik Anti Forensik berusaha untuk membuat putus asa investigator forensic dan teknik forensic yang digunakan[3]

Tools Forensic Toolskits

METODOLOGI

1. Melakukan Studi Literatur untuk mendapatkan objek yang layak/urgen menjadi objek baik dari sisi tipe file maupun medianya serta dasar pertimbangannya.
2. Ujicoba anti forensic mengunakan tools anti forensic dan
3. Uji efektivitas anti forensic menggunakan tools Forensik
4. Kerangka ujicoba menggambarkan berbagai jenis tools yang digunakan seperti ditunjukkan pada gambar di bawah ini :



Gambar 1 Kerangka Ujicoba

PENGUJIAN

Pada penelitian ini ujicoba menggunakan beberapa tools anti forensic berdasarkan 3 parameter pengujian :

1. *Time for deletion (TFD) (Quick, Fast, Moderate, Slow)*:Penghapusan diharapkan dapat berlangsung dengan cepat
2. *Percentage of deletion (POD) (100%)* : Penghapusan diharapkan dalam prosentase yang tinggi
3. Impact *of the anti forensic tool (IOAF) on FTK (Excellent, Good, Satisfactory, Unsatisfactory)* : File seharusnya tidak dapat diambil kembali oleh FTK

Penyembunyian Data

Berikut ini beberapa tools yang digunakan untuk uji coba Penyembunyian data untuk steganografi (tabel 1), penyembunyian partisi (tabel 2)

Tabel 1 Tools Anti Forensik penyembunyian data Teknik Steganografi

Tools Anti forensic	Objek	Data Penampung	Tools Uji Efektivit-as Anti Forensik
Invisible secret	file, Image (*.jpg,png,bmp), audio (*.wav), html(*.html)	Image,audio, html	Autopsy, Xsteg
OurSecret	Doc(*.doc, *.ppt, *.xls, *.txt), image(*.jpg,.png.bmp), Audio(*.wav,.mp3)	Dokumen, audio,video,	

Tabel 2 Tools Anti Forensik penyembunyian data (Teknik Penyembunyian Partisi)

Tools Anti forensic	Objek	Data Penampung	Tools Uji Efektivitas Anti Forensik
DISKPART (Windows Command Promp)	File, Folder, Partisi	Storage (hardisk, flashdisk)	Autopsy, FTK Imager, dan OSForensics
Minitool Partition Wizard	File, Folder, Partisi	Storage(hard isk, flashdisk)	

Data Destruction(Pengrusakan Data)

Berikut ini beberapa tools yang digunakan untuk uji coba pengerusakan data Teknik pemecahan file (tabel 3), Penghapusan (tabel 4), Pengformatan (tabel 5).

Tabel 3 Tools Anti Forensik untuk pengerusakan data dengan Teknik Pemecahan file

Tools Anti forensic	Objek	Tools Uji Efektivitas Anti Forensik
HJ Split	Semua Jenis file	autopsy 4.2.0, FTK Imager, dan FI File Find

Tabel 4 Tools Anti Forensik untuk pengerusakan data dengan Teknik Penghapusan

Tools Anti forensik	Objek	Tools Uji Efektivitas Anti Forensik
File Shredder	Semua jenis file	FTK Imager, dan OSForensics
Eraser	Semua jenis file	

Tabel 5 Tools Anti Forensic untuk Pengerusakan Data dengan Formating

Tools Anti forensic	Objek	Tools Uji Efektivitas Anti Forensik
Disk Wiping	Partisi media penyimpanan	Photorec, recuva, dan Easeus Data Recovery

HASIL DAN PEMBAHASAN

Data Hiding

Dalam implementasi data hiding teknik steganografi sekaligus teknik kriptografi menggunakan tool invisible secrets, uji efektivitas dengan autopsy.

Proses Steganografi

Ujicoba sesuai tabel 1 untuk objek file text, data penampung image(jpeg),

File tes_sembunyi.txt (146 bytes) (gambar 1) akan disembunyikan pada file img_0058.jpg (gambar 4)

Gambar 2 file Sumber Data Hiding

Gambar 3 Lokasi Penyembunyian

a. Proses Kriptografi

File penampung (carrier) selanjutnya dapat dienkripsi. Kunci enkripsi yang diinginkan dimasukkan, algortima enkrpsi yang disediakan dipilih (dipilih algoritma ghost) (gambar 4).

Gambar 4 Penggunaan Kriptografi

Setelah itu proses data hiding dengan steganografi dan sekaligus enkripsi dilakukan (gambar 5)

Gambar 5 Proses Data Hiding Steganografi dan Kriptografi

Hasil ujicoba (gambar 6) ukuran file target (hasilnya.jpg) tetap seperti sebelum dimasukkan data tersembunyi yakni sebesar 4,04 MB

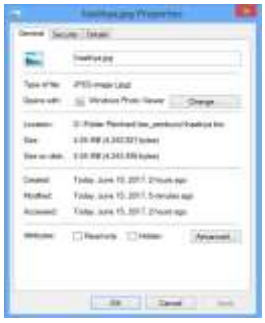
b. Uji Efektivitas

Uji efektivitas data hiding menggunakan tools forensic autopsy memiliki TFD sebesar 100 % (quick), POD sebesar 100% , IOAF sebesar 100% (Excelent).

Data Destruction

a. Data destruction dengan fileshreder

Dalam implementasi *data destruction* menggunakan tool fileshreder dengan objek file dan direktori (gambar 7) berhasil dilakukan

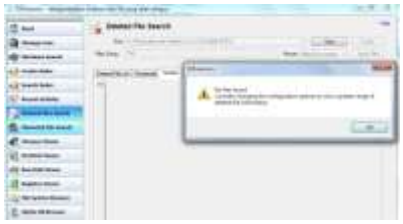


Gambar 6 Hasil Ujicoba

Gambar 7 objek Data Destruction

b. Uji Efektivitas

Uji efektivitas menggunakan tools Forensik OSForensic tidak berhasil mengembalikan direktori dan file yang telah dihapus (gambar 8)



Gambar 8 Uji Efektivitas Anti Forensik

KESIMPULAN

Dari penelitian ini dapat disimpulkan beberapa hal sebagai berikut :

1. Data Hiding dan Data Destruction didalam sebuah hardisk dan flashdisk berhasil dilakukan dengan menggunakan tools anti forensik.
2. Ukuran file tertentu objek data hiding dapat tetap tidak merubah ukuran file carrier sehingga dapat mengurangi kecurigaan investigator.
3. Uji efektivitas menggunakan tools Forensic autopsy dan OSForensic Data Ujicoba Hiding dan Destruction memiliki TFD sebesar 100 % (quick), POD sebesar 100% , IOAF sebesar 100% (Excelent).

DAFTAR PUSTAKA

[1] Implementation of Anti-Forensic Mechanisms and Testing with Forensic Methods, https://pdfs.semanticscholar.org/.../ee48a9ef927c805da49f4...

[2] The Rise of Anti-Forensic https://www.csoonline.com/article/ 2122329/ investigations-forensics/the-rise-of-anti-forensics.html

[3] Anti-Forensics: Techniques, Detection and Countermeasure, https://calhoun.nps.edu/bitstream/handle/10945/44248/Garfinkel_Anti-Forensics_2007.ICIW.AntiForensics.pdf%3Bjsessionid%3D5BAB9E403AECBBDD8CF7C8ECC8930B2E?sequence%3D1