

UAS Keamanan Informasi Kelas TI-PAGI

Nama: muhammad subaeri

Nim: 1410651187

Kelas: B

1. UAS Keamanan Informasi Kelas TI-PAGI

Aspek keamanan informasi mempunyai ruang lingkup yang luas. Menurut referensi dari ebook CISSP, ruang lingkup materi dari keamanan informasi terdiri dari 10 pokok permasalahan. Dari 10 pokok permasalahan tersebut, silakan buatlah resume salah satu pokok permasalahan dari keamanan informasi mengacu terhadap ebook CISSP yang sudah saya upload di elearning. Resume bukan hasil translate, melainkan inti-intinya saja dari materi yang sudah Anda pahami pada ebook tersebut. Hasil resume **tidak boleh** sama dengan teman-temannya, akan tetapi tema yang dibahas boleh sama.

2. UAS Keamanan Informasi Kelas TI-PAGI

Cari software atau tools pendukung keamanan informasi kemudian cobalah fungsional software tersebut untuk menangani kasus tertentu. Buatlah step by step yang terdiri dari screenshot, keterangan gambar, dan analisis. Misalnya penggunaan wireshark dalam melakukan analisis paket data jaringan (pcap file), penggunaan ftk forensic untuk mengetahui file steganografi, dan lain sebagainya. Review software boleh sama, akan tetapi kasusnya harus berbeda dengan temen-temennya.

JAWABAN NO 1

Kriptografi yang saya tahu dan yang sudah saya pelajari di di mata kuliah keamanan informasi

Itu arti dari krypto yaitu menyembunyikan sedangkan grafik itu text maka pengertian dari kriptografi adalah ilmu yang mempelajari teknik-teknik matematika dengan aspek keamanan informasi ,misalnya merahasiakan data ,tetapi semua aspek keamanan informasi bisa dapat di selesaikan dengan kriptografi ,serta krypto grafi juga seni untuk mengamankan keamanan pesan ,

Kriptorafi yang saya tau lagi digunakan untuk mengamankan text dengan mengacak atau menggunakan algoritma untuk bisa menjadi kode yang tidak bisa dibaca oleh seseorang ,dan proses yang sudah tidak bisa dibaca juga bisa dibuka dengan proses di bawah ini yang akan menjelaskan tentang perubahan yang akan di buat .

Kriptografi mempunyai 4 komponen yaitu :

1. Plaintext ,yaitu pesan yang bisa di baca
2. Ciphertext,pesan yang di acak yang tidak dapat di baca
3. Key,kunci untuk melakukan tehnik kriptografi
4. Algorith yaitu metode untuk melakuka encripsi dan dekripsi

Kemudian akan di proses

Yang pertama

Enkripsi adalah sebuah proses yang menjadikan pesan yang bisa di baca (plaintext)menjadi pesan acak yang tidak akan bisa di baca (chipertext).

Yang ke dua

Desripsi

Desripsi merupakan kebalikan dari encripsi di mana proses ini akan merubah chipertext menjadi plaintext dengan menggunakan algaridma 'pembalik 'dengan key yang sama ,

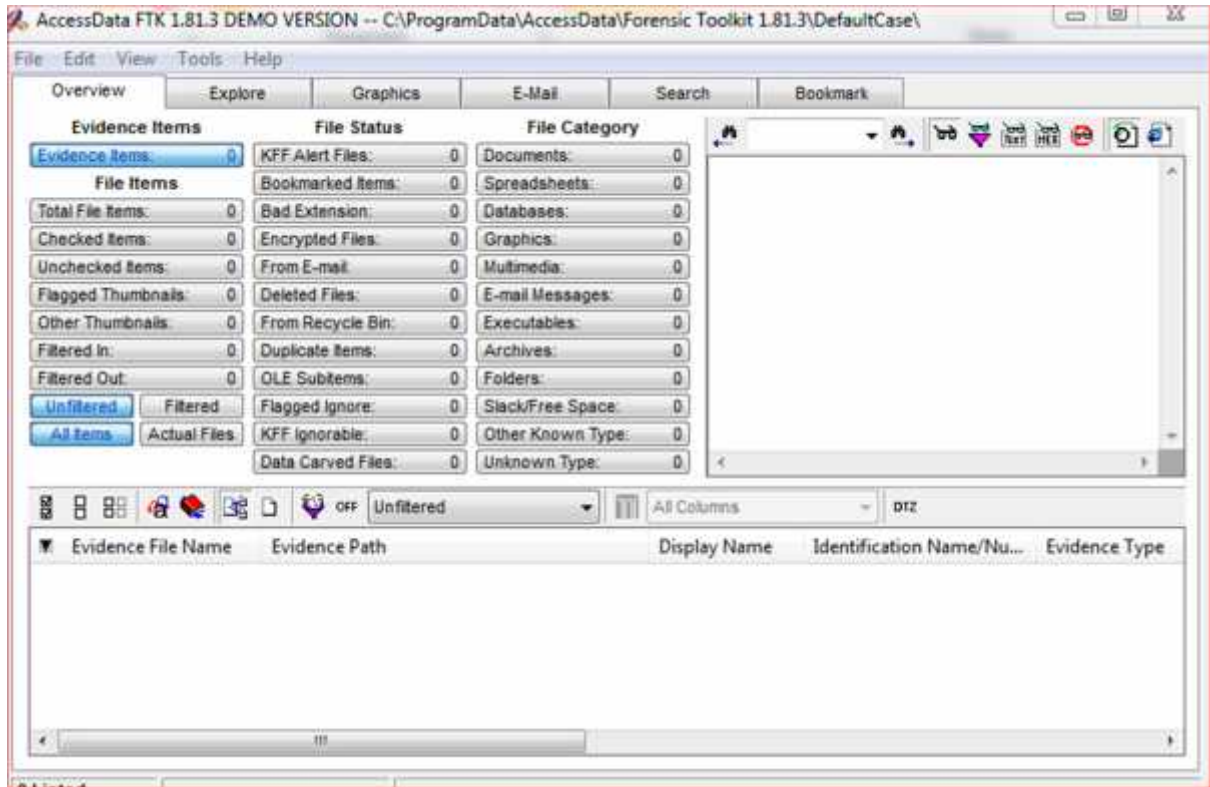
B

Dengan menggunakan ke dua proses di atas kita bisa membuat kode yang semula bisa di baca menjadi tidak bisa dibaca ,dan itulah kegunaan kriptografi atau bisa di katakan sebagai pembuatan kode ,dimana kode tersebut di buat dari data yang sudah ada dengan menggunakan algoritma matematika .

JAWABAN NO 2

Menganalisis/mengetahui file yang tersembunyi dengan menggunakan aplikasi toolkid

Pertama buka aplikasi tool kid



Ke dua klik file new case :

New Case

Find, Organize, & Analyze Computer Evidence

Forensic Toolkit®
Find Computer Evidence
Quickly and Easily

**AccessData's
Forensic Toolkit®-FTK®**
The Complete Analysis Tool

Wizard for Creating a New Case

Investigator Name: java

Case Information

Case Number: 1

Case Name: bay

Case Path: c:\ Browse...

Case Folder: c:\bay

Case Description:

Next > Cancel

Kemudian membuat nama folder yang akan di gunakan untuk menyimpan semua data yang ada di audio tersebut misalnya naman/case namanya bay seperti yang di atas , kemudian next dan terus next sampai di halaman yang ada namanya : Processes to perform

Evidence Processing Options

Processes to Perform

Evidence is added to a case in several steps. Some of the processes are always performed, while others are optional, depending on your needs and time/resource constraints.

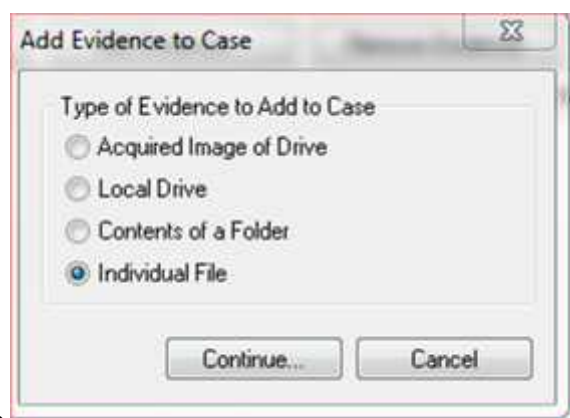
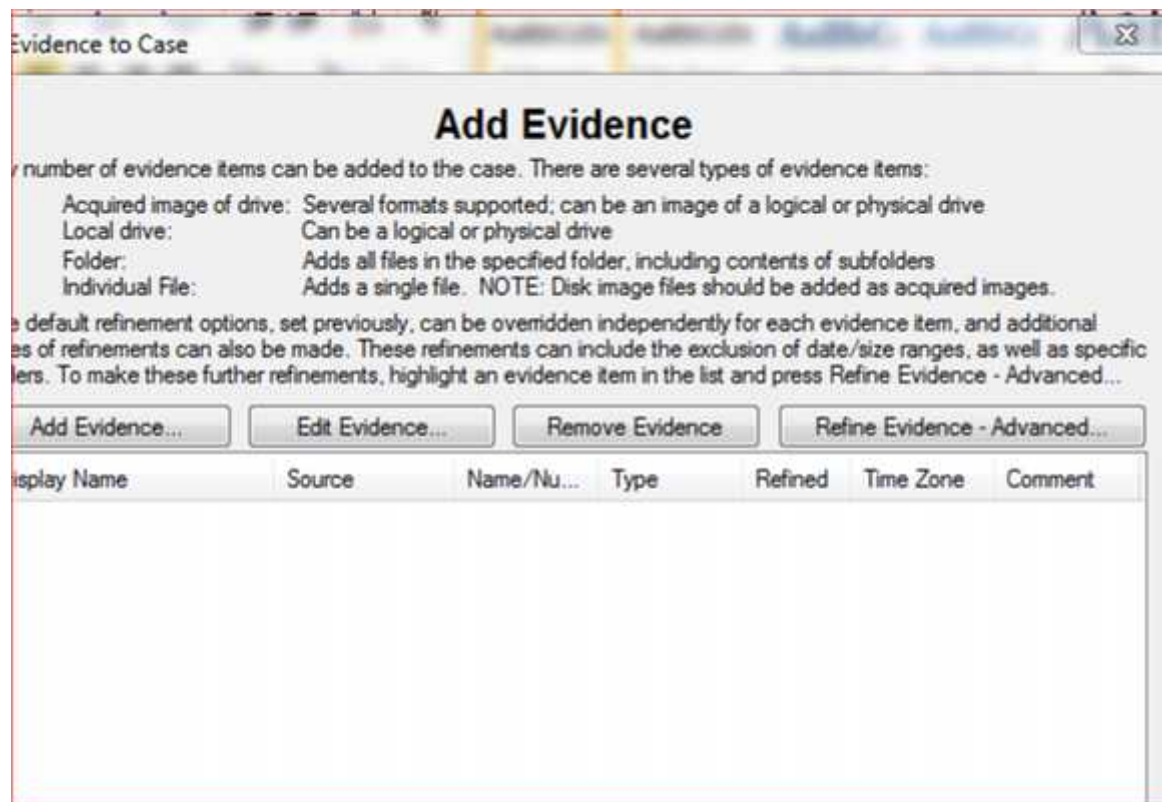
<input checked="" type="checkbox"/> MD5 Hash	An MD5 hash is a 16 byte value generated based upon a file's content. It is used to uniquely identify files. Hashes can be used to verify a file's integrity, or to identify duplicate files. MD5 hashes are used by the KFF to identify known files.
<input checked="" type="checkbox"/> SHA1 Hash	A SHA1 hash is a 20 byte value. The SHA1 hashing algorithm is newer than MD5, but is not yet as widely used.
<input checked="" type="checkbox"/> KFF Lookup	KFF (Known File Filter) is a utility that compares MD5 file hashes against a database of MD5 hashes from known files. The purpose of KFF is to eliminate files known to be unimportant, or to alert the investigator to known illicit or dangerous files.
<input checked="" type="checkbox"/> Entropy Test	For unknown file types, an entropy test is used to determine whether the file's data is compressed or encrypted. Such files contain no plain text and will not be indexed. Unnecessary indexing of such files can waste large amounts of time and resources.
<input checked="" type="checkbox"/> Full Text Index	The Forensic Toolkit includes a very powerful search engine, dtSearch, which enables the investigator to do instantaneous searching of textual data. In order to take advantage of this search feature, the data must first be indexed.
<input checked="" type="checkbox"/> Store Thumbnails	Create and store thumbnails for all graphics in the case. This option speeds up browsing through the Graphics view at the expense of consuming more space in the case folder.
<input checked="" type="checkbox"/> Decrypt EFS Files	Automatically locate and attempt to decrypt EFS encrypted files found on NTFS partitions within the case. (Requires AccessData Password Recovery Toolkit 5.20 or newer)
<input checked="" type="checkbox"/> File Listing Database	Create a Microsoft Access (Jet) database containing a list of all files in the case. The attributes included are based on the Preprocessing File Listing Database Column Setting. This database can be recreated with custom column settings in Copy Special.
<input type="checkbox"/> HTML File Listing	Create an HTML version of the File Listing.
<input type="checkbox"/> Data Carve	Automatically find specific file types embedded in other files and from free space. Retrieve results using Data Carving Option on Tools Menu.
<input type="checkbox"/> Registry Reports	Generate common registry reports during preprocessing.

Carving Options

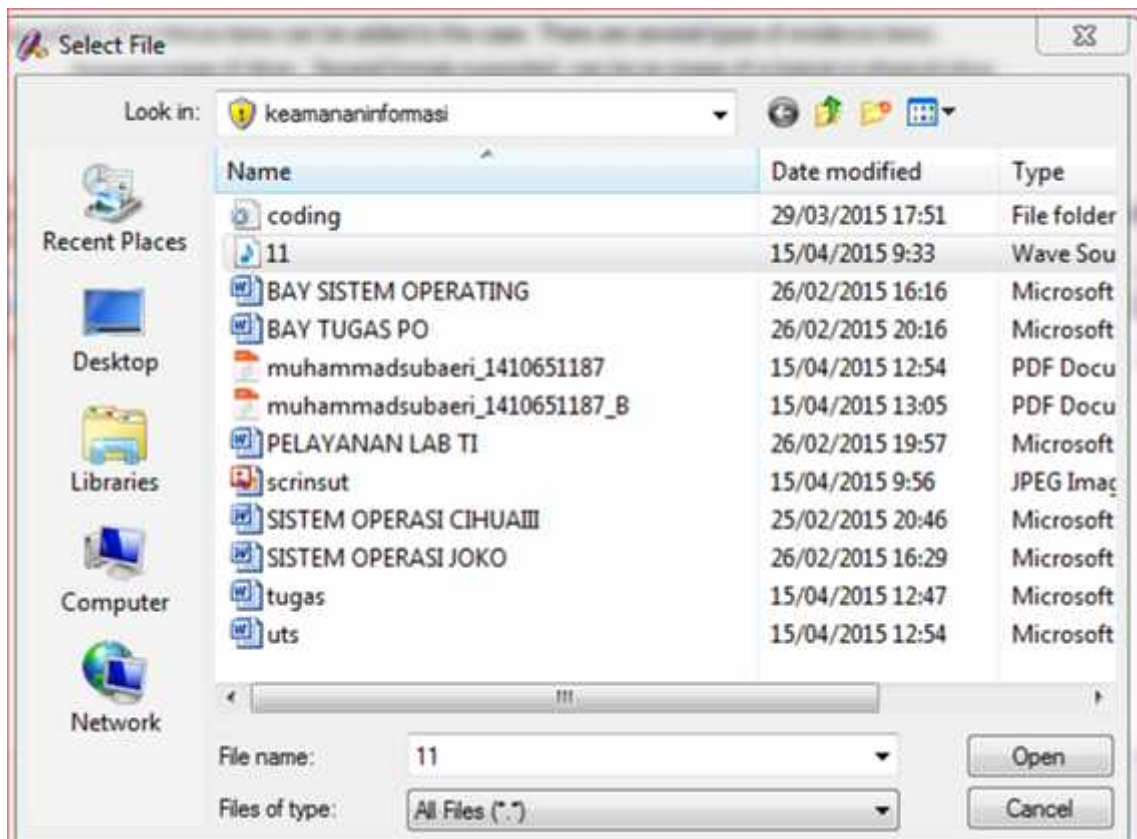
< Back Next > Cancel

kemudian anda centang semua nya terutama yang belum tercentang agar semua file itu bisa di temukan dan selanjutnya

next2 lagi sampai kehalaman {add evidence}

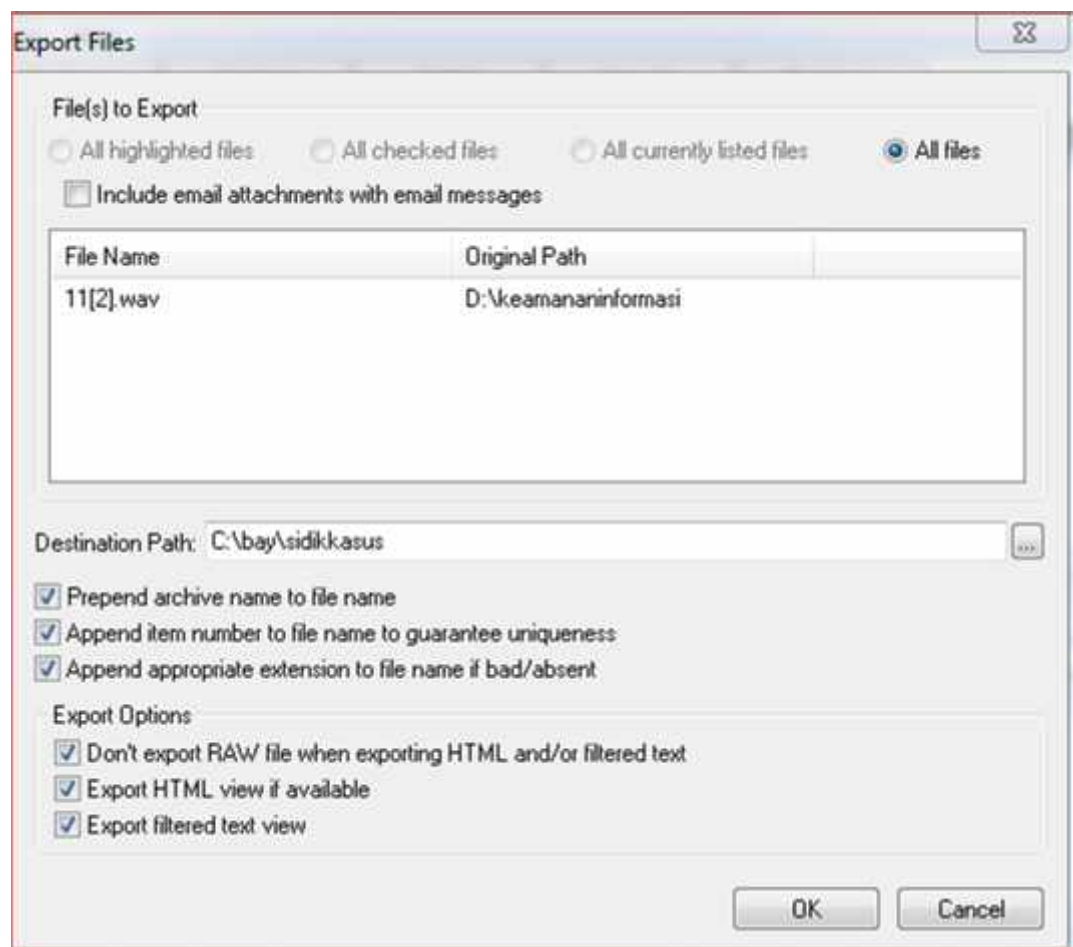


kemudian add evidence to case setelah ketemu maka di klikdan pilihlah individual file centang kemudian continue



pilih file yang akan di bongkar isinya misalnya seperti yang diatas jenisnya audio (11)kemudian dan next terus sampai kembali di halaman pertama .

kemudian untuk menemukannya file yang tersembunyi tersebut klik export file



Tuliskan tempat untuk menyimpan file yang akan anda cari contoh akan di simpan di data c maka beri format seperti yang di atas pada destinations path,dan silahkan centang semua pada export option jika sudah maka ok ,maka file yang akan anda cari akan ada di folder yang anda sudah tulis di destination path .kemudian anda ke folder c yang telah anda buat pertama di new case

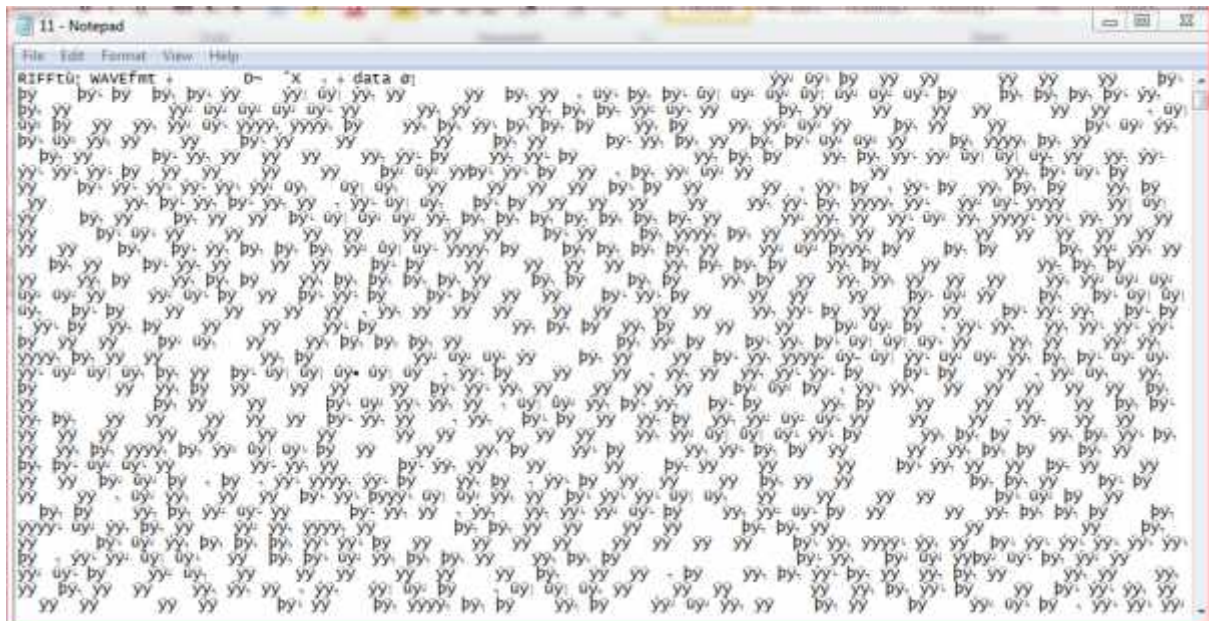
,kemudian ke folder yang telah di buat di export file (sidikkasus);

Cache	30/06/2015 19:42	File folder	
CrvTbIdx	30/06/2015 19:42	File folder	
efs	30/06/2015 19:43	File folder	
Export	30/06/2015 19:49	File folder	
index	30/06/2015 19:43	File folder	
sidikkasus	30/06/2015 19:51	File folder	
ThumbIdx	30/06/2015 19:42	File folder	
AccessDatabase	30/06/2015 19:43	Microsoft Access ...	80 KB
bay.ftk	30/06/2015 19:42	FTK File	1 KB
bfm	30/06/2015 19:43	GOM Media file(.d...	1.024 KB
bfm.idx	30/06/2015 19:43	IDX File	1.024 KB
bookmark	30/06/2015 19:43	GOM Media file(.d...	1.024 KB
bookmark.idx	30/06/2015 19:43	IDX File	1.024 KB
case	30/06/2015 19:45	GOM Media file(.d...	1.024 KB
case.idx	30/06/2015 19:45	IDX File	1.024 KB
case	30/06/2015 19:45	Configuration sett...	1 KB
evidence	30/06/2015 19:45	GOM Media file(.d...	1.024 KB
evidence.idx	30/06/2015 19:45	IDX File	1.024 KB
extract	30/06/2015 19:42	GOM Media file(.d...	1.024 KB
extract.idx	30/06/2015 19:42	IDX File	1.024 KB
file	30/06/2015 19:45	GOM Media file(.d...	1.024 KB
file.idx	30/06/2015 19:45	IDX File	1.024 KB
FTK	30/06/2015 19:45	Text Document	8 KB
FtkExaminer	30/06/2015 19:43	GOM Media file(.d...	1 KB
select	30/06/2015 19:43	GOM Media file(.d...	1.024 KB

next

11				
11	31...	Best op The Best	Mr. Jack	Laknat band

Seperti di bawah ini ,



Dari penemuan yang saya temukan seperti yang di atas ,saya jadi mengerti dan mengetahui bahwasanya file itu masih bisa dijadikan wadah atau tempat penyimpanan file lain dan itu sangat berguna bagi orang yang sering /memiliki file penting untuk tidak di ketahui oleh orang lain .dan dengan aplikasi tersebut saya bisa membuka kembli file yang sudah di sembunyikan ,meskipun saya masih belum tau cara menyimpan file tersebut .