YOGA AULA AGNA CHOIR
1310651057
E

Bab 5 ENKRIPSI : Tujuan Pembelajaran Meliputi, Konsep Kriptografik Cornerstone, Enkripsi Simetris, Enkripsi Asimetris, Fungsi Hash, Serangan Kriptografik dan Implementasi Kriptografi.

Kriptografi Merupakan sebuah Sains dalam Keamanan berkomunikasi, Teknik didalam Kriptografi Dibuat dan ditujukan agar hanya dapat dibaca dan dimengerti oleh penerima yang dituju. Data diubah agar keaslian dan nilai penting dari informasi yang dienkripsi tidak dapat dengan mudah dibaca oleh orang lain. Kriptografi memuat sebuah pesan tersembunyi, dan hanya dapat dipecahkan dengan metode yang disebut Kriptanalisis. Kriptografi terbagi menjadi 4 unsur didalamnya, pertama Cipher, cipher adalah suatu bentuk algoritma yang dihasilkan dari konsep kriptografi. kedua adalah Plaintext, Plaintext adalah Pesan yang masih mentah, dimana pesan tersebut belum diolah dan dirubah ke bentuk cipher dengan kriptografi, ketiga adalah Enkripsi, Enkripsi adalah suatu proses dalam mengubah Plaintext menjadi Cipher, dan yang terakhir Dekripsi, adalah proses mengubah kembali cipher ke bentuk plaintext. Keuntungan dalam menggunakan kriptografi yang pertama, Kerahasiaan, suatu rahasia yang tetap akan terjaga sampai pesan rahasia tersebut sampai ke tangan penerima yang sah, kedua Integritas adalah data tidak mudah dipecahkan oleh pihak yang tidak berkepentingan/ tidak berhak. ketiga adalah autotentikasi, dimana sistem kriptografi dapat mengetes bahwa pesan sudah sampai ke tangan yang berhak atau yang tidak mellalui autotentikasi ini. dan terakhir nonrepudiasi yan membuat bahwa pengguna yang sah menggunakan transaksi yang spesifik dan transaksi tersebut tidak berubah.

Pengertian Jaringan Arsitektur Dan Desain Jaringan komputer adalah interkoneksi dua atau lebih komputer dan perangkat jaringan untuk berkomunikasi satu sama lainnya dengan tujuan agar dapat menggunakan sumberdaya secara bersama sama. Adapun jenis jaringan ada 3 yaitu: LAN adalah jaringan komputer yang jaringannya hanya mencakup wilayah kecil; seperti jaringan komputer kampus, gedung, kantor, dalam rumah, sekolah atau yang lebih kecil. Saat ini, kebanyakan LAN berbasis pada teknologi IEEE 802.3 Ethernet menggunakan perangkat switch, yang mempunyai kecepatan transfer data 10, 100, atau 1000 Mbit/s. Selain teknologi Ethernet, saat ini teknologi 802.11b (atau biasa disebut Wi-fi) juga sering digunakan untuk membentuk LAN. MAN adalah Suatu jaringan dalam suatu kota dengan transfer data berkecepatan tinggi, yang menghubungkan berbagai lokasi seperti kampus, perkantoran, pemerintahan, dan sebagainya. Jaringan MAN adalah gabungan dari beberapa LAN. WAN adalah singkatan dari istilah teknologi informasi dalam bahasa Inggris: Wide Area Network merupakan jaringan komputer yang mencakup area yang besar sebagai contoh yaitu jaringan komputer antar wilayah, kota atau bahkan negara, atau dapat didefinisikan juga sebagai jaringan komputer yang membutuhkan router dan saluran komunikasi publik. 2. OSI LAYER Osi layer adalah suatu dekripsi abstrak mengenai desain lapisan-lapisan komunikasi dan protokol jaringan komputer yg dikembangkan sebagai bagian dari inisiatif open system interconnetion(OSI). Dalam osi layer terdapat tujuh lapisan osi layer yaitu: a. Physical layer b. Data link layer c. Network layer d. Transport layer e. Session layer f. Presentation layer g. Application layer

3. TCP/IP Adalah sebuah perangkat lunak jaringan komputer yang terdapat memungkinkan komputer satu dengan komputer lain dapat mentranfer dan network. Dalam TCP/IP ada 4 layer yaitu: a.application b. host-to-host transport c. internet d.network access

4. MAC Address adalah sebuah alamat jaringan yang diimplementasikan pada lapisan data-link dalam tujuh lapisan model OSI, yang merepresentasikan sebuah node tertentu dalam jaringan. Dalam sebuah jaringan berbasis Ethernet.

5. DNS (Domain Name System) adalah sebuah sistem yang menyimpan informasi tentang nama host maupun nama domain dalam bentuk basis data tersebar (distributed database) di dalam jaringan komputer, misalkan: Internet.

DNS menyediakan alamat IP untuk setiap nama host dan mendata setiap server transmisi surat (mail exchange server) yang menerima surat elektronik (email) untuk setiap domain.DNS adalah (Domain Name System) yang juga memiliki arti untuk mengidentifikasi setiap komputer sebagai titik dalam suatu jaringan Internet yang menggunakan bantuan sistem protokol internet adress untuk menerjemahkan dari suatu nama domain ke IP dan begitu juga sebaliknya.

6. Internet Control Message Protocol (ICMP)

adalah salah satu protokol inti dari keluarga. ICMP berbeda tujuan dengan TCP dan UDP dalam hal ICMP tidak digunakan secara langsung oleh aplikasi jaringan milik pengguna. salah satu pengecualian adalah aplikasi ping yang mengirim pesan ICMP Echo Request (dan menerima Echo Reply) untuk menentukan apakah komputer tujuan dapat dijangkau dan berapa lama paket yang dikirimkan dibalas oleh komputer tujuan. protokol internet. ICMP utamanya digunakan oleh sistem operasi komputer jaringan untuk mengirim pesan kesalahan yang menyatakan, sebagai contoh, bahwa komputer tujuan tidak bisa dijangkau.

7. HTTP dan HTTPS Http adalah suatu protocol yang digunakan oleh WWW(world Wide Web).http mendefinisikan bagaimana suatu pesan bisa diformat dan dikirimkan dari server ke client. Dan Https adalah versi aman dari http, menyediakan autentikasi dan komunikasi tersandi dan pengguanaan dalam komersi elektrik. 8. TELNET Adalah sebuah protokol jaringan yang digunakan di koneksi Internet atau Local Area Network. TELNET dikembangkan pada 1969 dan distandarisasi sebagai IETF STD 8, salah satu standar Internet pertama. 9. Bridge Bridge bisa menghubungkan tipe jaringan berbeda (seperti Ethernet dan Fast Ethernet) atau tipe jaringan yang sama. Bridge memetakan alamat Ethernet dari setiap node yang ada pada masing-masing segmen jaringan dan memperbolehkan hanya lalu lintas data yang diperlukan melintasi bridge. Ketika menerima sebuah paket, bridge menentukan segmen tujuan dan sumber. Jika segmennya sama, paket akan ditolak; jika segmennya berbeda, paket diteruskan ke segmen tujuannya. Bridge juga bisa mencegah pesan rusak untuk tak menyebar keluar dari satu segmen.

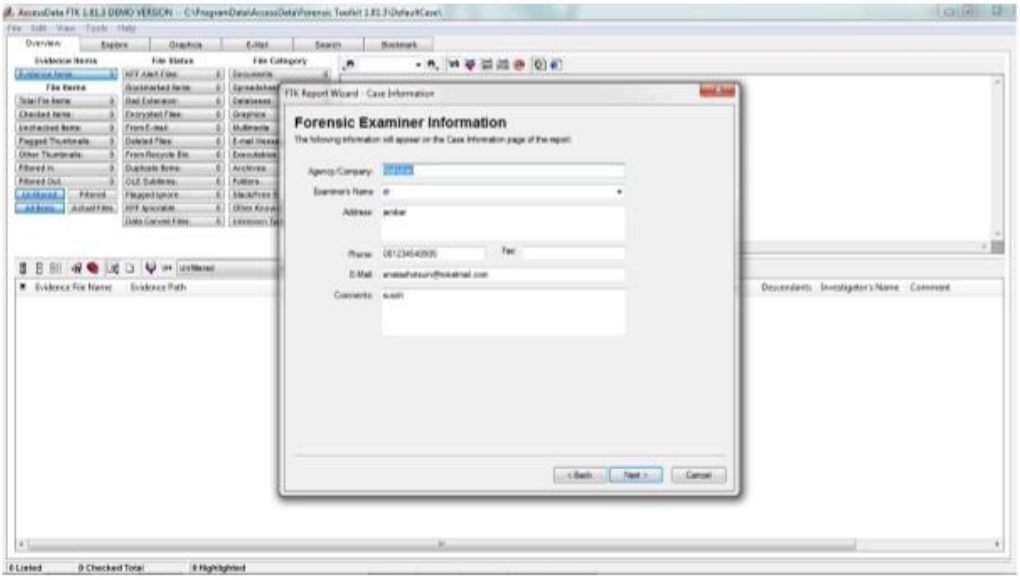
10. Switch yang dimaksud di sini adalah LAN switch. Switch adalah perluasan dari konsep bridge. Ada dua arsitektur dasar yang digunakan pada switch, yaitu • cut-through • store-and-forward. Switch cut-through memiliki kelebihan di sisi kecepatan karena ketika sebuah paket datang, switch hanya memperhatikan alamat tujuannya sebelum meneruskan ke segmen tujuan. Switch store-and-forward, kebalikannya, menerima dan menganalisa seluruh isi paket sebelum meneruskannya ke tujuan. Waktu yang diperlukan untuk memeriksa satu paket memakan waktu, tetapi ini memungkinkan switch untuk mengetahui adanya kerusakan pada paket dan mencegahnya agar tak mengganggu jaringan. Dengan teknologi terbaru, kecepatan switch store-and-forward ditingkatkan sehingga mendekati kecepatan switch cut-through. Di pasaran Anda juga bisa memilih switch hibrid yang menggabungkan arsitektur cut-through dan store-and- forward. Dengan switch, Anda

mendapatkan keuntungan karena setiap segmen jaringan memiliki bandwidth 10Mbps penuh, tidak terbagi seperti pada “shared network.” Dengan demikian kecepatan transfer data lebih tinggi. Jaringan yang dibentuk dari sejumlah switch yang saling terhubung disebut “collapsed backbone.” Saat ini banyak orang memilih menggunakan jaringan Ethernet 10Mbps pada segmen-segmennya dan Fast Ethernet 100Mbps pada koneksi ke server. Untuk keperluan ini digunakan switch 10/100 yang biasanya memiliki beberapa (4-24) port 10Mbps untuk koneksi ke komputer klien dan 1 port 100Mbps ke komputer server. Product sejenis ini adalah: • 3com superstack, corebuilder • cisco catalyst • dlink

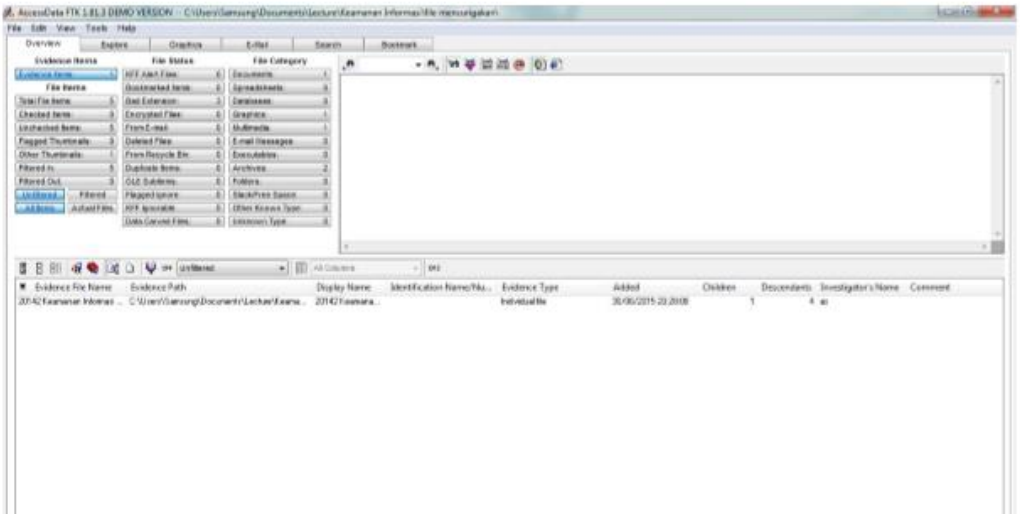
Metode pengamanan yang dihasilkan kriptografi adalah Subtitusi dan Permutasi, Subtitusi adalah kemampuan mengubah karakter satu dengan yang lainnya yang dapat membuat seseorang yang tidak berhak kebingungan. Permutasi atau biasa disebut transpisisi adalah fungsi untuk mengacak bentuk kata yang terkandung dalam pesan menjadi bentuk yang tidak karuan/ acak. bahkan tak jarang kedua metode tersebut digabungkan.

Kekuatan Kriptografi : Enkripsi yang baik haruslah kuat, untuk enkripsi berbasis kunci harus dibuat sesulit mungkin dan idealnya adalah tidak mungkin dipecahkan untuk mengubah ciphertext kembali ke bentuk plaintext tanpa adanya kunci. Sebaliknya, kerahasiaan dalam kriptografi algoritma terbukti tidak memberikan kekuatan, faktanya kriptografi algoritma selalu terbukti lemah.

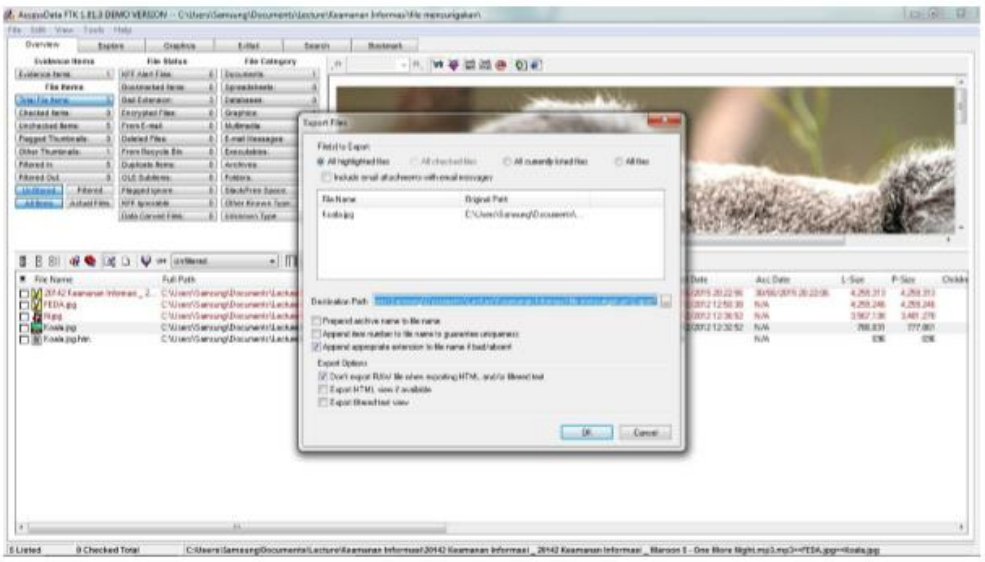
2. Pertama saya akan mengambil file mencurigakan yaitu file maroon five - one more night sekilas terlihat seperti file mp3 biasa namun didalamnya terdapat file lain, saya akan ungkap salah satunya.



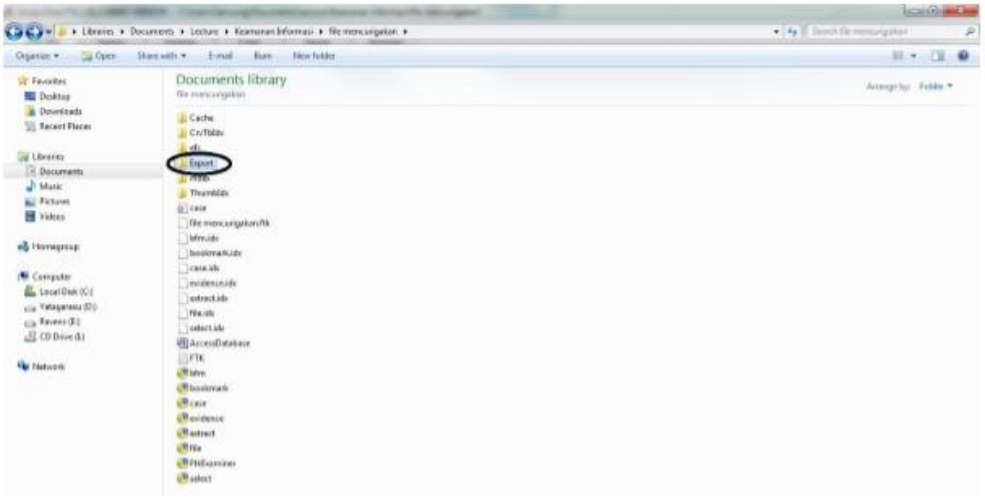
Saya menggunakan FTK toolkit, langsung saja, untuk dapat membuka sebuah case maka anda harus memiliki file berkas yang digunakan untuk menyimpan berkas dari file yang akan anda ungkap. langsung pilih File lalu pilih new case, anda akan diminta mengisi beberapa kolom termasuk identitas anda. seperti diatas.

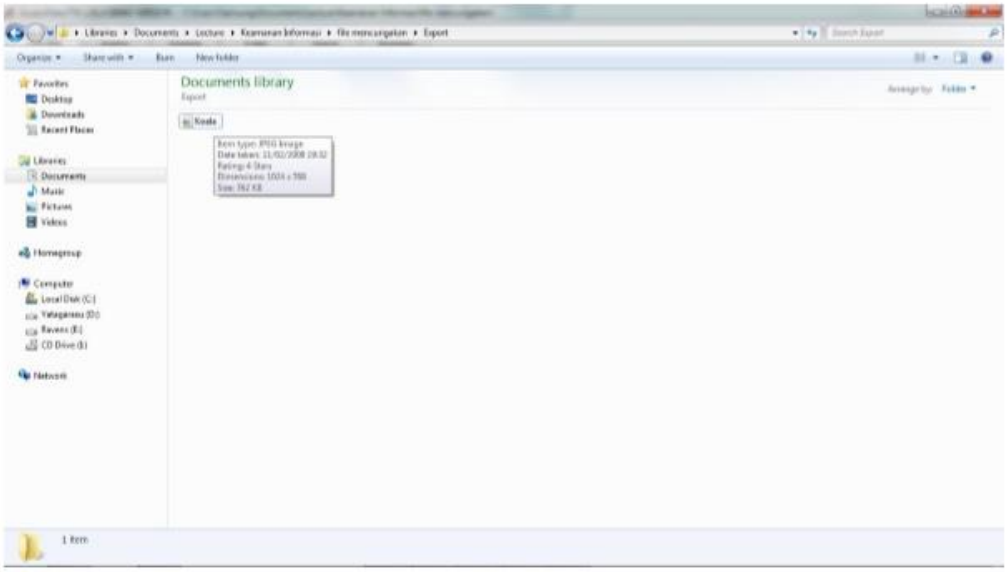


Apabila folder anda sudah terbuat, maka langsung pilih file > add evidence lalu pilih dan isikan kembali identitas penyidik anda.lalu pilih menu add evidence > individual file maka tampilan diatas akan terbuka.



Setelah itu klik menu total file item disamping dan akan muncul kelima file tersembunyi seperti diatas, langsung saja klik kanan koala dan centang menu diatas. dan file akan diexport pada folder yang anda buat tadi.





Terdapat 1 file yang telah diexport seperti diatas, ingat cara expor ini berhasil pada file2 tertentu saja seperti jpg notepad dll, untuk cara lainnya harus menggunakan pilihan cntang berbeda. segera klik dan hasil yang akan keluar adalah...