IMPLEMENTASI STEGANOGRAFI DENGAN ALGORITMA AES DI GOOGLE DRIVE

TUGAS AKHIR

Rizqi Ahmad Fauzan
41515120142

PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS MERCU BUANA
JAKARTA
2020

IMPLEMENTASI STEGANOGRAFI DENGAN ALGORITMA AES DI GOOGLE DRIVE

Tugas Akhir

Diajukan Untuk Melengkapi Salah Satu Syarat
Memperoleh Gelar Sarjana Komputer

Oleh:
Rizqi Ahmad Fauzan
41515120142

PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS MERCU BUANA
JAKARTA
2020

LEMBAR PERNYATAAN ORISINALITAS

Yang bertanda tangan dibawah ini:

NIM	:	41515120142
Nama	:	Rizqi Ahmad Fauzan
Judul Tugas Akhir	:	Implementasi Steganografi dengan Algoritma AES di Google Drive

Menyatakan bahwa Laporan Tugas Akhir saya adalah hasil karya sendiri dan bukan plagiat. Apabila ternyata ditemukan didalam laporan Tugas Akhir saya terdapat unsur plagiat, maka saya siap untuk mendapatkan sanksi akademik yang terkait dengan hal tersebut.

Jakarta, 18 Januari 2020

Rizqi Ahmad Fauzan

SURAT PERNYATAAN PERSETUJUAN PUBLIKASI TUGAS AKHIR

Sebagai mahasiswa Universitas Mercu Buana, saya yang bertanda tangan di bawah ini :

Nama Mahasiswa	:	Rizqi Ahmad Fauzan
NIM	:	41515120142
Judul Tugas Akhir	:	Implementasi Steganografi dengan Algoritma AES di Google Drive

Dengan ini memberikan izin dan menyetujui untuk memberikan kepada Universitas Mercu Buana **Hak Bebas Royalti Noneksklusif** (*None-exclusive Royalty Free Right*) atas karya ilmiah saya yang berjudul diatas beserta perangkat yang ada (jika diperlukan).

Dengan Hak Bebas Royalti/Noneksklusif ini Universitas Mercu Buana berhak menyimpan, mengalihmedia/formatkan, mengelola dalam bentuk pangkalan data (*database*), merawat dan mempublikasikan tugas akhir saya.

Selain itu, demi pengembangan ilmu pengetahuan di lingkungan Universitas Mercu Buana, saya memberikan izin kepada Peneliti di Lab Riset Fakultas Ilmu Komputer, Universitas Mercu Buana untuk menggunakan dan mengembangkan hasil riset yang ada dalam tugas akhir untuk kepentingan riset dan publikasi selama tetap mencantumkan nama saya sebagai penulis/pencipta dan sebagai pemilik Hak Cipta.

Demikian pernyataan ini saya buat dengan sebenarnya.

Jakarta, 25 Februari 2020

Rizqi Ahmad Fauzan

SURAT PERNYATAAN LUARAN TUGAS AKHIR

Sebagai mahasiswa Universitas Mercu Buana, saya yang bertanda tangan di bawah ini

Nama Mahasiswa	:	Rizqi Ahmad Fauzan
NIM	:	41515120142
Judul Tugas Akhir	:	Implementasi Steganografi dengan Algoritma AES di Google Drive

Menyatakan bahwa Luaran Tugas Akhir saya adalah sebagai berikut :

No	Luaran	Jenis			Status	
1	Publikasi Ilmiah	Jurnal Nasional Tidak Terakreditasi			Diajukan	√
		Jurnal Nasional Terakreditasi	√			
		Jurnal International Tidak Bereputasi			Diterima	
		Jurnal International Bereputasi				
	Disubmit/dipublikasikan di :	Nama Jurnal	: Jurnal Teknologi Informasi Yarsi			
		ISSN	: 1907-8331			
2	Kertas Kerja, Merupakan material haasil penelitian sebagai kelengkapan Artikel Jurnal. Terdiri dari (minimal 4)	Literatur Review				[√]
		Hasil analisa & perancangan aplikasi				[√]
		Source code				[√]
		Data set				[√]
		Tahapan eksperimen				[√]
		Hasil eksperimen seluruhnya				[√]
3	HAKI Disubmit / Terdaftar	HKI			Diajukan	
		Paten			Tercatat	
		No & Tanggal Permohonan				
		No & Tanggal Pencatatan	:			

Demikian pernyataan ini saya buat dengan sebenarnya.

Jakarta, 18 Januari 2020

Rizqi Ahmad Fauzan

LEMBAR PERSETUJUAN

Nama Mahasiswa	:	Rizqi Ahmad Fauzan
NIM	:	41515120142
Judul Tugas Akhir	:	Implementasi Steganografi dengan Algoritma AES di Google Drive

Tugas Akhir ini telah diperiksa dan disetujui

Jakarta, 11 Januari 2020

Menyetujui,

(Dr. Leonard Goeirmanto, S.T., M.Sc.)
Dosen Pembimbing

LEMBAR PERSETUJUAN PENGUJI

NIM	:	41515120142
Nama	:	Rizqi Ahmad Fauzan
Judul Tugas Akhir	:	Implementasi Steganografi Dengan Algoritma AES Di Google Drive

Tugas Akhir ini telah diperiksa dan disidangkan sebagai salah satu persyaratan untuk memperoleh gelar Sarjana pada Program Studi Teknik Informatika, Fakultas Ilmu Komputer, Universitas Mercu Buana.

Jakarta,15 February 2020

(Sabar Rudiarto, S.Kom, M.Kom)
Ketua Penguji

(Harni Kusniyati, ST., M.Kom)
Anggota Penguji 1

(Herry Derajad Wijaya, S.Kom., MM)
Anggota Penguji 2

LEMBAR PENGESAHAN

NIM : 41515120142

Nama : Rizqi Ahmad Fauzan

Judul Tugas Akhir : Implementasi Steganografi dengan Algoritma AES di Google Drive

Tugas Akhir ini telah diperiksa dan disidangkan sebagai salah satu persyaratan untuk memperoleh gelar Sarjana pada Program Studi Teknik Informatika, Fakultas Ilmu Komputer, Universitas Mercu Buana.

Jakarta, 11 Februari 2020

Menyetujui,

(Dr. Leonard Goeirmanto, S.T., M.Sc.)
Dosen Pembimbing

Mengetahui,

(Diky Firdaus, S.Kom, MM)	(Desi Ramayanti, S.Kom, MT)
Koord. Tugas Akhir Teknik Informatika	Ka. Prodi Teknik Informatika

KATA PENGANTAR

Puji syukur kita panjatkan kepada Allah Subhanahu Wa Ta'ala, karena atas limpahan rahmat dan karunia-Nya, saya dapat menyelesaikan tugas akhir yang berjudul **"Implementasi Steganografi dengan algoritma AES di Google Drive"**

Banyak pihak yang membantu hingga skripsi ini dapat saya selesaikan. Untuk itu, saya ingin menyampaikan ucapan terima kasih kepada:

1. Keluarga tercinta: Bapak Lutno, Ibu Parsinah, Dik Sururi, Dik Fuad yang telah memberi dukungan dan do'anya.
2. Bapak Dekan.
3. Bapak Dr. Leonard Goeirmanto, S.T., M.Sc., selaku dosen pembimbing yang telah meluangkan waktu, tenaga dan pikiran untuk mengarahakan sata dalam penyusunan tugas akhir ini.
4. Bapak Diky Firdaus, S.Kom, MM, selaku dosen akademik yang telah memberi arahan selama saya kuliah.
5. Teman teman seperjuangan UMB 2020 yang telah memberikan banyak bantuan informasi dan dukungan.

Akhir kata, penulis berharap semoga tugas akhir ini dapat bermanfaat untuk semua orang di masa mendatang.

Jakarta, 18 Januari 2020

Penulis

DAFTAR ISI

Naskah Jurnal

Implementasi Stegnografi dengan Algoritma AES di Google Drive

Rizqi Ahmad Fauzan, Leonard Goeirmanto

Jurusan Teknik Informatika

Universitas Mercu Buana

Jl. Meruya Selatan No. 1, Jakarta

41515120142@student.mercubuana.ac.id ,
leonard@mercubana.ac.id

Abstract*— Dalam dunia digital seperti sekarang, sangat mudah bagi kita untuk menyimpan data secara online. Google drive merupakan salah satu penyedia layanan untuk menyimpan file sacara online. Menyimpan file di googl drive memang aman, tetapi keamanan tersebut tidak berlaku jika kita meminjamkan handphone / komputer kita ke orang lainm karena orang tersebut dapat membuka data kita yang berada di google drive, baik sengaja ataupun tidak . Salah satu cara untuk menghindari hal tersebut adalah menggunakan kriptografi dan steganografi. Pada penelitian ini, penulis mengamankan file rahasia dengan cara menyisipkan hasil enkripsi file rahasia kedalam sebuah gambar. Metode ini efektif untuk mengamankan file karena gambar sebelum dan sesudah proses sangat mirip dan tidak dapat dibedakan dengan kasat mata.

***Keyword*— Steganografi, kriptografi, Algoritma AES, Google Drive**

PERKENALAN

Seiring perkembangan zaman, kebutuhan masyarakat akan tempat penyimpanan informasi semakin meningkat. Saat ini telah ditemukan tempat penyimpanan berbasis awan yang sering kita sebut *cloud storage*. *Cloud storage* merupakan tempat menyimpan file secara online sehingga masyarakat tidak perlu khawatir jika memori mereka penuh. Cukup dengan koneksi internet, maka masyarakat dapat menyimpan file mereka secara online.

Google Drive merupakan salah satu produk dari google untuk mengatasi masalah ini. Masyarakat dapat menggunakan 15 GB penyimapan secara gratis. Produk ini dapat digunakan dengan mudah melalui mobile ataupun web browser.

Menyimpan data di google drive tergolong aman, karena kita perlu memasukkan username dan password untuk mengakses akun kita. Menurut Wawan Gunawan, tingkat keamanan seperti ini tidak dapat mencegah orang lain yang meminjam hanphone / komputer kita untuk tidak membuka dokumen di google drive, baik secara sengaja ataupun tidak sengaja. Oleh karena itu penggunaan kriptografi dan steganografi merupakan hal yang sangat diperlukan.

Kriptografi merupakan teknik untuk mengubah suatu pesan menjadi pesan yang sulit dibaca. Sedangkan Steganografi merupakan teknik untuk menyembunyikan pesan agar pesan tersebut tidak ditemukan. Pengguna juga merasa khawatir karena menurut Ahmad Kodar, tenknik menyembunyian data dengan steganografi tidak mengubah mengubah data yang disembunyikan.

.

LINGKUP KERJA YANG BERHUBUNGAN

Cloud Storage

Hari ini akses internet dapat dengan mudah didapat. Cloud Storage merupakan salah satu teknologi yang digunakan untuk menyimpan data dengan memanfaatkan internet. Dengan adanya cloud storage merasakan manfaatnya seperti tidak perlu lagi membawa hard drive kemana mana dan tidak ada kekawatiran jika hard drive itu terjadi sesuatu yang tidak diinginkan.

Google Drive

Google Drive adalah salah satu product dari perusahaan google yang diluncurkan sejak 2012. Dengan google drive, siapapun dapat menyimpan file mereka secara online. Pengguna dapat mengakses google drive menggunakan web dan mobile.

Google Drive menyediakan 15 GB yang dapat digunakan secara gratis untuk setiap user secara gratis. Pengguna dapat menyimpan dokumen, video, gambar dan file lainya. Jika pengguna memerlukan lebih dari 15 GB, pengguna dapat mendaftarkan akun miliknya untuk dijadikan akun premium. Dengan akun premium pengguna dapat menyimpan file sebanyak 30 TB (30.000 GB).

Kriptografi

Kriptografi adalah teknik untuk menjaga kerahasiaan informasi dengan cara mengkoversikan teks biasa (plaintext) menjadi teks yang tidak dapat dipahami (chippertext). Dengan teknik ini, pembuat pesan harus membagikan teknik memecahkan chippertext hanya kepada pihak penerima yang diinginkan, agar tidak ada pihak lain yang dapat melakukan hal yang serupa.

Steganografi

Steganografi adalah teknik untuk menyembunyikan informasi dengan suatu metode sehingga hanya pengirim dan penerima yang menyadari bahwa ada informasi rahasia. Pada praktiknya, pesan rahasia disembunyikan dengan cara membuat sedikit perubahan kecil pada file digital lain. File digital yang sering dipakai untuk menyembunyikan informasi diantaranya bitmap (bmp), gif, pcx, jpeg, wav, voc, mp3, teks file, html, pdf, dll.

Algoritma AES

Algoritma AES adalah algoritma kriptografi yang digunakan untuk menganmankan data. Algoritma AES dikembangkan mulai tahun 1997 sampai 2001 oleh National Institute of Standard and Technology, Amerika Serikat.

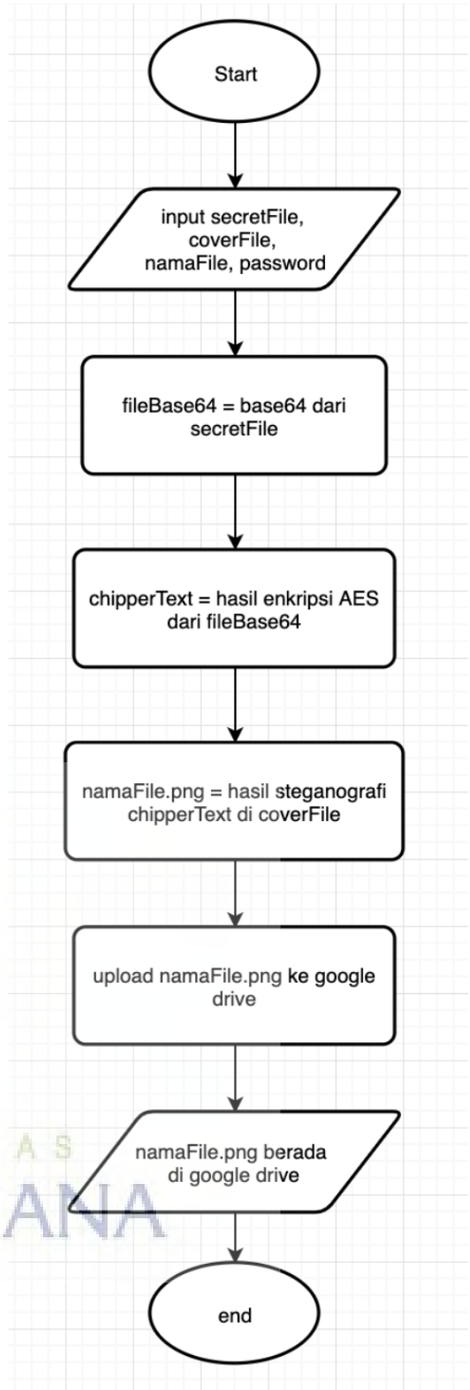
Base64

Base64 Encoding adalah suatu bentuk representasi data binari menjadi bentuk teks. Yang artinya, data data dalam komputer yang sejatinya adalah berbentuk binary, diubah menjadi bentuk teks yang dapat dibaca manusia. Teknik ini digunakan penulis untuk mengubah data pdf menjadi sebuah string.

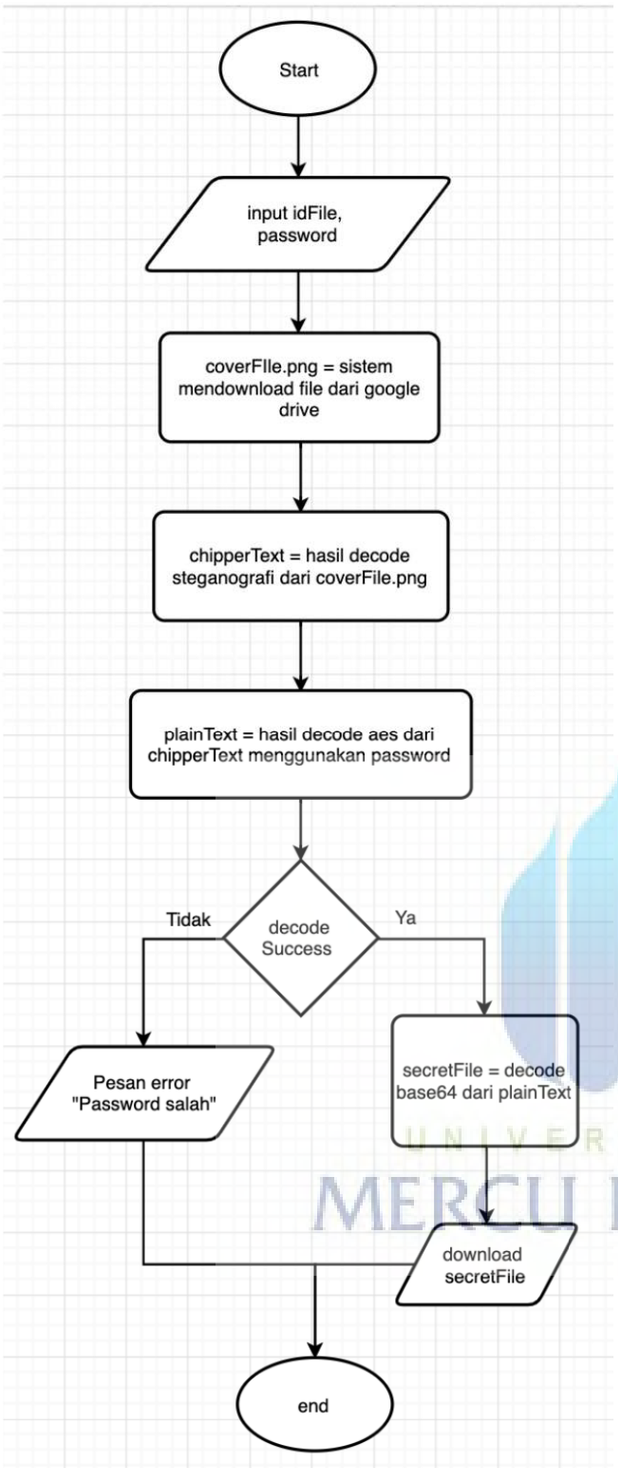
PERANCANGAN

Flowchart

Berikut flowchart yang dipakai pada jurnal ini



Gambar. 1. Flowchart upload file



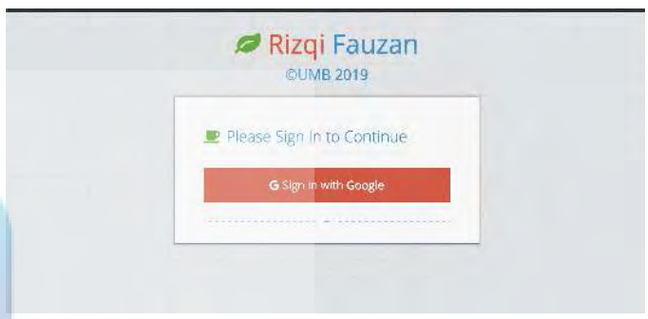
Gambar 2. Flowchart download file

Langkah langkah dekrisi sebagai berikut:

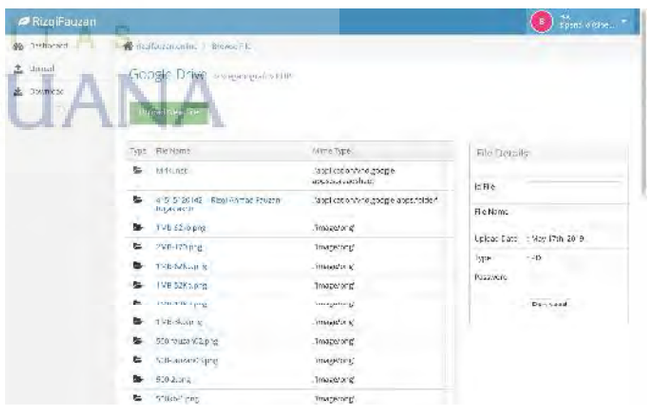
1. Mengakses halaman login
2. Sign in dengan akun google
3. Pilih file yang akan di dekripsi
4. Masukan password
5. Klik download`

Desain Antarmuka

Sistem ini mempunyai 3 anatrmuka, yaitu halaman login, halaman list file, dan halaman upload. Halaman login berhungsi sebagai tempat untuk memasukana credential pengguna google, halaman list file berfungsi sebagai tempat memilih document yang akan diunduh, dan halaman upload berfungsi sebagai tempat untuk mengunggah file.



Gambar 3. Halaman Login



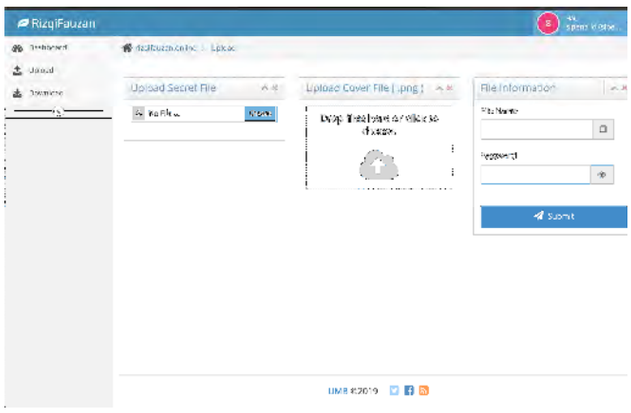
Gambar 4. Halaman List File

Langkah Kerja

Langkah kerja pada metode ini, dibagi menjadi 2 bagian, yaitu enkripsi dan dekripsi.

Langkah langkah enkripsi sebagai berikut:

1. Mengakses halaman login
2. Sign in dengan akun google
3. Klik `upload new file`
4. Pilih `secret file`, `cover file`
5. Isi `filename` dan `password`
6. Klik submit



Gambar 5. Halaman Upload File

Uji Coba

Dalam proses ujicoba, penguji mencoba menggunakan 2 cara, pengujian efektifitas dan pengujian keamanan. Pengujian efektifitas bertujuan untuk melihat apakah metode ini dapat digunakan untuk semua jenis file dan pengujian keamanan bertujuan untuk melihat membuktikan bahwa metode ini tidak mudah untuk direntas.

1. Pengujian efektifitas
   Dalam pengujian ini, penulis mencoba untuk menyembunyikan berbagai jenis file, dan bebagai ukuran secrete file dan berbagai resolusi cover image.

   a. Pengujian untuk beberapa jenis file

No	extensi file	jenis file	status enkripsi	status dekripsi
1	docx	dokument	yes	yes
2	pdf	dokument	yes	yes
3	xlxs	dokument	yes	yes
4	mp3	audio	yes	yes
5	png	image	yes	yes
6	jpg	image	yes	yes
7	jpeg	image	yes	yes
8	mp4	vidio	yes	yes

   b. Pengujian pada berbagai ukuran secrete file

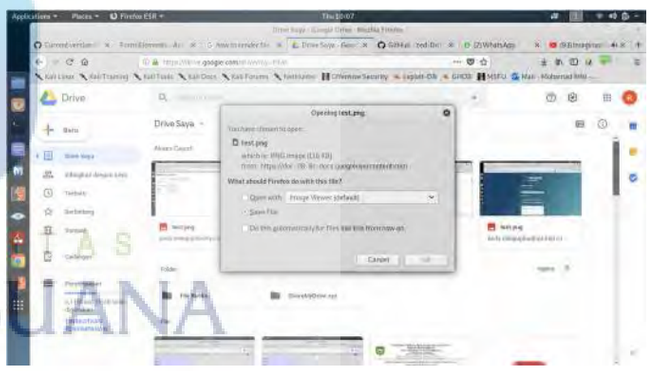
No	Resolusi secrete file	ukuran secrete File	Status enkripsi	status dekripsi
1	512 x 512	71 KB	Gagal	-
2	512 x 512	62 KB	Gagal	-
3	512 x 512	52 KB	Gagal	-
4	512 x 512	3 KB	Sukses	Sukses

   c. Pengujian pada berbagai resolusi cover image

No	Resolusi secrete file	ukuran secrete File	Status enkripsi	status dekripsi
1	1 x 1	3 KB	gagal	
2	2 x 2	3 KB	gagal	
3	4 x 4	3 KB	gagal	
4	8 x 8	3 KB	gagal	
5	16 x 16	3 KB	gagal	
6	32 x 32	3 KB	gagal	
7	128 x 128	3 KB	gagal	
8	256 x 256	3 KB	Sukses	Sukses
9	512 x 512	3 KB	Sukses	Sukses
10	1024 x 1024	3 KB	Sukses	Sukses

2. Pengujian keamanan
   Dalam pengujian ini penulis meminta bantuan seorang pentester yang bekerja di sebuah PT yang bergerak pada bidang sciber security. Hal ini bertujuan untuk memastikan kerahasiaan file yang disembunyikan oleh aplikasi.

Pertama pentester mencoba mengunduh salah satu file hasil enkripsi dari google drive seperti dibawah ini

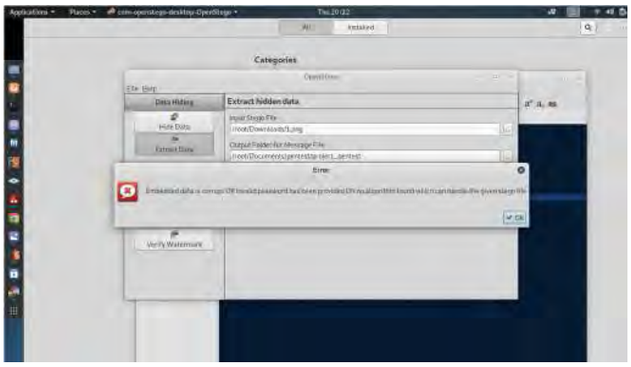


Pertama penguji mencoba mengunduh salah satu file hasil enkripsi dari google drive

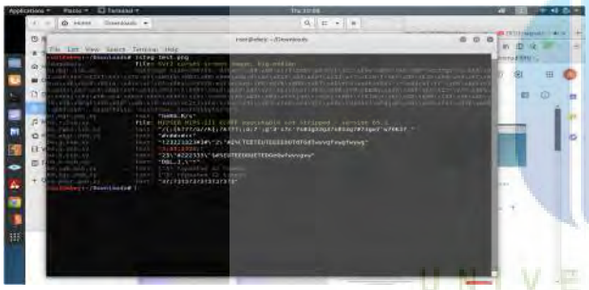
Setelah itu penguji mencoba untuk men-decode file untuk mendapatkan informasi tentang text rahasia didalam gambar menggunakan aplikasi online. Penguji tidak mendapatjan informasi apapun tentang pesan rahasia dan gagal menggunakan tool tersebut.

Setelah itu penguji juga mencoba menggunakan

aplikasi ‘openstego’ yang dikenal meripkan aplikasi yang sengat berguna untkm men-decode atau meng-ekstrak informasi sensitif untuk steganografi. Dan hasilnya seperti sebelumnya , penguji tidak mendapatkan informasi apapun seperti dibawah ini



Penguji melanjutkan dengan menggunakan aplikasi berbasis CLI pada sistem operasi kali linux untuk men-decode file staganografi seperti dibawah ini, dan tetap tidak dapat mendapatkan infomasi.



Gambar 12. Hasil pengujian

KESIMPULAN

Kesimpulan yang dapat diambil dari hasil pengamatan mulai dari perancangan, implementasi, dan proses uji coba sebagai berikut.

1. Ukuran secret file dan cover image mempengaruhi tingkat keberhasilan steganografi. Semakin tinggi resolusi cover image, semakin tinggi juga presentasi keberhasilanya.
2. Metode ini dapat dipakai di semua jenis file, mulai dari document, audio, video, dan lainya.
3. Perbedaan cover image sebelum dan sesudah proses steganography tidak bisa dilihat dengan kasat mata.
4. Secret file yang terdapat pada cover file hasil steganography tidak dapat dibuka dengan aplikasi atau metode lain.

REFERENCES

[1] A. P. Sari, I. M. Seno, and W. Gunawan, “Aplikasi Enkripsi dan Dekripsi untuk Keamanan Komunikasi Data pada SMS (Short Message Service) Berbasis Android Menggunakan Algoritma Blowfish,” *J. Ilm. FORMAT*, vol. 8, no. 1, pp. 34–41, 2019.

[2] R. Ferdiana, “The comparison of consumer cloud storage for a storage extension on the e-learning,” in 2016 6th International Annual Engineering Seminar (InAES), 2016.

[3] Y. U. Chandra and S. Hartono, “Analysis Factors of Technology Acceptance of Cloud Storage: A Case of Higher Education Students Use Google Drive,” in 2018 International Conference on Information Technology Systems and Innovation (ICITSI), 2018.

[4] T. Acharjee, A. Konwar, R. Kumar Ram, R. Sharma, and D. Goswami, “XORSTEG: A new model of text steganography,” in 2016 International Conference on Communication and Electronics Systems (ICCES), 2016.

[5] G. C. Prasetyadi, A. Benny Mutiara, and R. Refianti, “File encryption and hiding application based on advanced encryption standard (AES) and append insertion steganography method,” in 2017 Second International Conference on Informatics and Computing (ICIC), 2017.

[6] C.-P. Chang, H.-T. Chiao, Y.-S. Chang, C.-T. Tsai, K.-K. Yuen, and S.-M. Yuan, “UCS — A Unified Cloud Storage Integration Service,” in 2017 IEEE 7th International Symposium on Cloud and Service Computing (SC2), 2017.

[7] V. Saicheur and K. Piromsopa, “An implementation of AES-128 and AES-512 on Apple mobile processor,” in 2017 14th International Conference on Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology (ECTI-CON), 2017.

[8] M. Moizuddin, J. Winston, and M. Qayyum, “A comprehensive survey: Quantum cryptography,” in 2017 2nd International Conference on Anti-Cyber Crimes (ICACC), 2017.

[9] S. Wen and W. Dang, “Research on Base64 Encoding Algorithm and PHP Implementation,” in 2018 26th International Conference on Geoinformatics, 2018.

[10] A. Kodar, “Implementation of Steganography in Image Media Using Algorithm LSB (Least Significant Bit),” Int. Res. J. Comput. Sci., vol. 4, no. 8, pp. 6–13, 2017.

Penetration Test Report for https://rizqifauzan.online

v.1.0

Author : Muhamad Rifki , S.Kom

Penetration Tester @ PT. Q2 Technologies

1.1 Introduction

Penetration test report contains all efforts that were conducted in order to testing the vulnerability of the web application, mobile application and infrastructure. This report will be graded from a standpoint of correctness and fullness to all aspects of the testing. The purpose of this report is to ensure about the result of penetration testing are valid.

1.2 Information Gathering

First of all tester gather the information from the target website using nmap. From that tester found a lot of information from the target. Such as server information , web service technologies , open port , server system operation and version and more. But focus on scope and as the ethical of the concept during the testing. Tester just crawling information based on scope of testing which is web application running on port 443. During the testing on this scope tester found the information like

- Web application build with php version 5.6.40
- Web application using CRM technologies to management the service
- Steganography image

1.3 Findings

Findings is all about vulnerability which found by tester during the penetration testing.

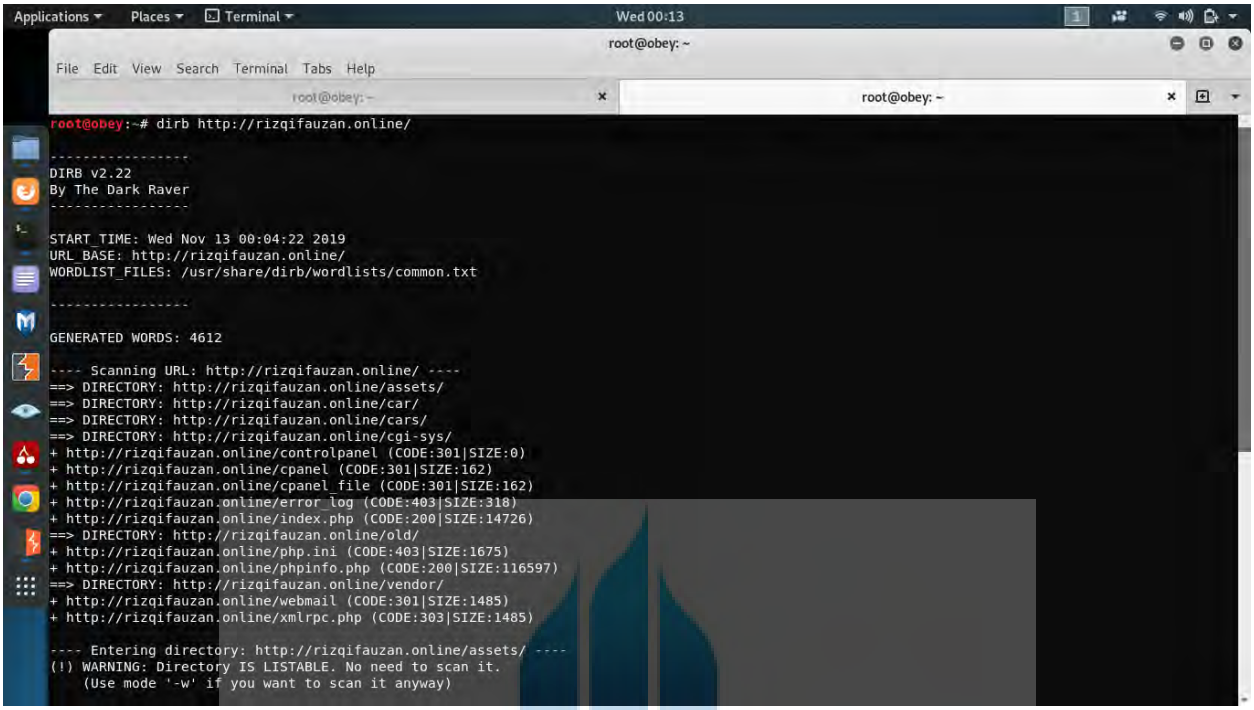
Vulnerability :
Directory Listing

Description :
Attackers will often attempt to exploit unpatched flaws or access default accounts, unused pages, unprotected files and directories, etc to gain unauthorized access or knowledge of the system.

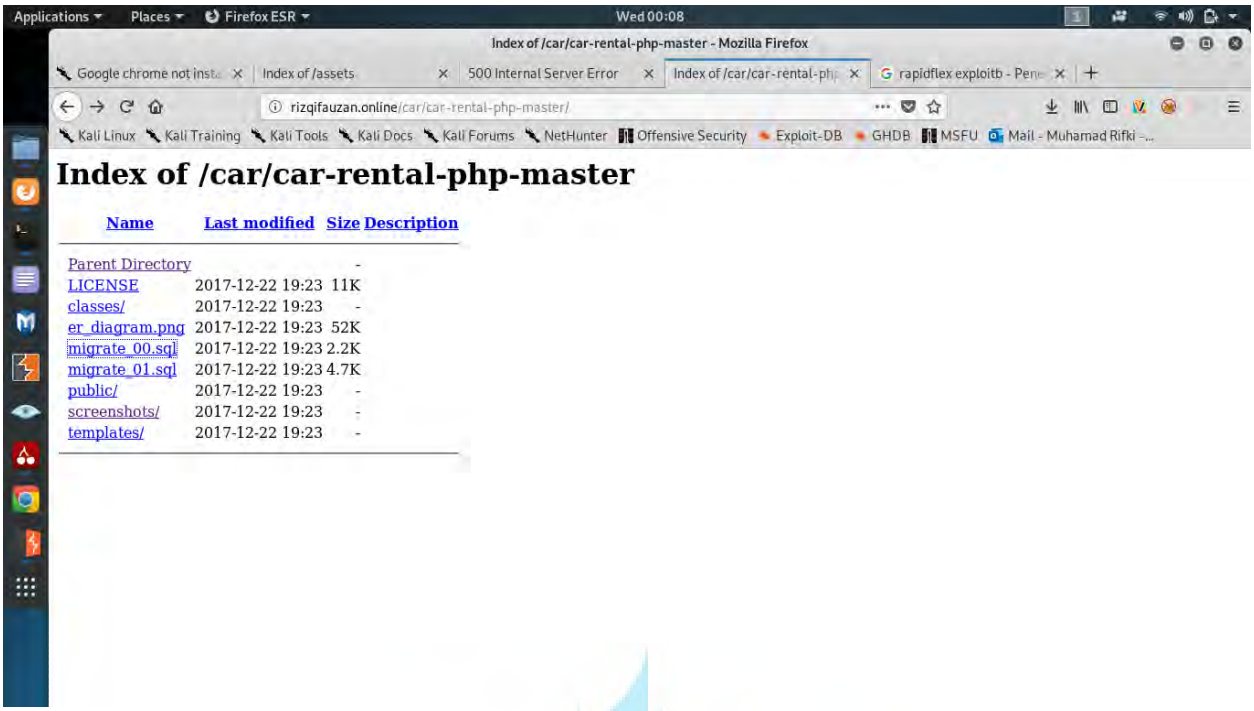
Impact :
From this findings , tester can found a lot of information like all directory name , configuration file , sensitive information and others.

Proof of concept :

Tester scanning all directory using dirbuster as shown by picture below.

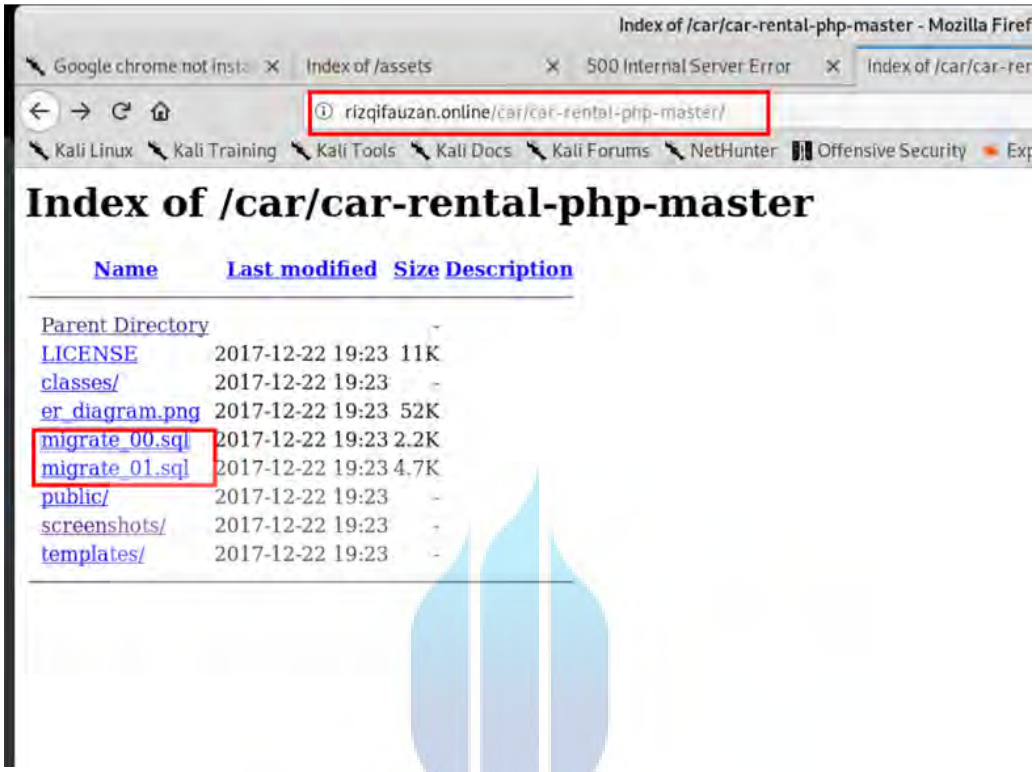


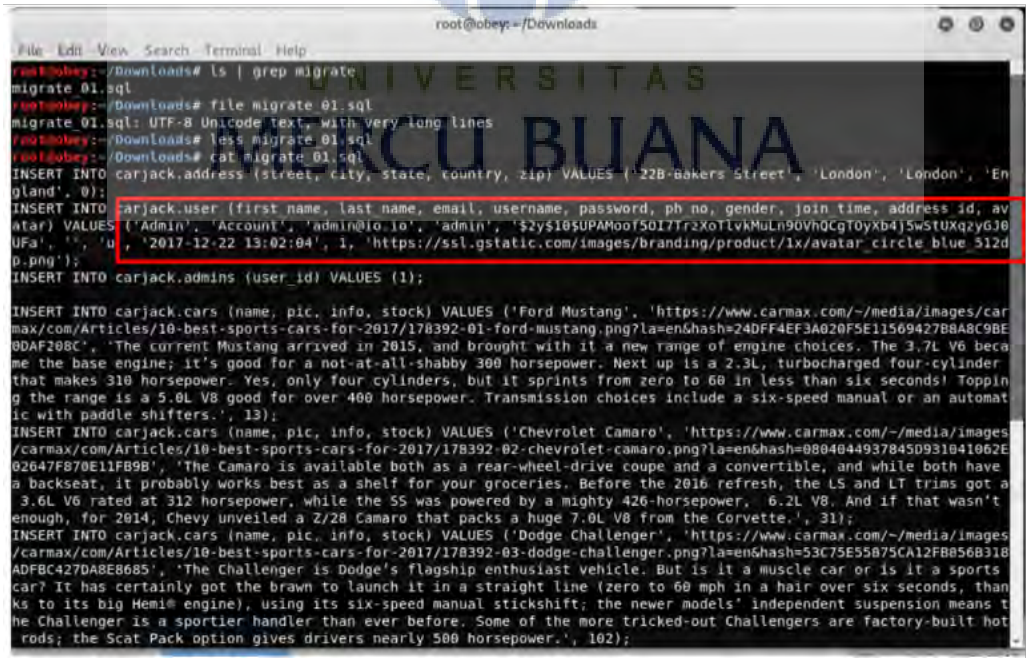
From that, tester crawling all the directory on web server manual with browser as figure out by a lot of image below.



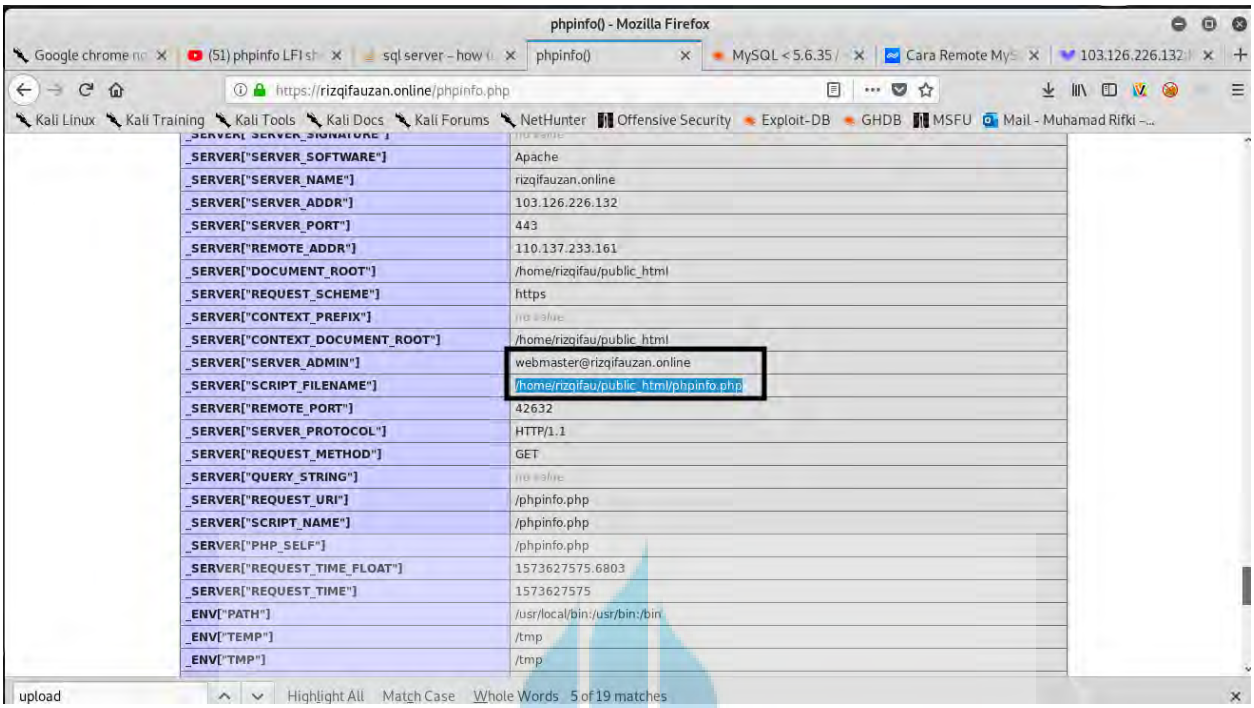
From all the directory findings above. Tester **Disclosing sensitive information** as shown below :

Database file (migrate.sql) which is containing the credential information from administrator and including the password.





After that , tester also found configuration file (php.info) on this server which is containing the email of crm web server , configuration script and others.



During about penetration testing, tester found a lot of directory listing enable on this web application. However, base on OWASP Framework. Directory listing is not allowed by the web application.

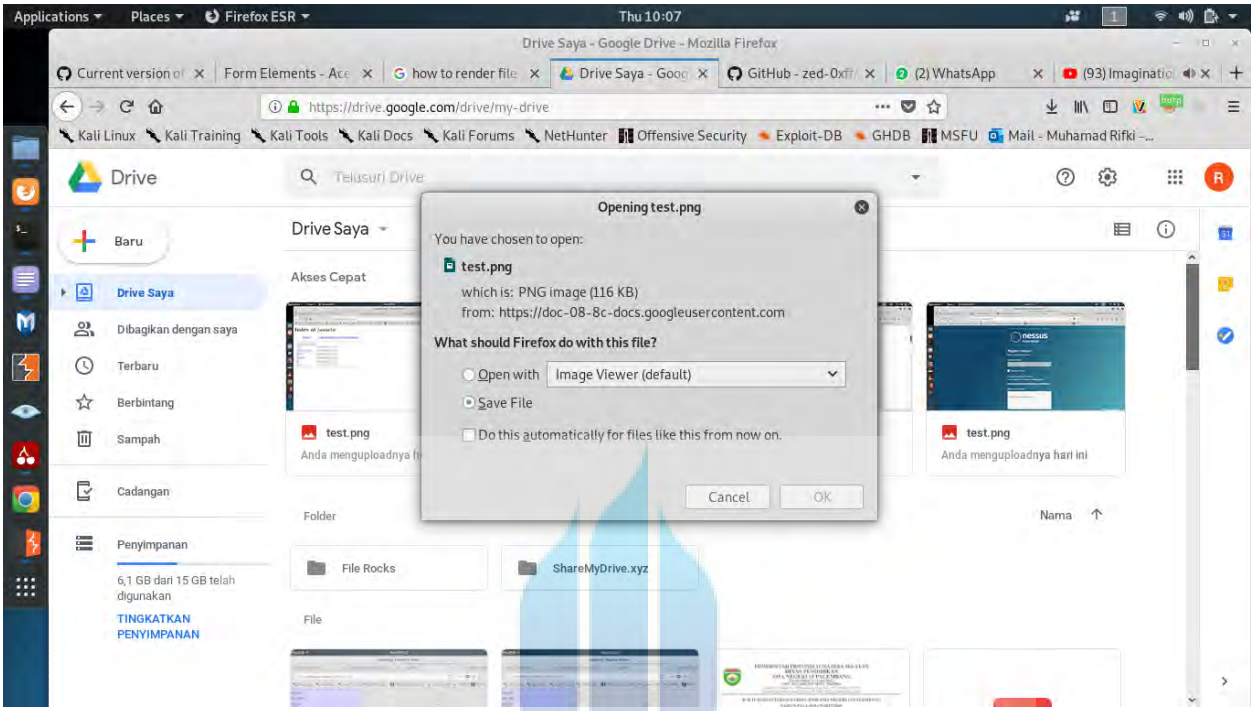
Reference : https://www.owasp.org/index.php/Top_10-2017_A6-Security_Misconfiguration

Recommendation :

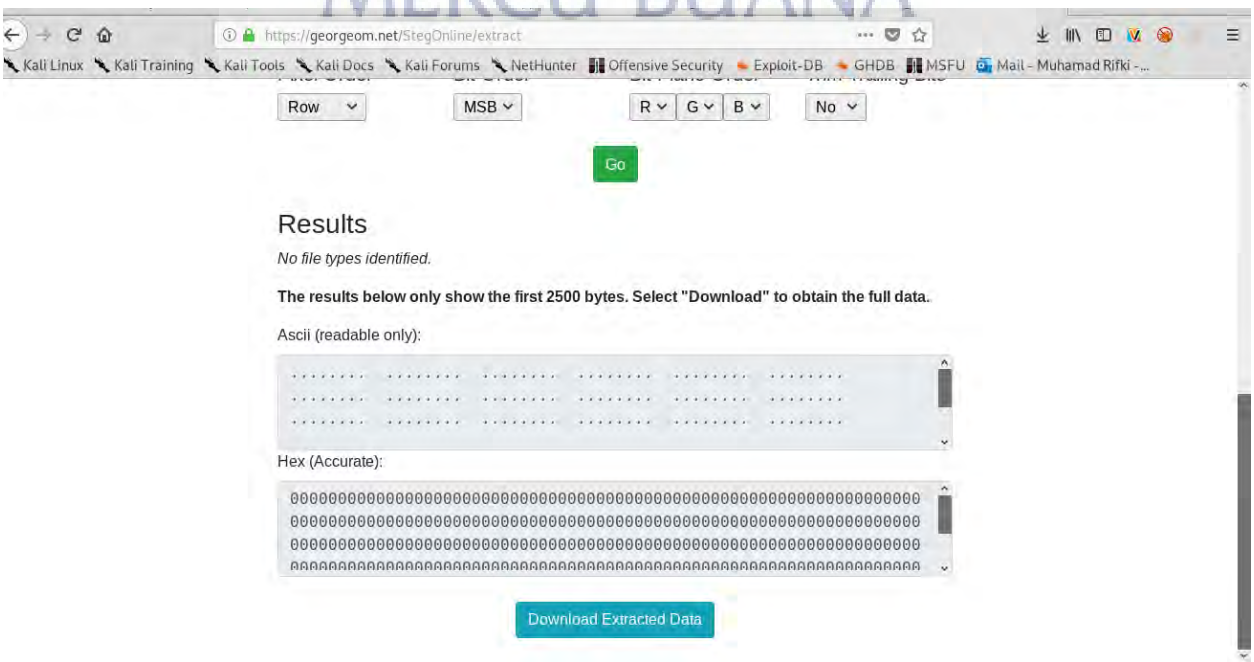
Disable all listed directory on web server by configure it Httaccess.

1.4 Steganography Testing

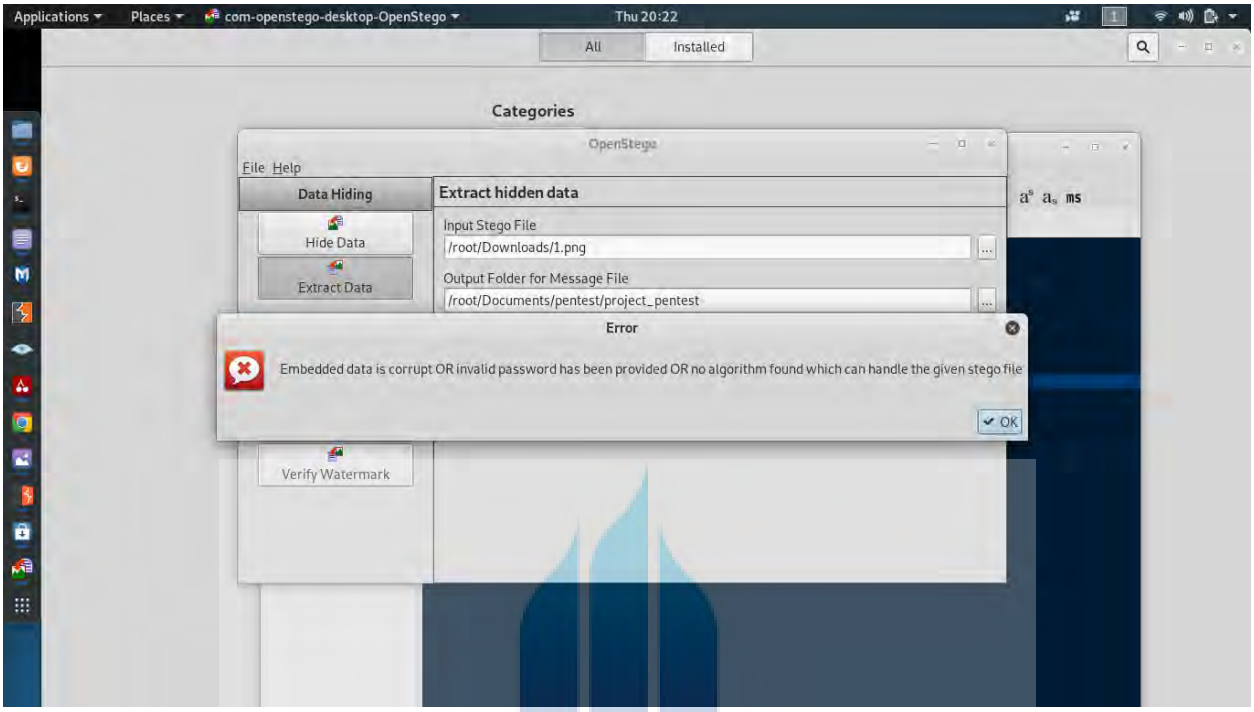
This web application giving us the service for hiding the secret text or document on to image file (png format). Tester try download one of encrypted file in web service as shown below.



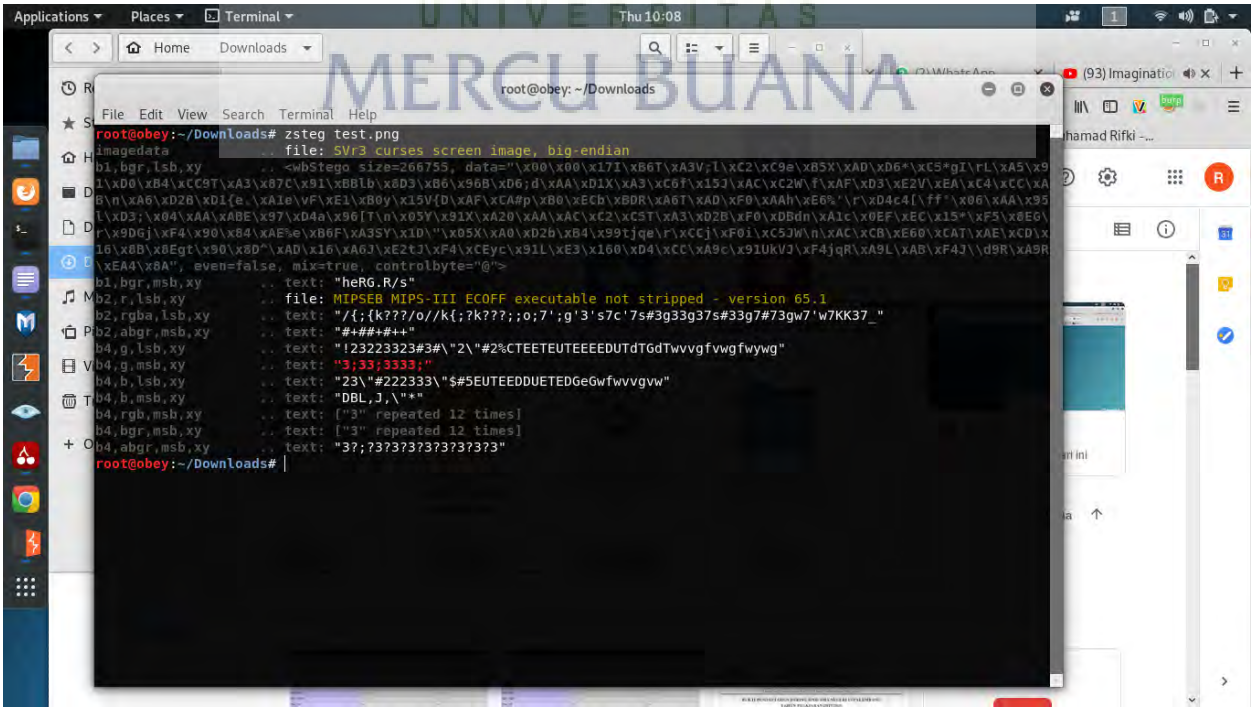
After that tester try to decode the file to get information about the secret text inside the png using online tools. Tester get no information about the secret text inside and fail to decode using this tools.



After that tester also try to decode it using openstego which is known as powerfull tools for decode / extracting sensitive information for steganography. And the result still same as before, this tools also giving no sensitive information as shown below.



Tester continue to use command line tools on kali linux to decode the stegano file as shown below and also can decode the steganography image.



KERTAS KERJA

Ringkasan

Seiring perkembangan zaman, kebutuhan masyarakat akan tempat penyimpanan informasi semakin meningkat. Saat ini telah ditemukan tempat penyimpanan berbasis awan yang sering kita sebut cloud storage. Cloud storage merupakan tempat menyimpan file secara online sehingga masyarakat tidak perlu khawatir jika memori mereka penuh. Cukup dengan koneksi internet, maka masyarakat dapat menyimpan file mereka secara online.

Google Drive merupakan salah satu produk dari google untuk mengatasi masalah ini. Masyarakat dapat menggunakan 15 GB penyimapan secara gratis. Produk ini dapat digunakan dengan mudah melalui mobile ataupun web browser.

Pada perkembanagn teknologi saat ini, internet bukan tempat yang dijamin aman untuk menyimpan dokumen. Berbagai cara dapat digunakan pengguna untuk menyadap dokumen yang kita simpan di internet. Oleh karena itu penggunaan kriptografi dan steganografi merupakan hal yang sangat diperlukan.

Kriptografi merupakan teknik untuk mengubah suatu pesan menjadi pesan yang sulit dibaca. Sedangkan Steganografi merupakan teknik untuk menyembunyikan pesan agar pesan tersebut tidak ditemukan. Dengan demikian diharapkan data yang tersimpan pada cloud storadge menjadi lebih aman.