UAS KEAMANAN INFORMASI

Disusun oleh:

(MUHAMMAD MUSYAFA)

(1310651220)

(KELAS:A)

PROGRAM STUDI TEKNIK INFORMATIKA

FAKULTAS TEKNIK

UNIVERSITAS MUHAMMADIYAH JEMBER

2015

KRIPTOGRAFI

Kriptografi adalah menulis rahasia komunikasi yang aman yang bisa dipahami oleh penerima yang telah ditentukan oleh pengirim pesan tersebut. Tujuan dari kriptografi tersebut adalah mengamankan informasi yang dikirim agar pesan tersebut tidak diketahui oleh pihak ketiga.

Kriptografi menciptakan pesan makna yang tersembunyi. Kriptanalisis adalah ilmu membobol terenkripsi pesan bijak.Kriptologi meliputi kriptografi dan pembacaan sandi.

Manfaat kriptografi adalah untuk memberikan kerahasiaan dan integritas yang bermaksud agar data tidak diubah dengan cara yang tidak sah atau tanpa seijin pemilik data tersebut yang mengakibatkan kerugian bagu sipemilik data tersebut. Kroptografi juga dapat memberikan otentifikasi atau membuktikan klaim identifikasi. Kriptografi juga memberikan nonrepudation yaitu jaminan bagi pengguna tertentu yang melakukan transaksi tertentu dan transaksi tersebut tidak bisa diubah dengan cara yang tidak sah atau tidak melalui prosedur yang benar atau yang ditentukan.

Enkripsi yang kuat menghancurkan pola. Jika satu bit perubahan plaintext, kemungkinan setiap sedikit menghasilkan ciphertext perubahan harus 50/50. Tanda-tanda nonrandomness dapat digunakan sebagai petunjuk untuk cryptanalyst sebuah, mengisyaratkan pada urutan yang mendasari asli plaintext atau kunci.

Enkripsi yang baik adalah yang kuat, maksudnya adalah kesulitan untuk mengkonversi ciphertext kembali ke plaintext tanpa kunci. Kerahasiaan algoritma kriptografi tidak memberikan kekuatan , akan tetapi kripto yang kuat bergantung pada matematika. Chiper yang telah teruji adalah algoritma umum, seperti Triple Data Encryption Standard dan Advanced Encryption Standard.

Ada dua macam chiper yaitu monoalphabetic yaitu menggunakan satu huruf, contohnya menggunakan huruf “E” diganti dengan huruf “X”. Polyalphabetic menggunakan beberapa huruf dan model ini sangat sulit untuk dipecahkan.

Ada tiga jenis utama dari enkripsi yang modern yaitu simetris , asimetris , dan hashing. Enkripsi simetris menggunakan satu kunci, sedangkan enkripsi asimetris menggunakan dua kunci , sedangkan hashing adalah transformasi kriptografi satu arah menggunakan algoritma.

Enkripsi simetris mungkin memiliki aliran dan blok mode. Modus aliran berarti setiap bit secara independen dienkripsi dalam "aliran." mode Block cipher mengenkripsi blok Data setiap putaran yaitu 56 bit untuk Data Encryption Standard (DES) dan 128, 192, atau 256 bit AES untuk, misalnya. Beberapa cipher blok dapat meniru stream cipher oleh pengaturan ukuran blok 1 bit, mereka masih dianggap cipher blok.

Vektor inisialisasi digunakan dalam beberapa cipher simetrik untuk memastikan bahwa pertama

blok dienkripsi data acak. Hal ini memastikan bahwa plaintext yang identik mengenkripsi untuk ciphertexts berbeda.

Kode Buku Elektronik (ECB) adalah bentuk yang paling sederhana dan paling lemah dari DES. Kode ini tidak mengguanakan inisialisasi vektor atau chaining. Mode ini mengenkripsi ke chiphertexts.

Cipher Block Chaining (CBC) Mode adalah mode blok DES yang XORs sebelumnya blok dienkripsi dari ciphertext ke blok berikutnya plaintext yang akan dienkripsi. Keterbatasan mode ini jika terdapat kesalahan akan menghancurkan integritas semuanya.

Cipher Feedback (CFB) mode sangat mirip dengan CBC, perbedaan utama adalah CFB adalah modus aliran. Mode ini menggunakan umpan balik untuk menghancurkan pola.

Output Feedback (OFB) modus berbeda dari CFB dengan cara umpan balik menemani plished. CFB menggunakan ciphertext sebelumnya untuk umpan balik.

Singgle DES adalah implementasi asli DES, enkripsi 64 bit blok data dengan kunci 56 bit, menggunakan 16 putaran enkripsi.

Triple DES berlaku enkriksi tunggal DES tiga kali blok disebut juga dengan Algoritma Triple Data Encryption.

Blowfish menggunakan 32 melalui 448 bit kunci untuk mengenkripsi 64 bit data. Twofish merupakan finalis AES, enkripsi Blok 128 bit menggunakan 128 melalui tombol 256 bit. Keduanya algoritma terbuka, unpatented, dan tersedia secara bebas.

RC5 menggunakan 32 (pengujian tujuan), 64 (pengganti DES), atau 128 bit blok. Rentang ukuran kunci 0-2040 bit.

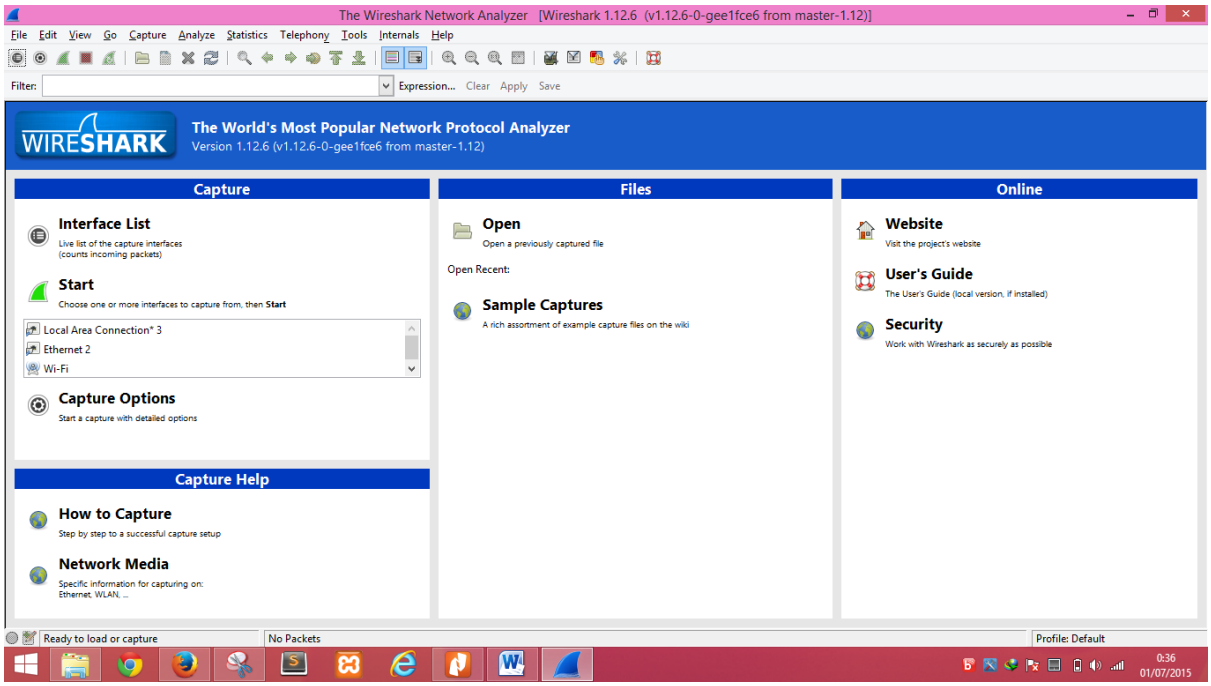
RC6 didasarkan pada RC5, diubah untuk memenuhi persyaratan AES. RC6 lebih kuat dari RC5 karena enkripsi 128, 192, 256 bit blok.

Fungsi hash memberikan enkripsi menggunakan algoritma dan tidak ada tombol. Fungsi utama hash digunakan untuk menyediakan integritas, jika hash dari perubahan plaintext, plaintext sendiri telah berubah.

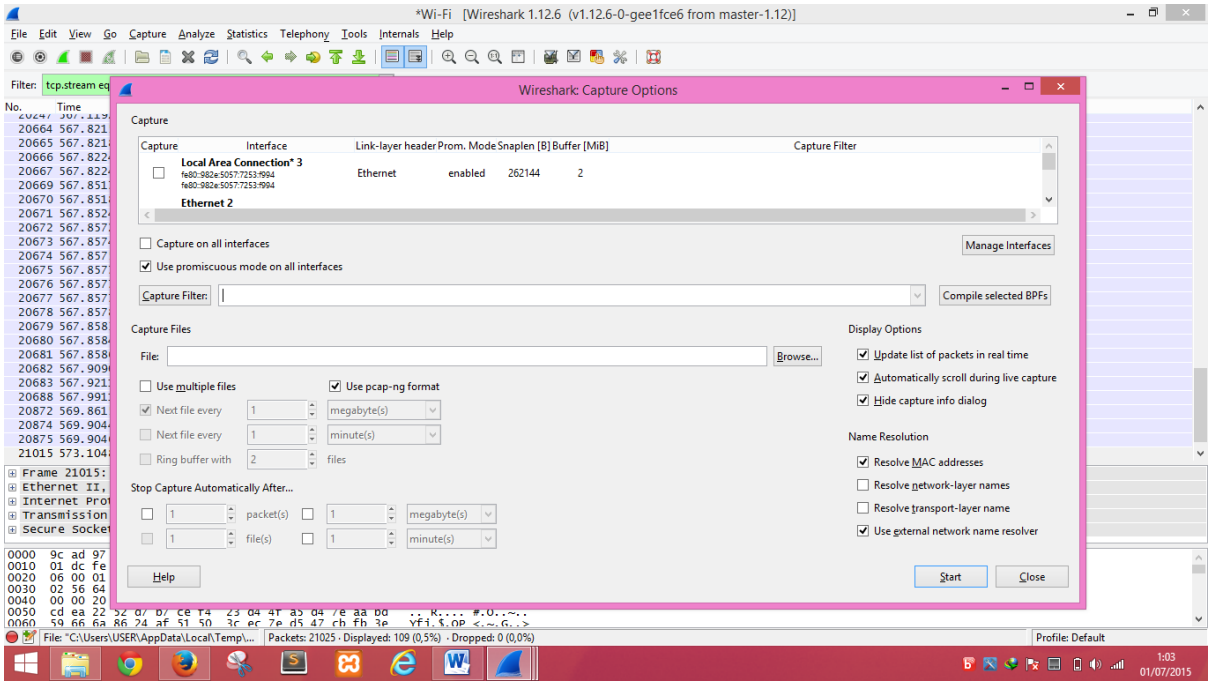
MD5 adalah algoritma Message Digest 5. MD5 memiliki nilai hash 128 bit pada setiap panjang input. Kelemahan MD5 adalah dimana tabrakan dapat ditemukan dalam jumlah yang besar.

Secure Hash Algorithm adalah nama dari serangkaian algoritma hash. SHA 1 memiliki nilai hash 160 bit.

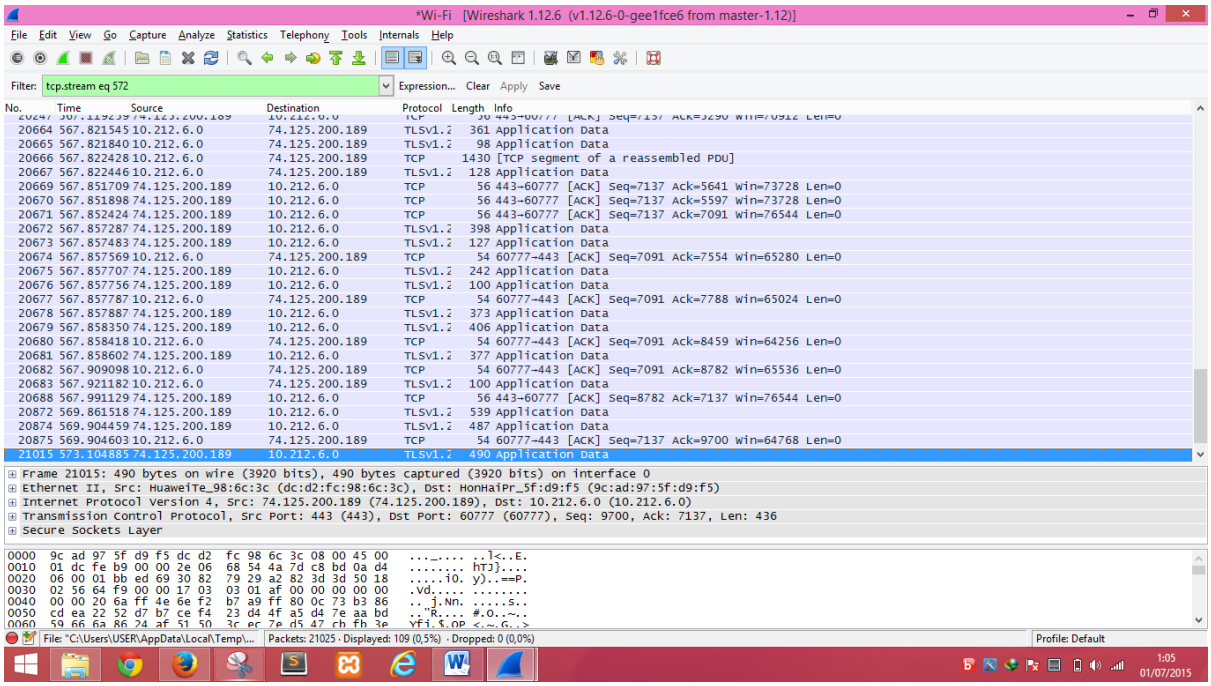
Buka wireshark terlebih dahulu



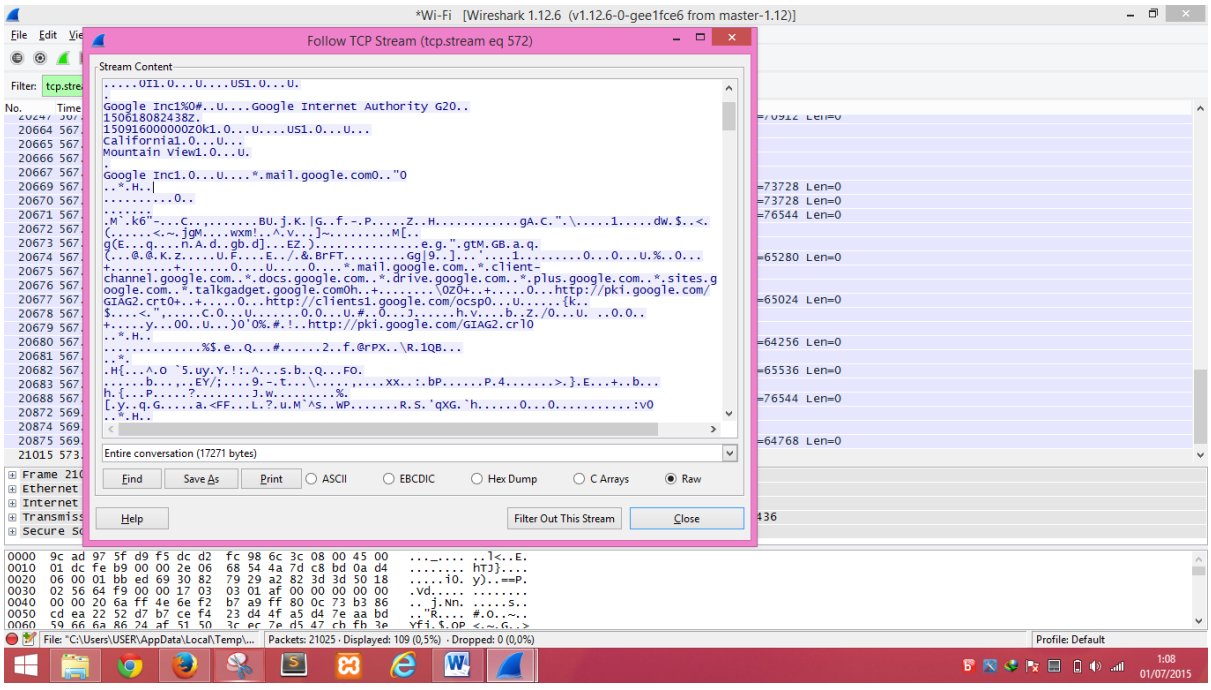
Pada tool capture pilih option, terus pilih interface yang ingin anda capture dan klik start



Maka akan muncul gambar seperti berikut



Setelah itu klik tombol stop, dan pilih salah satu untuk anda analisis data yang masuk dijaringan anda dan klik kanan dan pilih follow tcp stream



Dan selamat anda bisa menganalisis data yang masuk dan keluar di jaringan anda.