ANTI KOMPUTER FORENSIK DENGAN MENGGUNAKAN METODE STEGANOGRAFI DAN MANIPULASI FILE

SKRIPSI

untuk memenuhi salah satu syarat mencapai derajat Sarjana
Program Studi Teknik Komputer

diajukan oleh

SUNU AJI NUGROHO

18.83.0267

Kepada

PROGRAM SARJANA

PROGRAM STUDI TEKNIK KOMPUTER

FAKULTAS ILMU KOMPUTER

UNIVERSITAS AMIKOM YOGYAKARTA

YOGYAKARTA

2022

ANTI KOMPUTER FORENSIK DENGAN MENGGUNAKAN METODE STEGANOGRAFI DAN MANIPULASI FILE

SKRIPSI

untuk memenuhi salah satu syarat mencapai derajat Sarjana
Program Studi Teknik Komputer

diajukan oleh

SUNU AJI NUGROHO

18.83.0267

Kepada

PROGRAM SARJANA

PROGRAM STUDI TEKNIK KOMPUTER

FAKULTAS ILMU KOMPUTER

UNIVERSITAS AMIKOM YOGYAKARTA

YOGYAKARTA

HALAMAN PERSETUJUAN
SKRIPSI

ANTI KOMPUTER FORENSIK DENGAN MENGGUNAKAN METODE STEGANOGRAFI DAN MANIPULASI FILE

yang disusun dan diajukan oleh

Sunu Aji Nugroho

18.83.0267

telah disetujui oleh Dosen Pembimbing Skripsi
pada tanggal 12 Juli 2022

Dosen Pembimbing,

Wahid Miftahul Ashari, S.Kom., M.T
NIK. 190302452

HALAMAN PENGESAHAN

SKRIPSI

ANTI KOMPUTER FORENSIK DENGAN MENGGUNAKAN METODE STEGANOGRAFI DAN MANIPULASI FILE

yang disusun dan diajukan oleh

Sunu Aji Nugroho

18.83.0267

Telah dipertahankan di depan Dewan Penguji
pada tanggal 23 Agustus 2022

Susunan Dewan Penguji

Nama Penguji	Tanda Tangan
Jeki Kuswanto, M.Kom **NIK. 190302456**	
Ria Andriani, M.Kom **NIK. 190302458**	
Wahid Miftahul Ashari, S.Kom., M.T **NIK. 190302452**	

Skripsi ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Sarjana Komputer
Tanggal 23 Agustus 2022

DEKAN FAKULTAS ILMU KOMPUTER

Hanif Al Fatta,S.Kom., M.Kom.
NIK. 190302096

HALAMAN PERNYATAAN KEASLIAN SKRIPSI

Yang bertandatangan di bawah ini,

Nama mahasiswa : Sunu Aji Nugroho
NIM : 18.83.0267

Menyatakan bahwa Skripsi dengan judul berikut:

Anti Komputer Forensik Dengan Menggunakan Metode Steganografi Dan Manipulasi File

Dosen Pembimbing : Wahid Miftahul Ashari, S.Kom., M.T

1. Karya tulis ini adalah benar-benar ASLI dan BELUM PERNAH diajukan untuk mendapatkan gelar akademik, baik di Universitas AMIKOM Yogyakarta maupun di Perguruan Tinggi lainnya.
2. Karya tulis ini merupakan gagasan, rumusan dan penelitian SAYA sendiri, tanpa bantuan pihak lain kecuali arahan dari Dosen Pembimbing.
3. Dalam karya tulis ini tidak terdapat karya atau pendapat orang lain, kecuali secara tertulis dengan jelas dicantumkan sebagai acuan dalam naskah dengan disebutkan nama pengarang dan disebutkan dalam Daftar Pustaka pada karya tulis ini.
4. Perangkat lunak yang digunakan dalam penelitian ini sepenuhnya menjadi tanggung jawab SAYA, bukan tanggung jawab Universitas AMIKOM Yogyakarta.
5. Pernyataan ini SAYA buat dengan sesungguhnya, apabila di kemudian hari terdapat penyimpangan dan ketidakbenaran dalam pernyataan ini, maka SAYA bersedia menerima SANKSI AKADEMIK dengan pencabutan gelar yang sudah diperoleh, serta sanksi lainnya sesuai dengan norma yang berlaku di Perguruan Tinggi.

Yogyakarta, 23 Agustus 2022

Yang Menyatakan,

Sunu Aji Nugroho

HALAMAN PERSEMBAHAN

Dengan rasa syukur yang mendalam, dengan telah diselesaikannya Skripsi ini Penulis mempersembahkannya kepada:

1. Tuhan YME, yang senantiasa memberikan rahmat dan hidayah-Nya sehingga penulis dapat menyelesaikan laporan ini dengan baik.
2. Keluarga Besar Penulis yang telah senantiasa membantu menyelesaikan Skripsi ini.
3. Segenap *civitas* akademika kampus Universitas Amikom Yogyakarta, staf pengajar, karyawan, dan seluruh mahasiswa semoga tetap semangat dalam beraktivitas mengisi hari-harinya di kampus Universitas Amikom Yogyakarta.
4. Teman-teman Penulis baik itu teman kuliah seangkatan, adik kelas, kakak kelas pada Fakultas Ilmu Komputer Universitas Amikom Yogyakarta, maupun teman-teman dari fakultas dan universitas yang lain yang telah banyak membantu Penulis dalam menyelesaikan Skripsi ini.

Penulisan menyadari bahwa penulisan Skripsi ini masih banyak terdapat kekurangan. Oleh karena itu Penulis mengharapkan kritik dan masukan demi kesempurnaan penulisan Skripsi ini. Semoga penulisan ini bisa berguna dan bermanfaat bagi semua pihak yang membutuhkan

KATA PENGANTAR

Puji syukur diucapkan kehadirat Allah SWT dengan segala rahmatNya sehingga skripsi ini dapat diselesaikan dan dapat tersusun dengan baik. Tidak lupa kami mengucapkan terimakasih terhadap bantuan pihak yang telah memberikan dukungan supaya penulis segera menyelesaikan skripsi ini. Penulis berharap semoga skripsi ini dapat berguna untuk pembaca serta dapat memberikan wawasan dan pengetahuan lebih mengenai anti komputer forensik dan bisa diterapkan dalam kehidupan sehari-hari.

Bagi saya sebagai penulis merasa bahwa masih banyak kekurangan dalam penyusunan skripsi ini dikarenakan keterbatasan wawasan serta pengetahuan yang saya miliki. Untuk itu kami sangat mengharapkan kritik dan saran yang membangun kedepannya dari pembaca supaya penelitian dan skripsi ini lebih sempurna lagi.

Yogyakarta, 23 Agustus 2022
Penulis

DAFTAR ISI

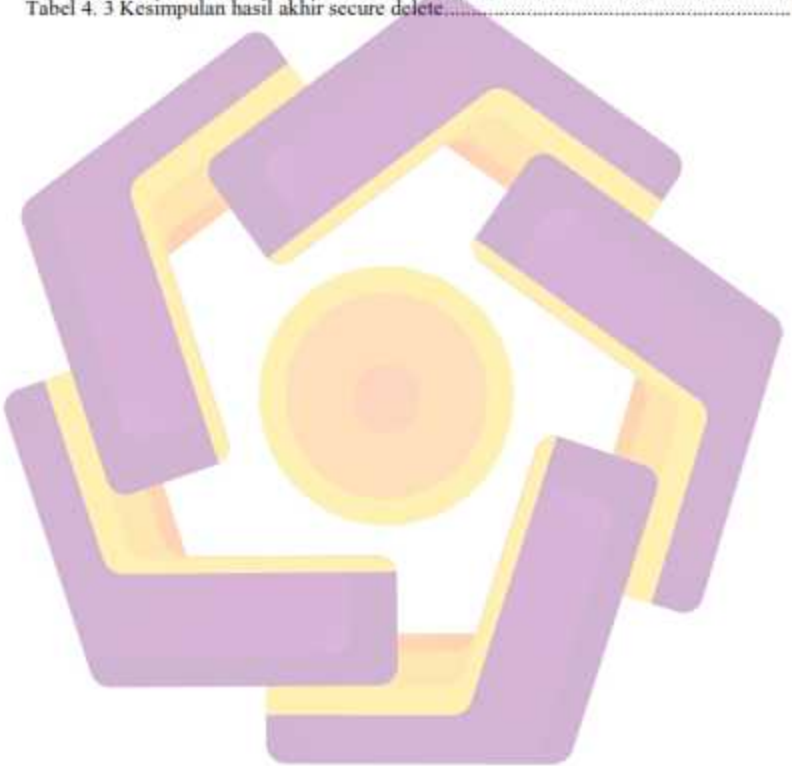
HALAMAN JUDUL ii
HALAMAN PERSETUJUAN iii
SKRIPSI iii
ANTI KOMPUTER FORENSIK DENGAN MENGGUNAKAN METODE STEGANOGRAFI DAN MANIPULASI FILE iii
HALAMAN PENGESAHAN iv
ANTI KOMPUTER FORENSIK DENGAN MENGGUNAKAN METODE STEGANOGRAFI DAN MANIPULASI FILE iv
HALAMAN PERNYATAAN KEASLIAN SKRIPSI v
HALAMAN PERSEMBAHAN vi
KATA PENGANTAR vii
DAFTAR ISI viii
DAFTAR TABEL x
DAFTAR GAMBAR xi
DAFTAR LAMBANG DAN SINGKATAN xiii
DAFTAR ISTILAH xiv
INTISARI xv
Abstract xvi
BAB I PENDAHULUAN 1
1.1 Latar Belakang 1
1.2 Perumusan masalah 2
1.3 Tujuan Penelitian 3
1.4 Batasan Masalah 3
1.5 Manfaat Penelitian 3
BAB II TINJAUAN PUSTAKA 4
2.1 Literature Review 4
2.2 Landasan Teori 7
2.2.1 Komputer Forensik 7

2.2.2 Anti Komputer Forensik 9
2.2.3 Perbandingan Komputer Forensik dan Anti Komputer Forensik ... 10
2.2.4 Steganografi 11
2.2.5 Manipulasi File 12
BAB III METODOLOGI PENELITIAN 15
3.1 Metode Experimental 15
3.2 Tahapan Metode Eksperimental 15
3.2.1 Penentuan Ide 15
3.2.2 Perumusan Masalah 15
3.2.3 Penentuan Tipe dan Desain Penelitian 16
3.2.4 Pelaksanaan Percobaan 17
3.2.5 Analisa Hasil 21
3.2.6 Penarikan Kesimpulan 21
BAB IV HASIL DAN PEMBAHASAN 22
4.1 Implementasi 22
4.1.1 Penyamaran File 22
4.1.2 Data Hiding 37
4.1.3 Secure Delete 46
4.2 Hasil Pengujian 52
4.2.1 Pengujian penyamaran file 52
4.2.2 Pengujian *Data Hiding* 55
4.2.2 Pengujian Secure Delete 56
BAB V KESIMPULAN DAN SARAN 58
5.1 Kesimpulan 58
5.2 Saran 59
DAFTAR PUSTAKA 60

DAFTAR TABEL

Tabel 2. 1 Perbandingan Penelitian 5
Tabel 2. 2 Perbedaan Komputer Forensik dan Anti Forensik 10

Tabel 4. 1 Kesimpulan hasil akhir penyamaran file 53
Tabel 4. 2 Kesimpulan hasil akhir data hiding 55
Tabel 4. 3 Kesimpulan hasil akhir secure delete 56



DAFTAR GAMBAR

Gambar 2. 1 Proses Embedding Message 11
Gambar 2. 2 Proses Extraction Message 12
Gambar 2. 3 Tabel ASCII 13

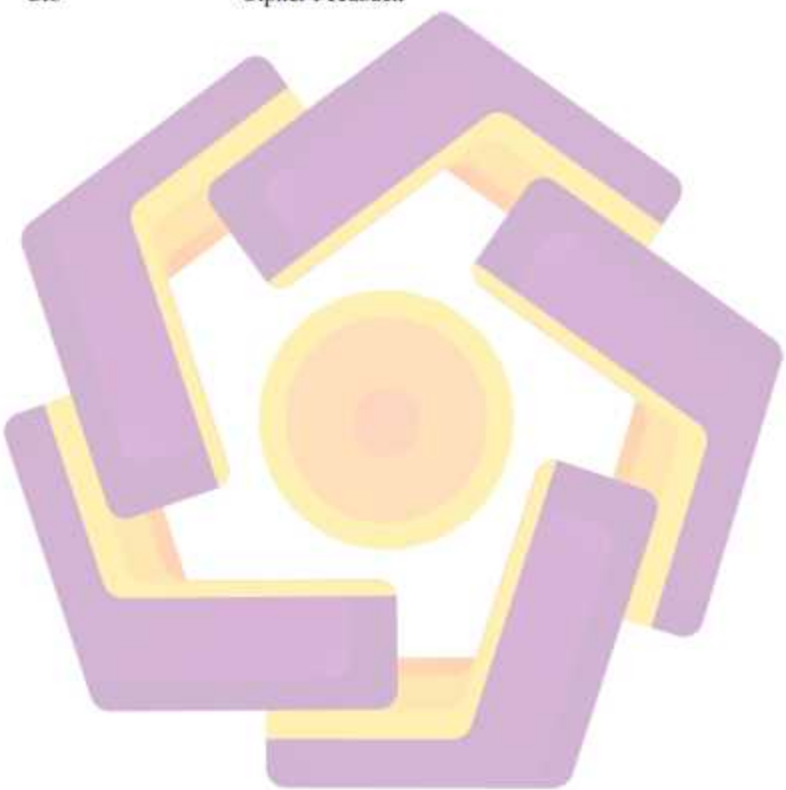
Gambar 3. 1 Desain penelitian 16
Gambar 3. 2 Teknik penyamaran file 19
Gambar 3. 3 Teknik data hiding 20
Gambar 3. 4 Teknik secure delete 21

Gambar 4. 1 Persiapan penyamaran file 22
Gambar 4. 2 Perbedaan file asli dengan file yang telah dirubah 23
Gambar 4. 3 Pengujian teknik pertama 24
Gambar 4. 4 Duplikat dan kompresi file asli 25
Gambar 4. 5 Sebelum perubahan header 26
Gambar 4. 6 Setelah perubahan header 26
Gambar 4. 7 Pengujian teknik kedua 27
Gambar 4. 8 Duplikat dan kompresi file asli 28
Gambar 4. 9 Sebelum perubahan header 29
Gambar 4. 10 Setelah perubahan header 29
Gambar 4. 11 Pengujian teknik ketiga 30
Gambar 4. 12 Duplikat dan kompresi file asli 31
Gambar 4. 13 Sebelum perubahan header 32
Gambar 4. 14 Sebelum perubahan header 32
Gambar 4. 15 Pengujian teknik keempat 33
Gambar 4. 16 Duplikat dan kompresi file asli 34
Gambar 4. 17 Sebelum perubahan header 35
Gambar 4. 18 Sesudah perubahan header 35
Gambar 4. 19 Pengujian teknik keempat 36

Gambar 4. 20 persiapan data hiding....37
Gambar 4. 21 tools OpenStego....38
Gambar 4. 22 File gambar.png....38
Gambar 4. 23 Stegofile gambar.png....39
Gambar 4. 24 Pengujian percobaan pertama....40
Gambar 4. 25 Tools Steghide....41
Gambar 4. 26 Pengujian percobaan kedua....42
Gambar 4. 27 Tools Openpuff....43
Gambar 4. 28 Hasil output OpenPuff....45
Gambar 4. 29 Pengujian terhadap gambar.jpg....45
Gambar 4. 30 Pengujian terhadap gambar.png....46
Gambar 4. 31 Pengujian terhadap suara.wav....46
Gambar 4. 32 persiapan secure delete....47
Gambar 4. 33 Penghapusan secara biasa masih bisa direstore....48
Gambar 4. 34 Penghapusan dengan Shift+Delete....48
Gambar 4. 35 Pengujian percobaan kedua....49
Gambar 4. 36 Penghapusan file dengan File Shredder....50
Gambar 4. 37 Pengujian percobaan ketiga....51
Gambar 4. 38 Penghapusan file dengan Sdelete....51
Gambar 4. 39 Pengujian percobaan keempat....52

DAFTAR LAMBANG DAN SINGKATAN

ASCII	American Standard Code for Information Interchange
AES	Advanced Encryption Standard
FrHed	Free Hex Editor
DOS	Disk Operating System
Cfb	Cipher Feedback



DAFTAR ISTILAH

Steganografi	Seni menyembunyikan pesan
Recovery	Melakukan pemulihan ulang
Data hiding	Menyembunyikan data
Secure delete	Penghapusan secara aman
Embedding	Melakukan penyisipan
Stego Medium	Wadah untuk melakukan steganografi
Stego File	File hasil dari steganografi
Signature	Identitas dan verifikasi file
File carrier	Medium untuk proses steganografi
Decoy file	File palsu

INTISARI

Anti komputer forensik adalah kebalikan atau lawan dari bidang komputer forensik. Komputer forensik berfokus pada upaya untuk menemukan dan mencari data, menjaga keutuhan dan integritas data, sedangkan bidang anti komputer forensik justru menitik beratkan pada sisi sebaliknya yaitu tentang bagaimana cara menyebunyikan sebuah file atau citra digital sehingga tidak dapat dideteksi fakta yang sebenarnya oleh uji forensik dengan memanfaatkan teknik steganografi dan manipulasi file untuk mengurangi kualitas dan kuantitas, serta menyamarkan barang bukti.

Penelitian ini menggunakan metode anti komputer forensik yang berupa Steganografi dan Manipulasi file. Steganografi itu sendiri adalah sebuah ilmu untuk menyembunyikan sebuah file didalam sebuah file guna menjaga kerahasiaan pesan sehingga hanya pengirim dan penerima saja yang dapat mengetahui isi dari pesan itu. Manipulasi File adalah sebuah proses rekayasa dengan melakukan penyembunyian, penambahan, serta penghapusan terhadap bagian atau keseluruhan dari file-file yang ada didalam perangkat komputer yang pastinya akan berpengaruh terhadap isi, ukuran dan integritas suatu file.Teknik manipulasi file nantinya yang akan digunakan berupa penyamaran file, penyembunyian data dan penghapusan file secara aman.

Output yang dihasilkan dari penelitian ini berupa pengujian terhadap teknik anti komputer forensik. Hasil yang didapat dari skenario pertama yaitu penyamaran ekstensi file diperoleh hasil bahwa penyamaran dengan cara manual dan dengan menggunakan notepad tidak berhasil dilakukan dan file masih terdeteksi sebagai file .zip. Skenario kedua melakukan data hiding dengan hasil pengujian forensik berupa file carrier .jpg dengan mudah terdeteksi oleh tools forensik sebagai stego file. Skenario ketiga melakukan secure delete atau penghapusan secara aman diperoleh hasil bahwa percobaan penghapusan dengan menggunakan delete ataupun shift+delete masih bisa dilakukan recovery ulang oleh tools forensik.

Kata kunci: Anti Komputer Forensik, Steganografi, Manipulasi File

Abstract

Anti computer forensics is opposite of the field of computer forensics. Computer forensics focuses on efforts to find and search data, maintaining the integrity and integrity of data, while the field of anti-computer forensics focuses on the opposite side, namely how to hide a file or digital image so that the actual facts cannot be detected by forensic testing by utilizing steganography and file manipulation techniques to reduce the quality and quantity, as well as disguise the evidence.

This research uses anti-computer forensics methods in the form of steganography and file manipulation. Steganography itself is a science to hide a file in a file in order to maintain the confidentiality of the message so that only the sender and recipient can know the contents of the message. File manipulation is an engineering process by hiding, adding, and deleting part or all of the files on a computer device which will certainly affect the content, size and integrity of a file. File manipulation techniques will later be used in the form of file disguise, data hiding and secure file deletion.

The output of this research is in the form of testing of anti-computer forensic techniques. The results obtained from the first scenario, namely the disguise of the file extension, the results showed that the disguise manually and using notepad was not successful and the file was still detected as a .zip file. The second scenario is doing data hiding with the results of forensic testing in the form of a carrier .jpg file that is easily detected by forensic tools as a stego file. The third scenario is to perform a secure delete or secure deletion. The result is that an attempted deletion using delete or shift+delete can still be re-recovered by forensic tools.

Keyword: *Anti-Computer Forensics, Steganography, File Manipulation*