KEAMANAN JARINGAN KOMPUTER

SIMULASI ALGORITMA STEGANOGRAFI DENGAN SOFTWARE OPEN PUFF

NAUFAL AHMAD FARAUQ

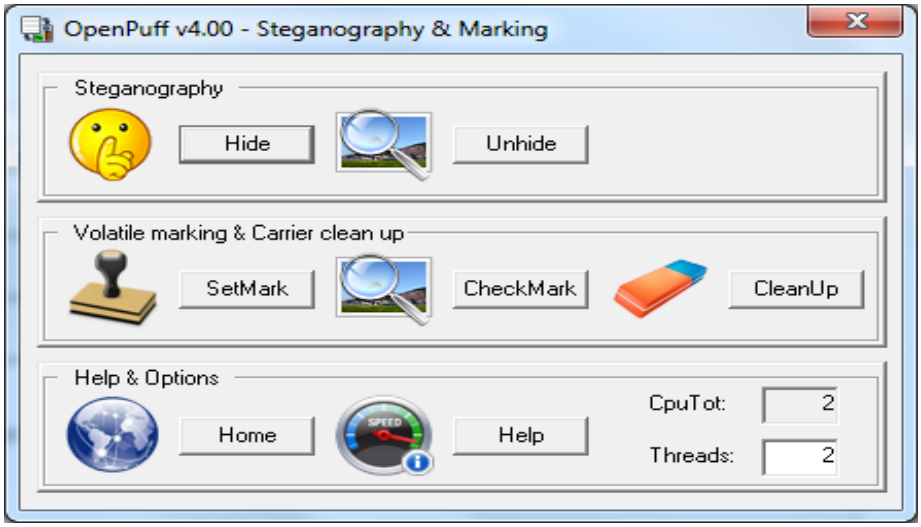
I. PENDAHULUAN

Steganografi adalah suatu teknik untuk menyembunyikan informasi yang bersifat pribadi dengan sesuatu yang hasilnya akan tampak seperti informasi normal lainnya. Media yang digunakan umumnya merupakan suatu media yang berbeda dengan media pembawa informasi rahasia, dimana disinilah fungsi dari teknik steganography yaitu sebagai teknik penyamaran menggunakan media lain yang berbeda sehingga informasi rahasia dalam media awal tidak terlihat secara jelas. Steganography juga berbeda dengan cryptography yaitu terletak padahasil keluarannya. Hasil dari cryptography biasanyaberupa data yang berbeda dari bentuk aslinya dan biasanya datanya seolah-olah berantakan namun dapat dikembalikan ke data semula. Sedangkan hasil dari keluaran steganography memiliki bentuk yang sama dengan data aslinya, tentu saja persepsi ini oleh indra manusia, tetapi tidak oleh komputer atau pengolah data digital lainnya. Selain itu pada steganography keberadaan informasi yang disembunyikan tidak terlihat/diketahui dan terjadi penyampulan tulisan (covered writing). Sedangkan pada cryptography informasi dikodekan dengan enkripsi atau teknik pengkodean dan informasi diketahui keberadaanya tetapi tidak dimengerti maksudnya. Namun secara umum steganography dan cryptography mempunyai tujuan yang sama yakni mengamankan data, bagaimana supaya data tidak dapat dibaca, dimengerti atau diketahui secara langsung. Steganography memanfaatkan kekurangan - kekurangan indra manusia seperti mata dan telinga. Dengan kekurangan inilah maka teknik ini dapat diterapkan dalam berbagai media digital. Media yang dimaksudkan adalah media dalam bentuk file digital dengan berbagai format, antara lain :Images (bmp, gif, jpeg, tif, dll), Audio (wav, Mp3, dll), Video (flv).

II. LANGKAH PERCOBAAN

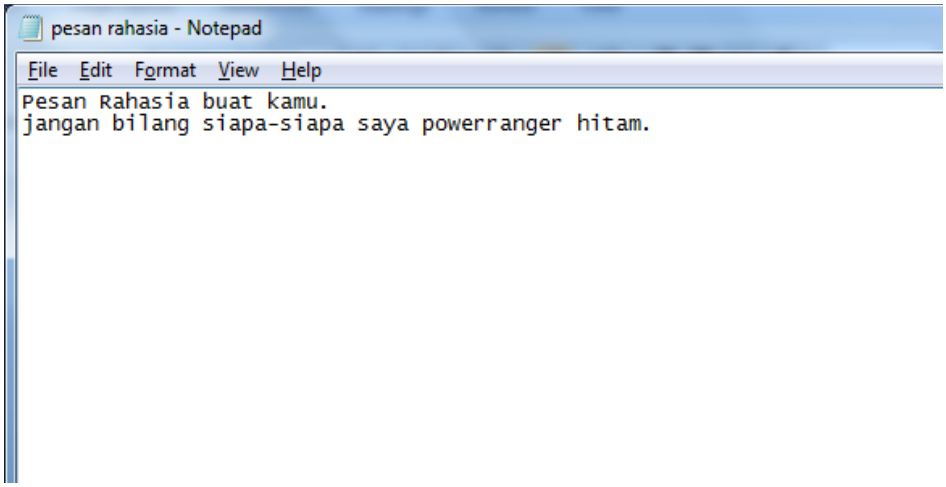
HIDING INFORMATION

1. Buka software Open Puff v4.00



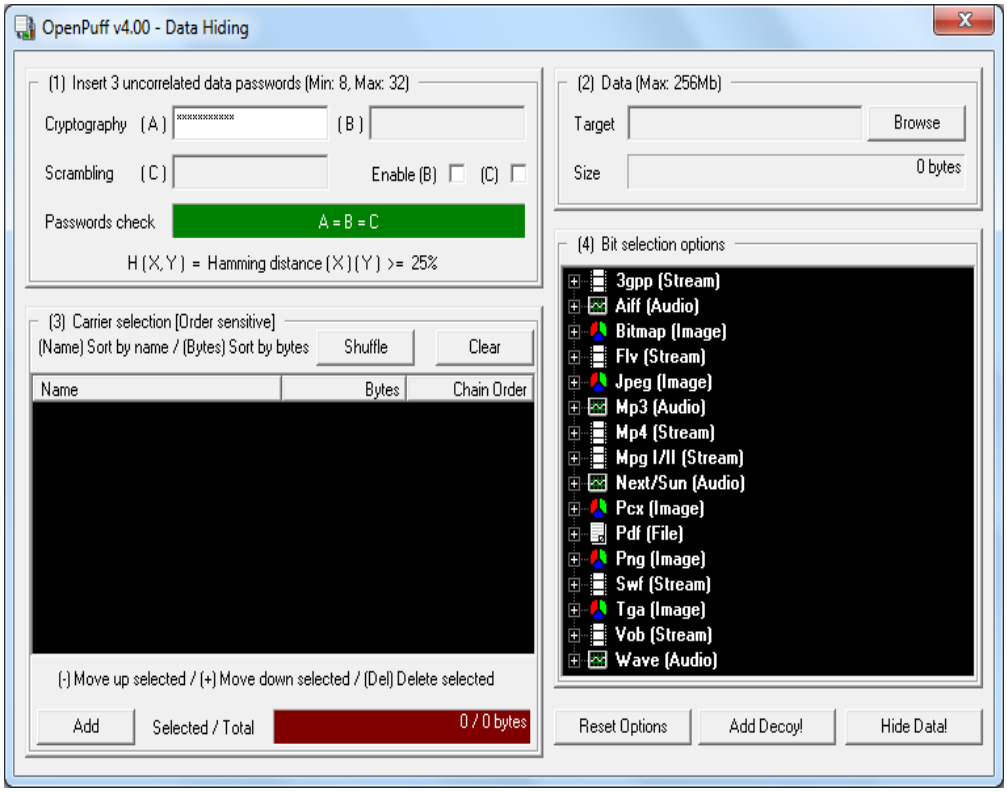
2. Pada gambar diatas merupakan tampilan dari Open Puff v4.00. Pilih menu steganography, menu hide untuk menyembunyikan informasi dan menu unhide untuk membuka informasi yang telah di-*hide*.

3. Buat file pesan yang akan disembunyikan dengan teknik steganografi. File pesan bisa berupa file .txt, .bmp, .jpg, .wav, .flv, dll. Dalam praktikum ini file pesan menggunakan file .txt

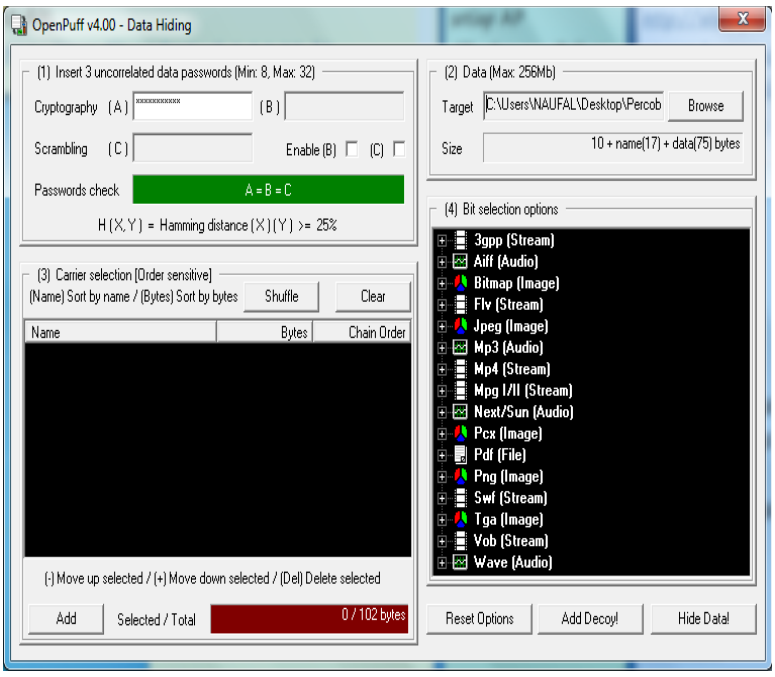


4. Klik hide pada Open Puff v4.00.

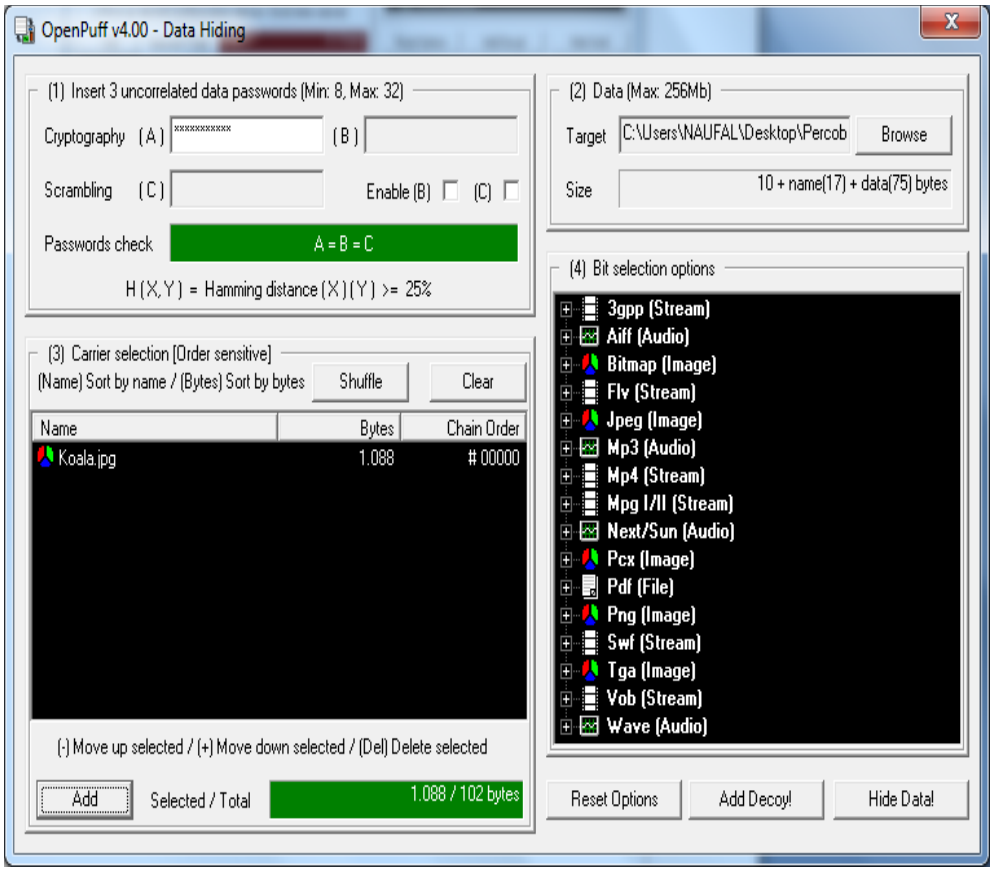
5. Masukkan *password* cryptography dengan minimal 8 karakter dan maksimal 32 karakter. Lihat seperti gambar dibawah ini.



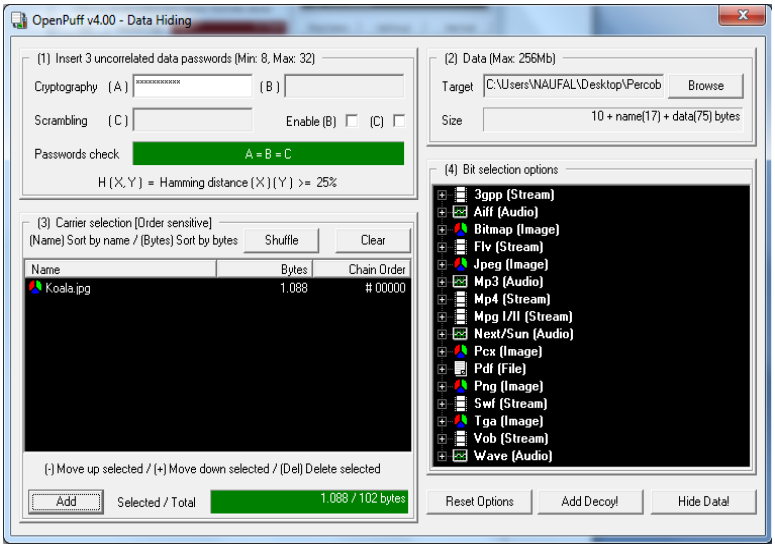
6. Pilih file dengan klik *browse* dengan maksimum data sebesar 256Mb, seperti gambar dibawah ini.



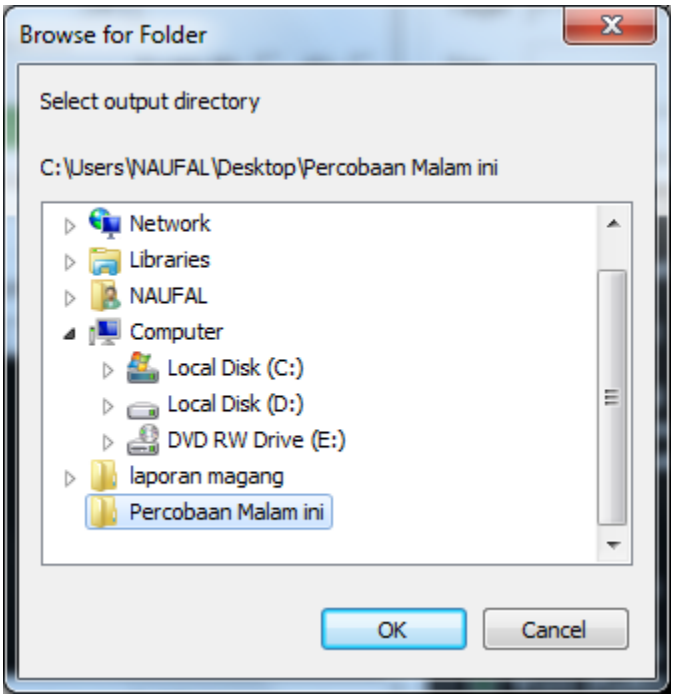
7. Tentukan file yang dijadikan sebagai file pengangkut. Kriteria file pengangkut harus lebih besar dari file yang akan dibawa. Klik add seperti gambar dibawah ini. Dari keterangan gambar dibawah ini diketahui bahwa file pengangkut dapat mengangkut maksimum sebesar file 1.088 bytes dan file yang diangkut sebesar 102 bytes.

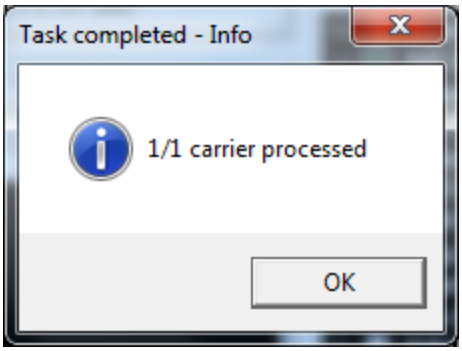


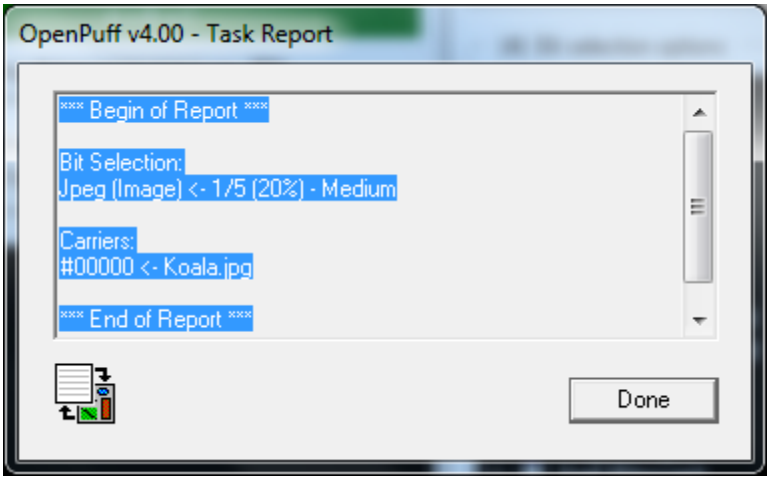
8. Klik *Hide Data*!



9. Pilih lokasi data akan disimpan.







10. Hasil dari langkah-langkah 1-9. Pada gambar dibawah ini dapat diketahui secara kasat mata bahwa file yang telah disisipi pesan dengan yang aslinya tampak sama.

Koala.jpg

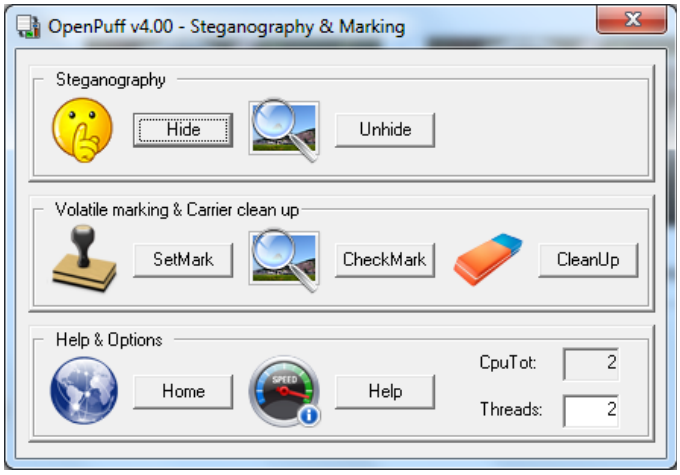
File asli yang tidak ada pesannya.

Koala A-1.jpg

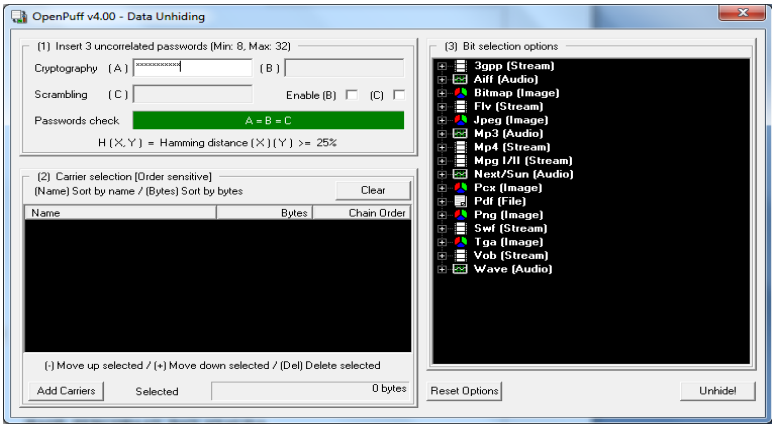
File yang telah disisipi pesan.

UNHIDE INFORMATION

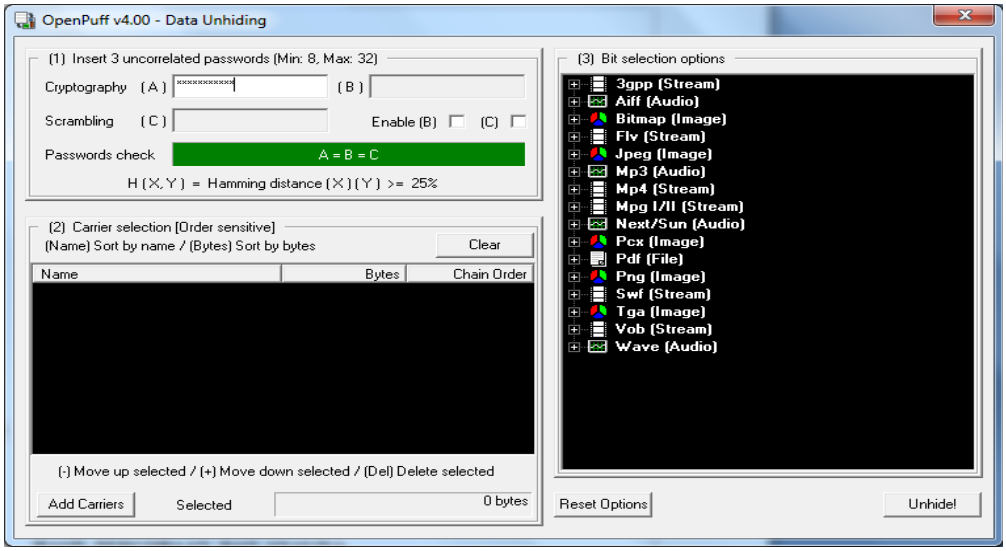
1. Buka software Open Puff v4.00. Klik *Unhide*

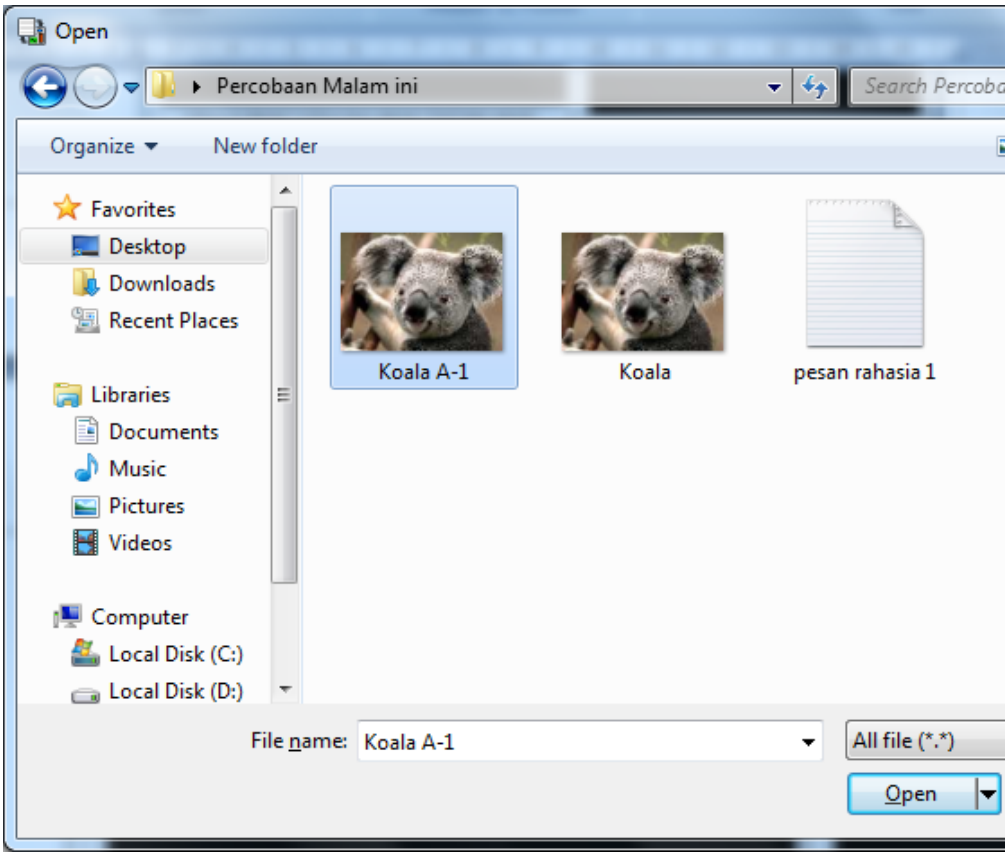


2. Masukkan *password* yang sama sesuai dengan saat *hidding Information*.

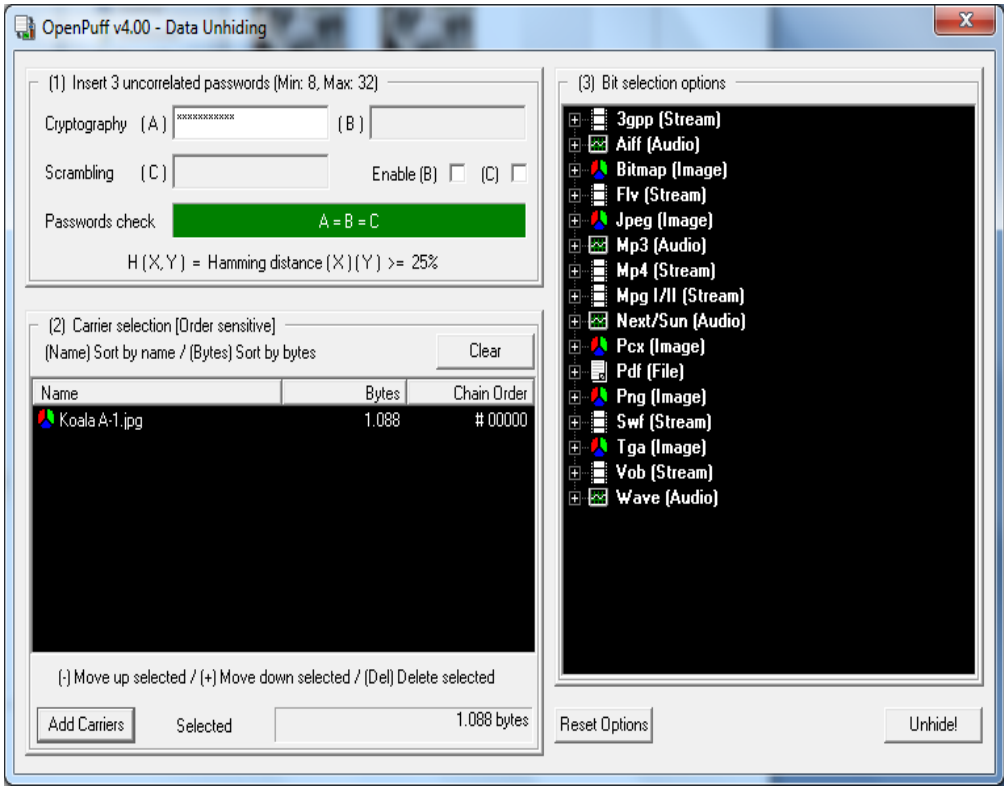


3. Selanjutnya *upload* file yang menjadi file pengangkut/pembawa. Klik *add carrier* dan cari file pembawa tadi.

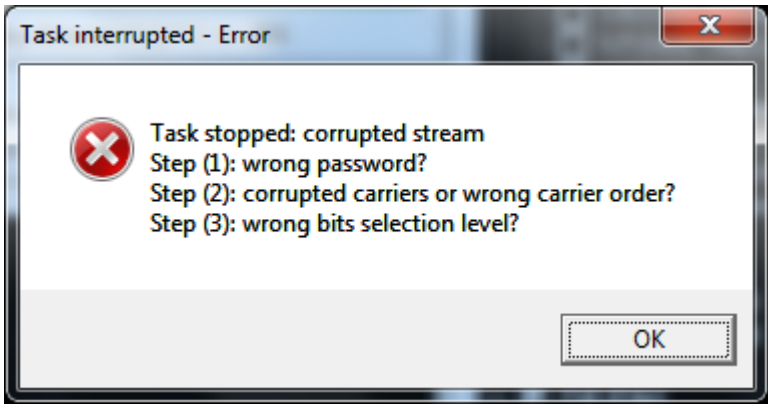




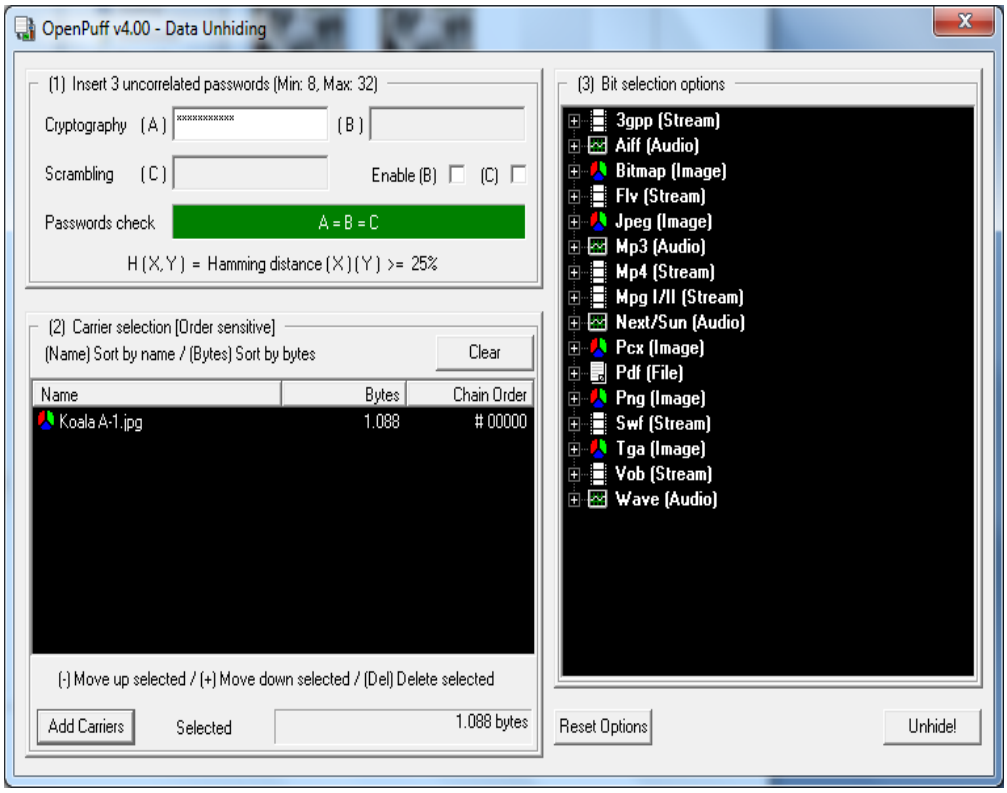
4. Setelah itu maka tampilan akan seperti gambar dibawah ini. Dan dapat diketahui juga file tersebut masih sama terdapat informasi file tersebut dapat mengangkut file sebesar 1088 bytes.

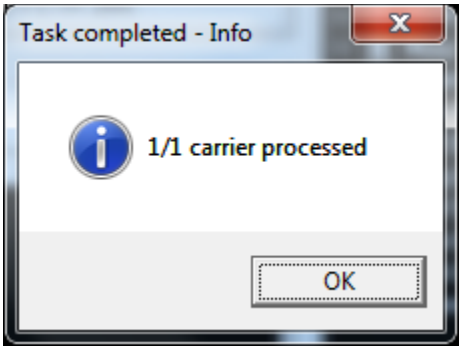


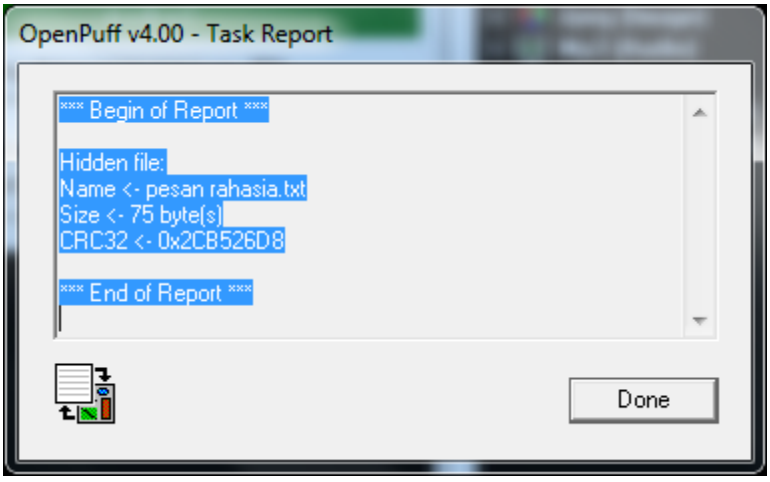
5. Sebelum *unhide* pastikan bahwa *password*, file pembawa, dan *bit selection levels* nya sama dengan saat *hiding information*. Jika dari kesemuanya itu tidak sama maka tidak akan bisa melakukan *unhide*. Seperti tampilan gambar dibawah ini.



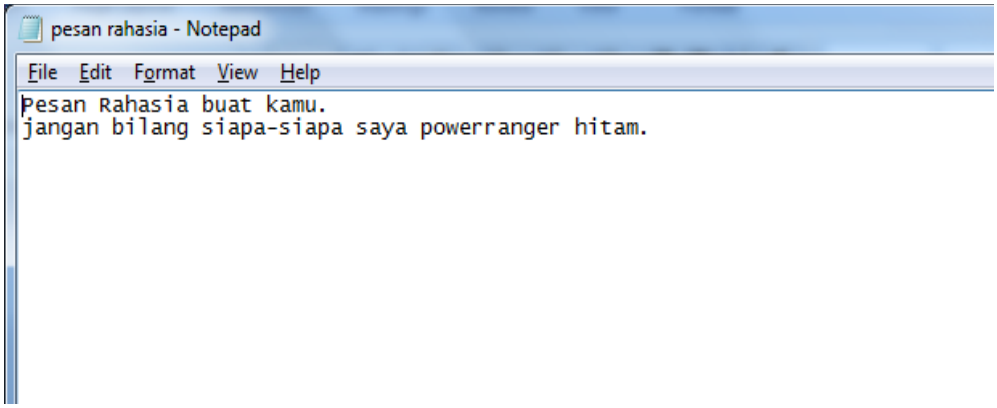
6. Kemudian klik *unhide*.







7. Setelah berhasil, file pesan yang tadinya terlebur dengan file pembawa dengan melakukan proses *unhide information* maka file pesan tersebut akan berpisah dengan file pembawanya. Tampilan dibawah ini merupakan file pesan setelah dipisahkan dari file pembawanya dan masih dalam keadaan dengan file format dan file name yang sama.



III. HASIL PERCOBAAN DAN ANALISA

Hasil percobaan seperti tabel dibawah ini.

Tabel. Hasil Percobaan

no	pesan msgs	yang harus diangkut (byte)	Jumlah byte yang dapat diangkut oleh pesan carrier (byte) dengan bit selection levels medium								
			JPG (581 KB)	JPG (836 MB)	JPG (3.45 MB)	MP3 (3.04 MB)	MP3 (4.75 MB)	MP3 (5.24 MB)	FLV (3.19 MB)	FLV (123 MB)	FLV (204 MB)
1	pesan-1.txt	26	448	1136	3488	4048	5792	8848	1360	35680	69008
2	pesan 1 - encrypted.txt	59									
3	pesan-2.txt	39									
4	pesan 2 - encrypted.txt	79									
5	pesan-3.txt	51									
6	pesan 3 - encrypted.txt	99									
7	pesan-4.txt	75									
8	pesan 4 - encrypted.txt	123									
9	pesan-5.txt	146									
10	pesan 5 - encrypted.txt	207									

Dari data tabel diatas dapat diketahui bahwa korelasi antara besar file message dengan besar file carrier yaitu seberapa besar file pesan yang dapat diangkut file penggankut dengan ukuran file yang sama, maka jumlah maksimum byte yang dapat diangkut besarnya sama.

Untuk jenis file *carrier* yang dapat mengangkut dengan daya angkut yang lebih besar dari data diatas adalah file MP3. Dari data percobaan diatas untuk file *carrier* dengan besar file lebih dari kisaran 3Mb dari jenis file *carrier* yang memiliki daya angkut yang lebih besar yakni MP3.

Kemudian untuk parameter pengaruh pesan yang telah terenkripsi pada proses steganografi, pengaruhnya hanya terletak pada besar file yang akan diangkut. Karena dapat dilihat dari tabel hasil percobaan diatas file pesan yang terenkripsi lebih besar dari pesan yang tidak terenkripsi. Dan juga lebih besarnya file yang harus diangkut dari file terenkripsi lebih besar dari file yang harus diangkut dari file tidak terenkripsi. Perbedaan file yang harus diangkut itulah yang merupakan perbedaan dari file yang terenkripsi dan tidak terenkripsi.

IV. KESIMPULAN

1. Software Open Puff digunakan untuk membuat keamanan pesan dengan teknik steganografi.
2. Agar dapat terjadi steganografi, besar file carriernya dari pengangkut harus lebih besar dengan file message yang harus diangkut.
3. Besar file message semakin besar maka semakin besar pula yang harus diangkut.
4. Besar jenis file carrier dengan daya angkut yang lebih besar adalah jenis .MP3.
5. Pengaruh file enkripsi pada file message dalam proses steganografi terletak pada besar ukuran yang harus diangkut lebih besar dari besar file message yang tidak terenkripsi.

V. REFERENSI

1. http://id.wikipedia.org/wiki/Steganografi
2. http://elista.akprind.ac.id/staff/catur/Multimedia/12-Keamanan%20Multimedia.pdf