

# **Tugas UAS Keamanan Informasi**



**Disusun oleh:**

**(Mohamad Rievan Hamdany)**

**(1310651095)**

**(A)**

**JURUSAN TEKNIK INFORMATIKA**

**FAKULTAS TEKNIK**

**UNIVERSITAS MUHAMMADIYAH JEMBER**

**2015**

# Tugas UAS 1

## Bab 10: Keamanan Lingkungan fisik

### TUJUAN UJIAN DALAM BAB INI

- Pertahanan Perimeter
- Pemilihan, Desain, dan Konfigurasi
- Pertahanan Sistem
- Kontrol Lingkungan

### PENGANTAR

Fisik (lingkungan) keamanan melindungi kerahasiaan dan integritas fisik aset: orang, bangunan, sistem, dan data. Ujian CISSP® menganggap manusia keselamatan sebagai perhatian yang paling penting dari domain ini, yang mengalahkan semua kekhawatiran lainnya.

### Pertahanan garis

Pertahanan perimeter membantu mencegah, mendeteksi, dan akses fisik tidak sah yang benar. Bangunan, seperti jaringan, harus menggunakan pertahanan berlapis. Salah satu pertahanan mungkin gagal, sehingga aset penting yang harus dilindungi oleh beberapa kontrol keamanan fisik, seperti pagar, pintu, dinding, kunci, dll yang ideal perimeter pertahanan aman, mencegah tidak sah masuknya, dan jika memungkinkan, menawarkan otentikasi dan akuntabilitas.

### Pagar

Pagar bisa berkisar dari pencegah sederhana (seperti 3-ft / 1-m pagar tinggi) untuk pencegahan perangkat, seperti 8-ft (2,4 m) -tall pagar dengan kawat berduri di atas. Pagar harus dirancang untuk mengarahkan masuknya dan jalan keluar untuk poin dikendalikan, seperti pintu eksterior.

### Gerbang

Gerbang berkisar kekuatan dari hias (kelas I gerbang dirancang untuk mencegah akses) ke gerbang kelas IV dirancang untuk mencegah mobil dari menabrak (seperti gerbang di bandara dan penjara). Untuk informasi lebih lanjut, lihat ASTM International "ASTM F2200" Spesifikasi Standar untuk Automated Vehicular Gerbang Konstruksi.

### Trotoar

Sebuah tonggak lalu lintas adalah posting yang kuat yang dirancang untuk menghentikan mobil. Istilah ini berasal dari singkat / posting yang kuat (disebut mooring bollards) digunakan untuk mengikat kapal untuk dermaga saat berlabuh.

## **Lampu**

Lampu dapat bertindak baik sebagai detektif dan kontrol jera. Cahaya harus terang cukup untuk menerangi bidang yang diinginkan visi (daerah yang dilindungi).

## **CCTV**

Closed-Circuit Television (CCTV) adalah perangkat detektif yang digunakan untuk penjaga bantuan dalam mendeteksi kehadiran penyusup di daerah terlarang. CCTV menggunakan spektrum cahaya normal membutuhkan visibilitas yang cukup untuk menerangi bidang pandang yang terlihat pada kamera. Perangkat inframerah dapat "melihat dalam gelap" dengan menampilkan panas. Lama "tabung kamera" adalah perangkat analog.

## **Kunci**

Kunci adalah kontrol keamanan fisik preventif, digunakan pada pintu dan jendela untuk mencegah akses fisik tidak sah. Kunci mungkin mekanik, seperti kunci kunci atau kombinasi kunci, atau elektronik, yang sering digunakan dengan kartu pintar atau magnet kartu strip.

## **Kunci kombinasi**

Kunci kombinasi memiliki cepat yang harus berpaling ke nomor tertentu, di tertentu order (bolak searah jarum jam dan berlawanan ternyata) untuk membuka. Tombol atau kunci keypad juga menggunakan kombinasi angka. Akuntabilitas terbatas karena bersama kombinasi adalah masalah keamanan utama mengenai jenis kunci.

## **Tailgating / membonceng**

Tailgating (juga dikenal sebagai membonceng) terjadi ketika orang yang tidak berhak berikut orang yang berwenang dalam gedung setelah orang yang berwenang membuka dan membuka pintu. Kebijakan harus melarang karyawan dari memungkinkan Tailgating dan keamanan upaya kesadaran harus menjelaskan risiko ini.

## **Jerat dan pintu putar**

Sebuah jerat adalah kontrol fisik preventif dengan dua pintu. Pintu pertama harus menutup dan kunci sebelum pintu kedua dapat dibuka. Setiap pintu biasanya membutuhkan bentuk terpisah dari otentikasi untuk membuka. Penyusup terjebak antara pintu setelah memasuki jerat tersebut. Pintu Putar dirancang untuk mencegah Tailgating dengan menegakkan "satu orang perotentikasi" aturan, seperti yang mereka lakukan di sistem kereta bawah tanah.

## **Cek Contraband**

Cek selundupan berusaha untuk mengidentifikasi benda-benda yang dilarang untuk memasuki aman. Pemeriksaan ini sering digunakan untuk mendeteksi logam, senjata, atau bahan peledak. Barang selundupan cek santai dianggap kontrol detektif, tapi kehadiran mereka dikenal membuat mereka juga jera ancaman aktual.

## **Detektor gerak dan alarm perimeter lainnya**

Ultrasonik dan gerak microwave detektor bekerja seperti "radar Doppler" yang digunakan untuk memprediksi cuaca. Gelombang energi dikirim keluar, dan "echo" dikembalikan ketika memantul obyek. Echo akan dikembalikan lebih cepat jika benda baru (Seperti orang yang berjalan di berbagai sensor) mencerminkan gelombang. Sebuah sensor gerak fotolistrik mengirimkan seberkas cahaya di ruang dipantau untuk sensor fotolistrik

## **Pintu dan jendela**

Selalu mempertimbangkan kekuatan dan kelemahan relatif dari pintu, jendela, dinding, lantai, langit-langit, dll Semua harus sama-sama kuat dari sudut pandang defensif: penyerang akan menargetkan "link terlemah dalam rantai" dan tidak harus mencari titik lemah untuk mengekspos. Jalan keluar harus terlepas dalam keadaan darurat, sehingga sebuah tombol sederhana atau detektor gerak yang sering digunakan untuk memungkinkan egress. Eksternal menghadapi darurat Pintu harus ditandai untuk penggunaan darurat saja dan dilengkapi dengan panik bar. Penggunaan bar panik harus memicu alarm. Jendela kaca secara struktural lemah dan dapat berbahaya ketika hancur. Antipeluru atau ledakan-tahan kaca dapat digunakan untuk daerah yang aman. Wire mesh atau Film keamanan dapat menurunkan bahaya kaca hancur dan memberikan kekuatan tambahan. Alternatif untuk jendela kaca termasuk polikarbonat seperti Lexan dan akrilik seperti sebagai plexiglass.

## **Dinding, lantai, dan langit-langit**

Dinding di sekitar perimeter aman setiap internal seperti pusat data harus "slab untuk slab, "yang berarti mereka harus mulai dari lantai slab dan lari ke slab langit-langit. Menonjol lantai dan langit-langit drop dapat mengaburkan mana dinding yang benar-benar mulai dan berhenti. Penyerang tidak harus bisa merangkak di bawah dinding yang berhenti di atas lantai mengangkat atau memanjat dinding yang berhenti di langit-langit drop.

## **Pengawal**

Penjaga kontrol dinamis yang dapat digunakan dalam berbagai situasi. Pengawal mungkin bantuan dalam pemeriksaan kredensial akses, memantau CCTV, monitor kontrol lingkungan, menanggapi insiden, bertindak sebagai pencegah (semua hal yang sama, penjahat lebih mungkin untuk menargetkan sebuah bangunan dijaga lebih bangunan dijaga), dan masih banyak lebih. Penjaga profesional telah mengikuti pelatihan lanjutan dan / atau sekolah; amatir penjaga (kadang-kadang merendahkan secara disebut "Mall Polisi") belum. Pseudo jangka Penjaga berarti penjaga keamanan bersenjata.

## **Anjing**

Anjing menyediakan perimeter tugas pertahanan, menjaga kaku "rumput." Mereka sering digunakan dalam daerah yang dikuasai, seperti antara bangunan dinding eksterior dan pagar perimeter. Kelemahan utama untuk menggunakan anjing sebagai kontrol perimeter adalah tanggung jawab hukum.

# SITUS SELEKSI, DESAIN, DAN KONFIGURASI

Seleksi, desain, dan konfigurasi menggambarkan proses membangun fasilitas yang aman seperti pusat data, dari proses pemilihan lokasi melalui desain akhir.

## Keandalan utilitas

Keandalan utilitas lokal merupakan masalah penting untuk tujuan pemilihan lokasi. Listrik padam adalah yang paling umum dari semua kegagalan dan bencana yang kita alami. Uninterruptible Power Supplies (UPS) akan memberikan perlindungan terhadap kegagalan listrik untuk waktu yang singkat (biasanya jam atau kurang). Generator memberikan lagi perlindungan tetapi akan membutuhkan pengisian bahan bakar untuk mengoperasikan untuk waktu yang lama.

## Kejahatan

Tingkat kejahatan lokal juga faktor dalam pemilihan lokasi. Masalah utama adalah karyawan keselamatan: semua karyawan memiliki hak untuk lingkungan kerja yang aman. Masalah tambahan termasuk pencurian aset perusahaan.

## Desain situs dan masalah konfigurasi

Setelah situs telah dipilih, sejumlah keputusan desain harus dibuat. Akankah Situs secara eksternal ditandai sebagai pusat data? Apakah ada bersama sewa di gedung? Dimana demarc telekomunikasi (titik demarkasi telekomunikasi)?

## Situs menandai

Banyak pusat data tidak eksternal ditandai untuk menghindari menarik perhatian fasilitas (Dan isi mahal dalam). Kontrol serupa termasuk perhatian-menghindari rincian seperti desain bangunan diredam.

# Pertahanan SYSTEM

Pertahanan sistem adalah salah satu garis pertahanan terakhir dalam strategi pertahanan-mendalam. Pertahanan ini mengasumsikan penyerang memiliki akses fisik ke perangkat atau media yang mengandung informasi sensitif. Dalam beberapa kasus, kontrol lain mungkin gagal dan ini kontrol adalah kontrol akhir melindungi data.

## Pelacakan aset

Rinci database pelacakan aset meningkatkan keamanan fisik. Anda tidak dapat melindungi Anda Data kecuali Anda tahu di mana (dan apa) itu. Aset rinci database pelacakan dukungan peraturan kepatuhan dengan mengidentifikasi di mana semua data diatur adalah dalam sebuah sistem. Dalam kasus pemutusan hubungan kerja karyawan, database aset akan menunjukkan peralatan apa sebenarnya dan data karyawan harus kembali ke perusahaan.

## Drive dan pita enkripsi

Drive dan enkripsi pita melindungi data pada saat istirahat dan merupakan salah satu dari sedikit kontrol

yang akan melindungi data setelah keamanan fisik telah dilanggar. Kontrol ini dianjurkan untuk semua perangkat mobile dan media yang mengandung informasi sensitif yang secara fisik dapat meninggalkan situs atau zona keamanan. Enkripsi seluruh disk dari perangkat mobile hard drive dianjurkan.

### **Media penyimpanan dan transportasi**

Semua data backup sensitif harus disimpan off-site, apakah menular off-site via jaringan atau fisik dipindahkan sebagai media backup. Situs menggunakan media backup harus ikuti prosedur yang ketat untuk media berputar off-site.

### **Pembersihan dan kerusakan Media**

Semua bentuk media harus aman dibersihkan atau dihancurkan sebelum dibuang untuk mencegah reuse objek, yang merupakan tindakan memulihkan informasi dari digunakan sebelumnya benda, seperti file komputer. Benda dapat bersifat fisik (seperti file-file kertas di manila folder) atau elektronik (data pada hard drive).

### **Shredders kertas**

Shredders kertas memotong kertas untuk mencegah penggunaan kembali objek. Jalur-cut shredders memotong kertas menjadi strip vertikal. Shredders potong lebih aman daripada strip-cut dan memotong kedua vertikal dan horizontal, menciptakan kertas kecil "confetti."

### **Timpa**

Timpa menulis lebih setiap karakter dari file atau seluruh disk drive dan jauh lebih mengamankan dari menghapus atau memformat disk drive. Metode umum termasuk menulis semua nol atau menulis karakter acak. Shredding elektronik atau menyeka menimpa file data sebelum menghapus entri FAT.

### **Degaussing dan kehancuran**

Degaussing dan kehancuran yang kontrol yang digunakan untuk mencegah serangan menggunakan kembali objek terhadap media magnetik seperti kaset magnetik dan disk drive.

## **KONTROL LINGKUNGAN**

Kontrol lingkungan dirancang untuk memberikan lingkungan yang aman bagi personil dan peralatan. Listrik, HVAC, dan keselamatan kebakaran dianggap kontrol lingkungan.

### **listrik**

Listrik yang dapat diandalkan sangat penting untuk data center dan merupakan salah satu prioritas utama saat memilih, membangun, dan merancang sebuah situs. Kesalahan listrik melibatkan pendek dan jangka panjang gangguan listrik, serta berbagai kasus tegangan rendah dan tinggi.

### **Pelindung Surge, UPS, dan generator**

Pelindung gelombang melindungi peralatan dari kerusakan akibat lonjakan listrik. Mereka berisi

sirkuit atau sekering yang tersandung selama lonjakan listrik atau lonjakan, korslet listrik atau mengatur itu ke tingkat yang dapat diterima.

## **HVAC**

HVAC (pemanas, ventilasi, dan pendingin udara) kontrol menjaga udara di wajar suhu dan kelembaban. Mereka beroperasi di loop tertutup, sirkulasi diperlakukan udara. Hal ini membantu mengurangi debu dan kontaminan udara lainnya. Unit HVAC harus mempekerjakan tekanan positif dan drainase. Pusat data unit HVAC dirancang untuk mempertahankan suhu optimum dan tingkat kelembaban untuk komputer

## **Statis dan korosi**

Statis diatasi dengan menjaga kelembaban yang tepat, landasan semua sirkuit dalam yang tepat cara, dan menggunakan semprotan antistatik, tali pergelangan tangan, dan permukaan kerja. Semua personil bekerja dengan peralatan komputer yang sensitif seperti papan, modul, atau memori chip harus tanah sendiri sebelum melakukan pekerjaan apapun. Tingkat kelembaban yang tinggi dapat memungkinkan air di udara mengembun ke (dan ke) peralatan, yang dapat menyebabkan korosi. Baik statis dan korosi yang dikurangi dengan mempertahankan tingkat kelembaban yang tepat.

## **Panas, api, dan detector asap**

Detektor panas peringatan ketika suhu melebihi sebuah dasar yang aman didirikan. Mereka dapat memicu ketika suhu tertentu terlampaui atau ketika perubahan suhu pada tingkat tertentu. Detektor asap bekerja melalui dua metode utama: ionisasi dan fotolistrik. Berbasis ionisasi detektor asap mengandung sumber radioaktif kecil yang menciptakan biaya listrik kecil. Sensor fotolistrik bekerja dengan cara yang sama, kecuali bahwa mereka mengandung LED (Light-Emitting Diode) dan sensor fotolistrik yang menghasilkan biaya kecil saat menerima cahaya. Kedua jenis peringatan alarm ketika interupsi asap radioaktivitas atau cahaya, menurunkan atau memblokir muatan listrik. Detektor api mendeteksi inframerah atau ultraviolet cahaya yang dipancarkan dalam api. Satu kelemahan untuk jenis deteksi adalah bahwa detektor biasanya membutuhkan line-of-sight untuk mendeteksi api; detektor asap tidak memiliki keterbatasan ini.

## **Keselamatan personel, pelatihan, dan kesadaran**

Keselamatan personel adalah nomor satu tujuan keamanan fisik. Ini termasuk keamanan personel sementara di tempat dan off. Pelatihan keselamatan memberikan keterampilan mengatur seperti belajar untuk mengoperasikan sistem tenaga darurat. Kesadaran keselamatan perubahan perilaku pengguna (Jangan biarkan orang mengikuti Anda ke dalam gedung setelah Anda menggesek kartu akses Anda). Kedua pelatihan keselamatan dan kesadaran sangat penting untuk memastikan keberhasilan fisik program keamanan. Anda tidak pernah bisa berasumsi bahwa personel rata-rata akan tahu apa yang harus dilakukan dan bagaimana melakukannya: mereka harus dilatih dan disadarkan.

## **Rute evakuasi**

Rute evakuasi harus jelas diposting, karena mereka berada di kamar hotel. Semua personil harus diberitahukan mengenai rute evakuasi tercepat dari daerah mereka. Tamu harus disarankan rute evakuasi juga. Semua situs harus menggunakan titik pertemuan, di mana semua

personil akan bertemu dalam acara darurat. Poin rapat penting: tragedi terjadi di mana seseorang Kontrol lingkungan luar depan bangunan tidak menyadari lain di luar kembali dan masuk kembali bangunan untuk berusaha menyelamatkan.

### **Peran dan prosedur evakuasi**

Kedua peran evakuasi utama adalah sipir keamanan dan pemimpin titik pertemuan. Itu Sipir keselamatan memastikan bahwa semua personel aman mengevakuasi bangunan dalam hal keadaan darurat atau bor. Pemimpin titik pertemuan menjamin bahwa semua personil menyumbang di titik pertemuan darurat

### **Kebakaran ABCD dan penindasan**

Isu keamanan utama dalam kasus kebakaran adalah evakuasi yang aman. Sistem pemadaman kebakaran digunakan untuk memadamkan kebakaran, dan berbagai jenis kebakaran memerlukan penekanan yang berbeda agen. Sistem ini biasanya dirancang dengan keselamatan personil sebagai primary perhatian.

### **Kelas agen kebakaran dan penindasan**

Kebakaran kelas A adalah bakar umum seperti kayu, kertas, dll Jenis api yang paling umum dan harus dipadamkan dengan air atau asam soda. Kebakaran kelas B membakar alkohol, minyak, dan produk minyak bumi lainnya seperti bensin. Mereka dipadamkan dengan asam gas atau soda.

### **peralatan**

atau kabel. Kebakaran listrik kebakaran konduktif, dan agen pemadam harus menjadi nonconductive, seperti jenis gas. Banyak sumber keliru daftar asam soda sebagai direkomendasikan untuk kebakaran kelas C: ini tidak benar, karena asam soda bisa menghantarkan

### **listrik.**

Kebakaran kelas D membakar logam dan dipadamkan dengan bubuk kering. Kebakaran kelas K kebakaran dapur, seperti membakar minyak atau lemak. Bahan kimia basah digunakan untuk memadamkan kebakaran kelas K. Tabel 10.1 merangkum kelas kebakaran dan penindasan

### **agen.**

Jenis agen pencegah kebakaran Semua agen pencegah kebakaran bekerja melalui empat metode (kadang-kadang dalam kombinasi): mengurangi suhu api, mengurangi pasokan oksigen, mengurangi pasokan bahan bakar, dan campur dengan reaksi kimia dalam api.

### **Air**

Air menekan api dengan menurunkan suhu di bawah titik ranting (juga disebut titik pengapian). Air adalah yang paling aman dari semua agen penekan dan dianjurkan untuk pemadam kebakaran terbakar umum seperti kertas terbakar atau kayu.



## Tugas UAS 2

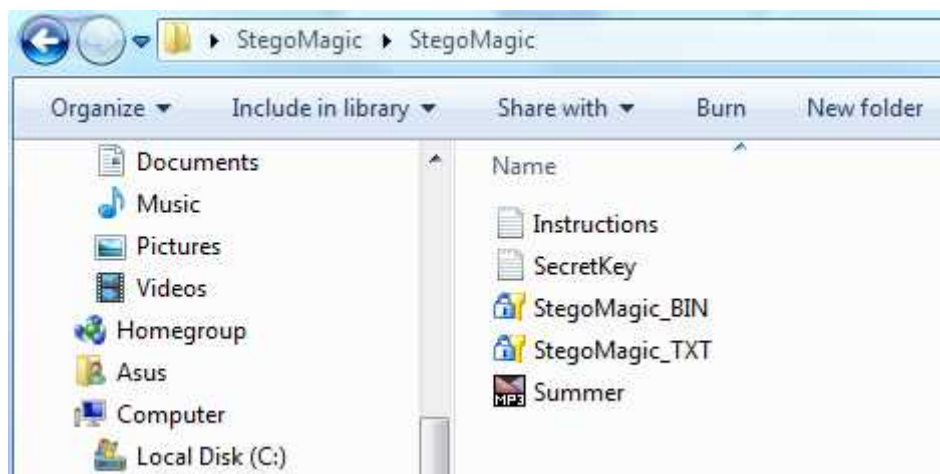
### StegoMagic

Pada Kesempatan kali ini saya akan membagikan tutorial atau step by step cara bagaimana menyimpan file rahasia dan membukanya kembali menggunakan software StegoMagic

- 1) Siapkan software StegoMagic



- 2) Masukkan file yang akan dijadikan tempat menyimpan sebuah pesan rahasia

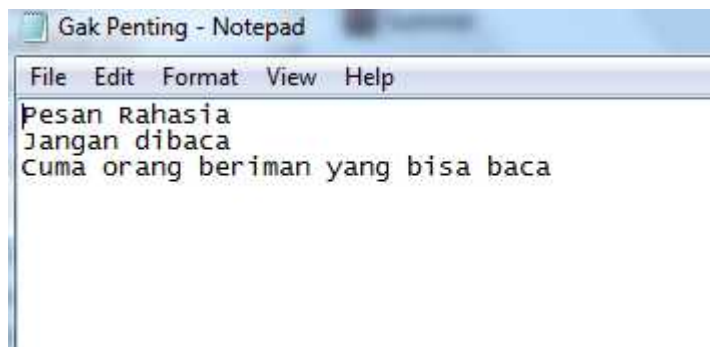


Disini saya menggunakan file Summer.mp3 sebagai tempat untuk menyimpan sebuah pesan rahasia

3) Membuat pesan rahasia yang di inginkan

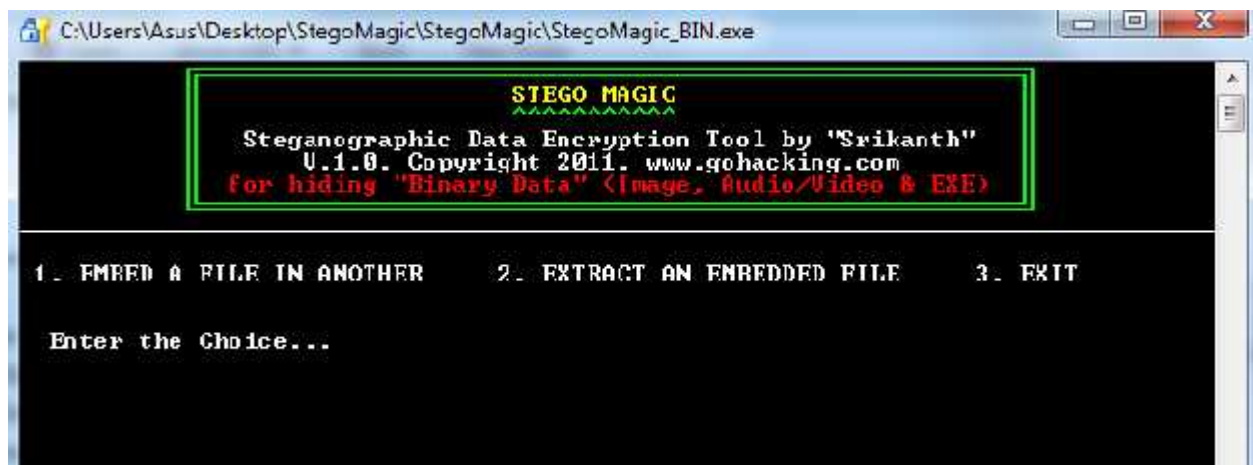


Disini saya menambahkan file Gak Penting.txt sebagai file pesan yang akan di rahasiakan

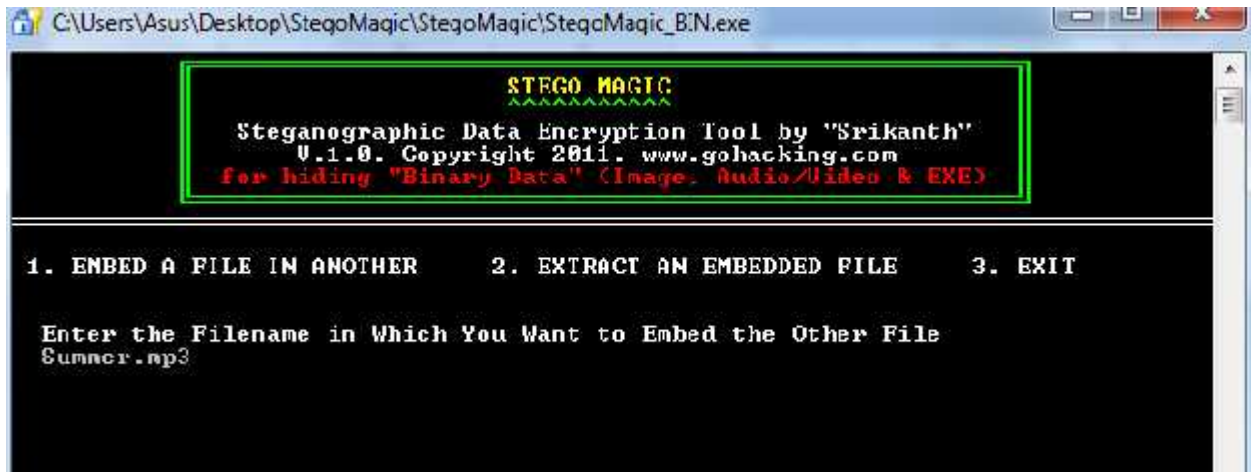


Ketik pesan apa yang akan di rahasiakan

4) Buka software StegoMagic\_BIN



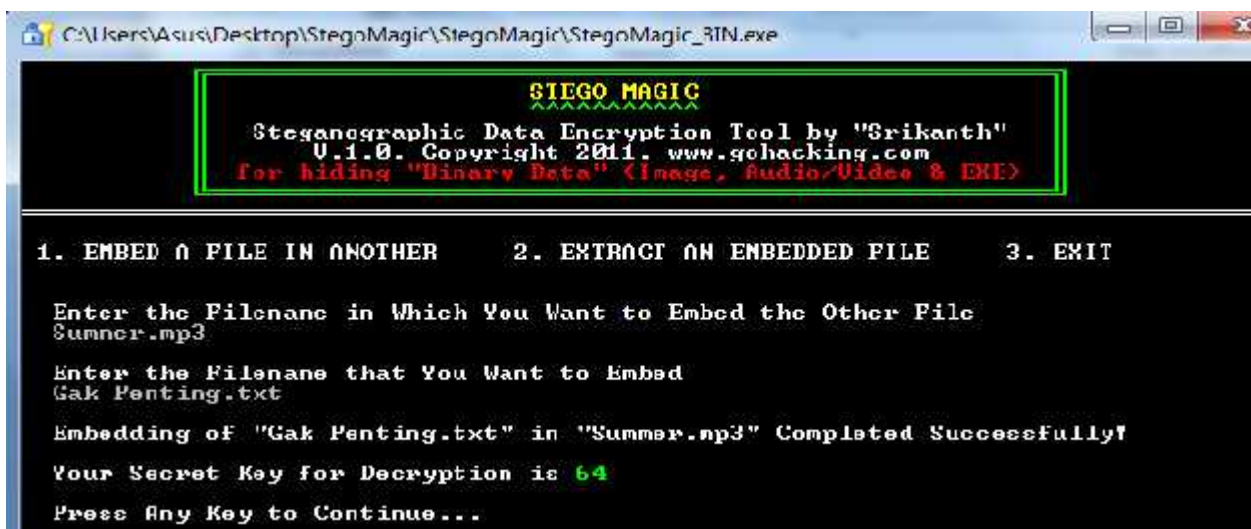
Lalu tekan 1 dan Ketik nama file yang akan dibuat sebagai tempat menyimpan pesan rahasia lalu enter



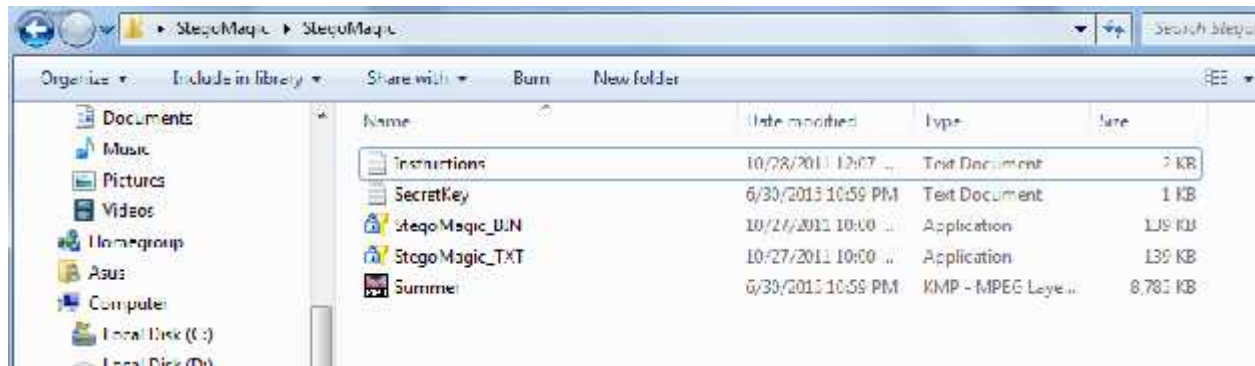
Selanjutnya Ketik nama file yang akan di rahasiakan lalu enter



Ingat secret key buat membuka file yang dirahasiakan tadi

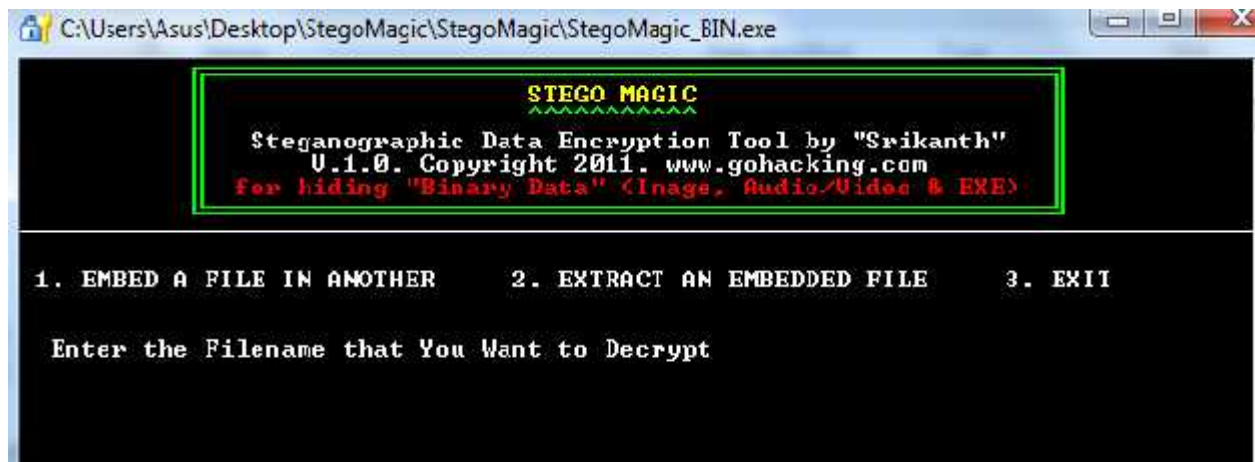


Dan hasilnya file telah di rahasiakan di dalam file Summer.mp3



5) Cara untuk membuka file yang sudah di sembunyikan,

Buka StegoMagic\_BIN kembali dan tekan 2

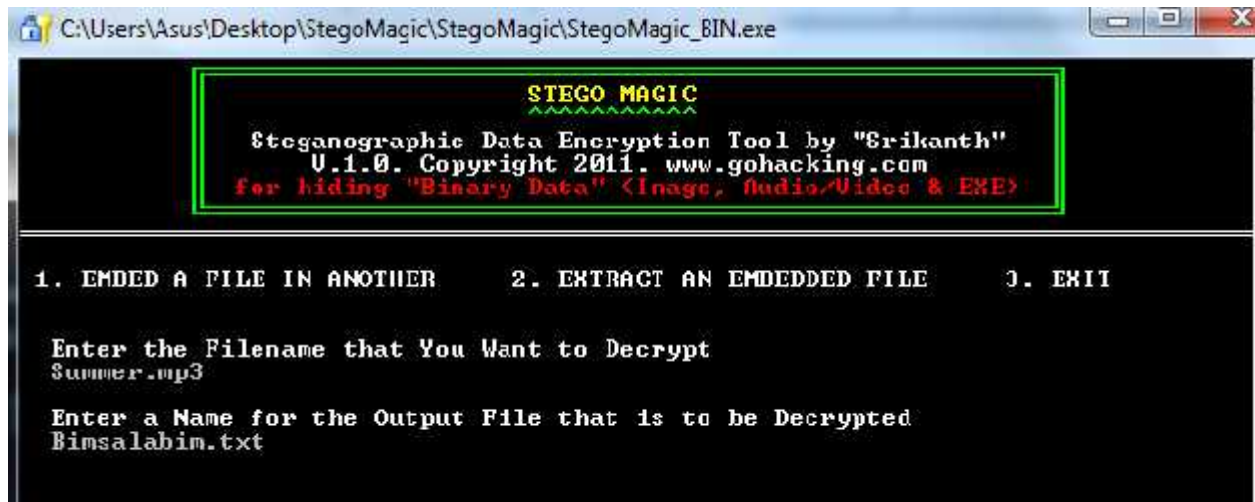


Lalu ketikkan kembali nama file yang digunakan sebagai tempat menyimpan file rahasia lalu enter





Lalu ketikkan nama file rahasia tersebut sesuai keinginan anda disini sana memberi nama Bimsalabin.txt lalu enter



The screenshot shows a Windows application window titled "C:\Users\Asus\Desktop\StegoMagic\StegoMagic\StegoMagic\_BIN.exe". The application has a black background with yellow and red text. At the top, it says "STEGO MAGIC" followed by "Steganographic Data Encryption Tool by 'Srikanth'" and "V.1.0. Copyright 2011. www.gohacking.com for hiding 'Binary Data' (Image, Audio/Video & EXE)". Below this, there are three menu options: "1. EMBED A FILE IN ANOTHER", "2. EXTRACT AN EMBEDDED FILE", and "3. EXIT". The user has entered "Summer.mp3" for the filename to decrypt and "Bimsalabin.txt" for the output file name.

```
C:\Users\Asus\Desktop\StegoMagic\StegoMagic\StegoMagic_BIN.exe


STEGO MAGIC
Steganographic Data Encryption Tool by "Srikanth"
V.1.0. Copyright 2011. www.gohacking.com
for hiding "Binary Data" (Image, Audio/Video & EXE)

1. EMBED A FILE IN ANOTHER    2. EXTRACT AN EMBEDDED FILE    3. EXIT

Enter the Filename that You Want to Decrypt
Summer.mp3

Enter a Name for the Output File that is to be Decrypted
Bimsalabin.txt
```

Selanjutnya ketik Kode secret key yang tadi tersimpan



This screenshot is similar to the previous one, but it shows the next step in the process. The user has entered the secret key "64" for decryption.

```
C:\Users\Asus\Desktop\StegoMagic\StegoMagic\StegoMagic_BIN.exe

STEGO MAGIC
Steganographic Data Encryption Tool by "Srikanth"
V.1.0. Copyright 2011. www.gohacking.com
for hiding "Binary Data" (Image, Audio/Video & EXE)

1. EMBED A FILE IN ANOTHER    2. EXTRACT AN EMBEDDED FILE    3. EXIT

Enter the Filename that You Want to Decrypt
Summer.mp3

Enter a Name for the Output File that is to be Decrypted
Bimsalabin.txt

Enter the Secret Key for Decryption
64
```

File Rahasia yang kita simpan tadi sudah muncul kembali



The final screenshot shows the application displaying a success message: "File Decryption Completed Successfully!" and "Output File is: Bimsalabin.txt". It also prompts the user to "Press Any Key to Continue...".

```
C:\Users\Asus\Desktop\StegoMagic\StegoMagic\StegoMagic_BIN.exe

STEGO MAGIC
Steganographic Data Encryption Tool by "Srikanth"
V.1.0. Copyright 2011. www.gohacking.com
for hiding "Binary Data" (Image, Audio/Video & EXE)

1. EMBED A FILE IN ANOTHER    2. EXTRACT AN EMBEDDED FILE    3. EXIT

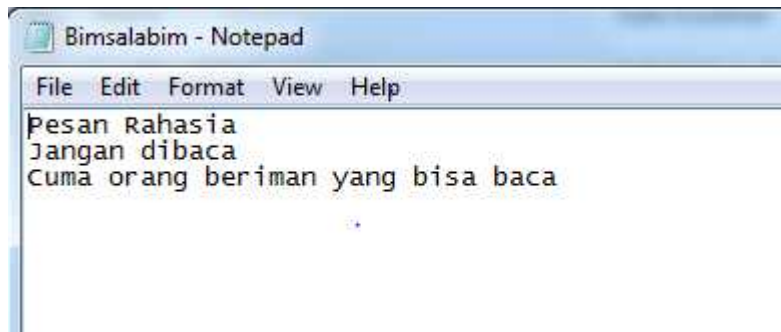
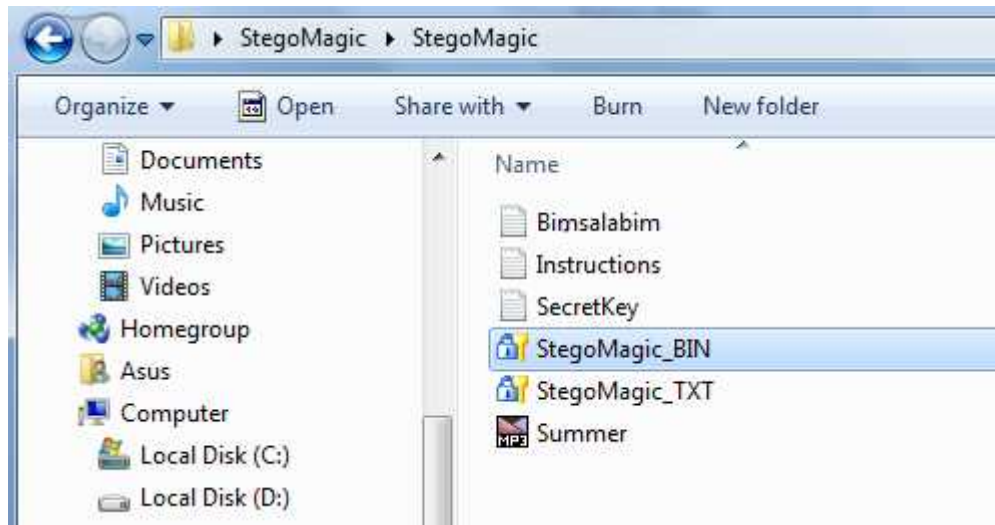
Enter the Filename that You Want to Decrypt
Summer.mp3

Enter a Name for the Output File that is to be Decrypted
Bimsalabin.txt

Enter the Secret Key for Decryption
64

File Decryption Completed Successfully!
Output File is: Bimsalabin.txt

Press Any Key to Continue...
```



**Terima Kasih**