Nama : Zulfy Ainur Rohman

Nim : 1310651013

Kelas : A

**Soal nomer 1**

*Cryptography*

*Cryptography* berasal dari kata *crypto* yang berarti ”*hidden, secret*” dan pada bidang studi informatika dapat diartikan dengan studi mengenai menyembunyikan informasi atau informasi yang disembunyikan (*hiding information*). Pada saat ini, ilmu ini berkembang dan dapat dikategorikan menjadi tiga kelompok utama, yaitu:

1. Penggunaan operasi matematika yang mengubah *plaintext* (sumber informasi atau informasi aslinya) ke dalam bentuk ciphertext (informasi yang sudah dikodekan) menggunakan kunci enkripsi.

2. Apakah dibentuk sebuah block atau sebuahstream cipher.

3. Penggunaan satu atau dua kunci sistem.

Tujuan kriptografi: 1. *Deter* (menghalangi)

2. *Prevent* (mencegah)

3. *Detect* (menemukan)

4. *Correct* (membetulkan)

atas pelanggaran keamanan, termasuk pada saat melakukan pengiriman (*transmission*) informasi.

* Kriptografi dapat memenuhi kebutuhan umum suatu transaksi:
  + Kerahasiaan (confidentiality) dijamin dengan melakukan enkripsi (penyandian).
  + Keutuhan (integrity) atas data‐data pembayaran dilakukan dengan fungsi hash satu arah.
  + Jaminan atas identitas dan keabsahan (authenticity) pihak‐pihak yang melakukan transaksi dilakukan dengan menggunakan password atau sertifikat digital. Sedangkan keotentikan data transaksi dapat dilakukan dengan tanda tangan digital.
  + Transaksi dapat dijadikan barang bukti yang tidak bisa disangkal (non‐repudiation) dengan memanfaatkan tanda tangan digital dan sertifikat digital
* Karakteristik cryptosytem yang baik sebagai berikut :
  + Keamanan sistem terletak pada kerahasiaan kunci dan bukan pada kerahasiaan algoritma yang digunakan.
  + Cryptosystem yang baik memiliki ruang kunci (keyspace) yang besar.
  + Cryptosystem yang baik akan menghasilkan ciphertext yang terlihat acak dalam seluruh tes statistik yang dilakukan terhadapnya.
  + Cryptosystem yang baik mampu menahan seluruh serangan yang telah dikenal sebelumnya
* Macam Cryptosytem
  + Symmetric Cryptosystem    
    Dalam symmetric cryptosystem ini, kunci yang digunakan untuk proses enkripsi dan dekripsi pada prinsipnya identik, tetapi satu buah kunci dapat pula diturunkan dari kunci yang lainnya.
  + Assymmetric Cryptosystem    
    Dalam assymmetric cryptosystem ini digunakan dua buah kunci. Satu kunci yang disebut kunci publik (public key) dapat dipublikasikan, sedang kunci yang lain yang disebut kunci privat (private key) harus dirahasiakan. Proses menggunakan sistem ini dapat diterangkan secara sederhana sebagai berikut : bila A ingin mengirimkan pesan kepada B, A dapat menyandikan pesannya dengan menggunakan kunci publik B, dan bila B ingin membaca surat tersebut, ia perlu mendekripsikan surat itu dengan kunci privatnya. Dengan demikian kedua belah pihak dapat menjamin asal surat serta keaslian surat tersebut, karena adanya mekanisme ini. Contoh : sistem ini antara lain RSA Scheme dan Merkle‐Hellman Scheme.
* Protokol Cryptosystem   
    
  Cryptographic protocol adalah suatu protokol yang menggunakan kriptografi. Protokol ini melibatkansejumlah algoritma kriptografi, namun secara umum tujuan protokol lebih dari sekedar kerahasiaan.Pihak‐pihak yang berpartisipasi mungkin saja ingin membagi sebagian rahasianya untuk menghitungsebuah nilai, menghasilkan urutan random, atau pun menandatangani kontrak secara bersamaan.   
  Penggunaan kriptografi dalam sebuah protokol terutama ditujukan untuk mencegah atau pun mendeteksi adanya eavesdropping dan cheating.
* Jenis Penyerangan Pada Protokol
  + Ciphertext‐only attack. Dalam penyerangan ini, seorang cryptanalyst memiliki ciphertext dari sejumlah pesan yang seluruhnya telah dienkripsi menggunakan algoritma yang sama.
  + Known‐plaintext attack. Dalam tipe penyerangan ini, cryptanalyst memiliki akses tidak hanya ke ciphertext sejumlah pesan, namun ia juga memiliki plaintext pesan‐pesan tersebut.
  + Chosen‐plaintext attack. Pada penyerangan ini, cryptanalyst tidak hanya memiliki akses atas ciphertext dan plaintext untuk beberapa pesan, tetapi ia juga dapat memilih plaintext yang dienkripsi.
  + Adaptive‐chosen‐plaintext attack. Penyerangan tipe ini merupakan suatu kasus khusus chosen‐plaintext attack. Cryptanalyst tidak hanya dapat memilih plaintext yang dienkripsi, ia pun memiliki kemampuan untuk memodifikasi pilihan berdasarkan hasil enkripsi sebelumnya. Dalam chosen‐plaintext attack, cryptanalyst mungkin hanya dapat memiliki plaintext dalam suatu blok besar untuk dienkripsi; dalam adaptive‐chosen‐plaintext attack ini ia dapat memilih blok plaintext yang lebih kecil dan kemudian memilih yang lain berdasarkan hasil yang pertama, prosesini dapat dilakukannya terus menerus hingga ia dapat memperoleh seluruh informasi.
  + Chosen‐ciphertext attack. Pada tipe ini, cryptanalyst dapat memilih ciphertext yang berbeda untuk didekripsi dan memiliki akses atas plaintext yang didekripsi.
  + Chosen‐key attack. Cryptanalyst pada tipe penyerangan ini memiliki pengetahuan tentang hubungan antara kunci‐kunci yang berbeda.
  + Rubber‐hose cryptanalysis. Pada tipe penyerangan ini, cryptanalyst mengancam, memeras, atau bahkan memaksa seseorang hingga mereka memberikan kuncinya.

6. Jenis Penyerangan Pada Jalur Komunikasi.

* Sniffing: secara harafiah berarti mengendus, tentunya dalam hal ini yang diendus adalah pesan (baik yang belum ataupun sudah dienkripsi) dalam suatu saluran komunikasi. Hal ini umum terjadi pada saluran publik yang tidak aman. Sang pengendus dapat merekam pembicaraan yang terjadi.
* Replay attack [DHMM 96]: Jika seseorang bisa merekam pesan‐pesan handshake (persiapan komunikasi), ia mungkin dapat mengulang pesan‐pesan yang telah direkamnya untuk menipu salah satu pihak.
* Spoofing [DHMM 96]: Penyerang – misalnya Maman – bisa menyamar menjadi Anto. Semua orang dibuat percaya bahwa Maman adalah Anto. Penyerang berusaha meyakinkan pihak‐pihak lain bahwa tak ada salah dengan komunikasi yang dilakukan, padahal komunikasi itu dilakukan dengan sang penipu/penyerang. Contohnya jika orang memasukkan PIN ke dalam mesin ATM palsu – yang benar‐benar dibuat seperti ATM asli – tentu sang penipu bisa mendapatkan PIN‐nya dan copy pita magentik kartu ATM milik sang nasabah. Pihak bank tidak tahu bahwa telah terjadi kejahatan.
* Man‐in‐the‐middle [Schn 96]: Jika spoofing terkadang hanya menipu satu pihak, makadalam skenario ini, saat Anto hendak berkomunikasi dengan Badu, Maman di mata Anto seolah‐olah adalah Badu, dan Maman dapat pula menipu Badu sehingga Maman seolah‐olah adalah Anto. Maman dapat berkuasa penuh atas jalur komunikas ini, dan bisa membuat berita fitnah.

**Soal Nomer 2**

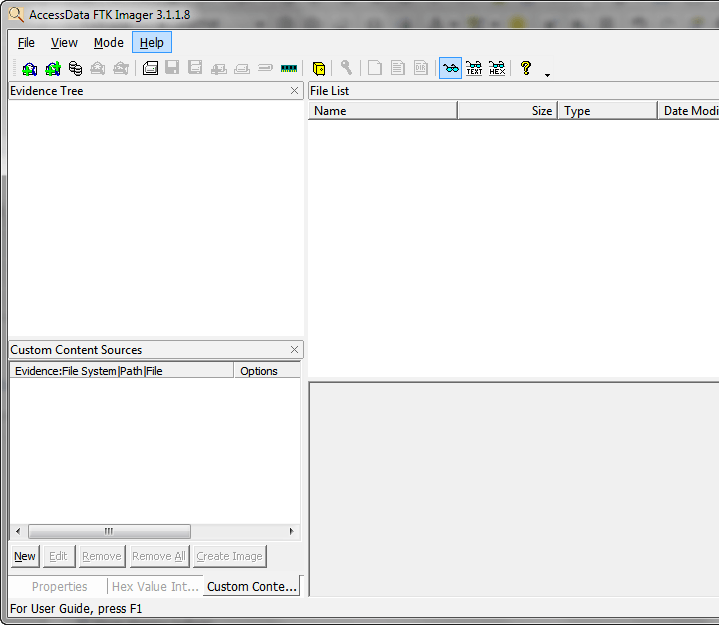
# Menggunakan FTK Imager untuk menjamin keaslian Data Elektronik

Data elektronik yang kita peroleh dari WP harus dijamin keasliannya, dengan kata lain tidak boleh diubah satu byte-pun agar hasil analisa kita bisa diyakini kebanarannya karena sesuai dengan pepatah “Garbage In Garbage out” maka jika inputnya salah maka apapun hasilnya pasti juga dianggap salah

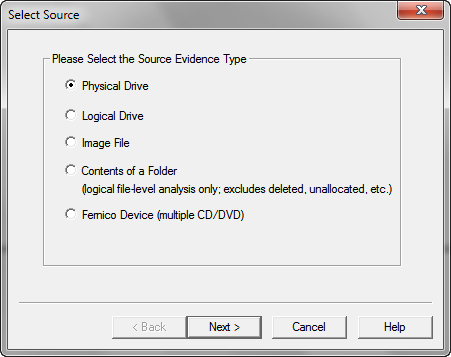
Oleh karena itu ada beberapa cara yang bisa kita lakukan untuk menjamin keaslian data tersebut :

1. Kita pastikan bahwa data diberikan dalam bentuk yang **Read Only,**seperti dalam media CR-ROM yang hanya bisa ditulis sekali
2. Kita lakukan Cloning atas data tersebut sehingga kita memiliki salinannya baik dalam bentuk pisik ataupun image file
3. Kita Buat file list yang berisi daftar semua file dalam CD\_ROM tersebut
4. Kita buat Hash value untuk CD tersebut untuk menjamin bahwa datanya adalah identik/ sama dengan aslinya, karena jika satu bytepun dari file2 tersebut diubah maka nilai hash valuenya pun berubah

# Tampilan aplikasinya



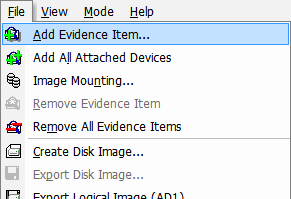
Untuk membuat Hash value maupun direktory listing kita bisa lakukan dengan membuat Image dari CDRom tersebut. FTK imager mengenal beberapa sumber dari Image yaitu :



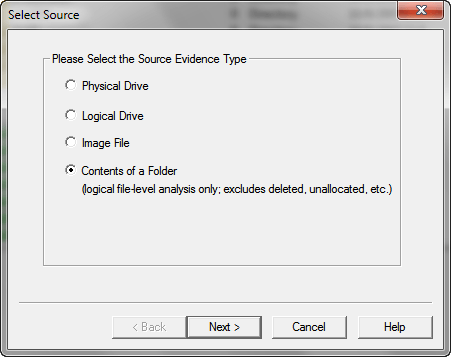
1. Physical Drive, biasanya berupa harddisk atau flash disk, disini kita bicara mengenai drive secara fisik, jadi kalau kapasitas ada 500 gb maka image kita juga akan memiliki size sebesar 500 gb (kecuali kita compress), jadi kita akan mengclone harddisk secara fisik , tidak perduli apakah ada isinya atau tidak. Ini biasanya untuk melihat apakah ada file2 yang didelete
2. Logical Drive, berupa drive di computer, yaitu biasanya A:, C:, D:, dst.  Bisa saja satu harddisk dibagi/ dipartisi menjadi 2 atau lebih logical Drive, misalnya C: untuk system dan D: untuk data. Kalau kita membuat Image dari Logical drive berarti satu drive utuh termasuk bagian yang kosong/tidak ada datanya
3. Image file, ini merupakan cloning dari suatu drive/folder/CDROM yang berupa suatu file dengan ekstensiaon ISO, VC4, dll tergantung softwarenya. Image berguna juga sebagai backup dari aslinya dan bisa disimpan dalam hardisk kita sehingga kita tidak perlu mencari2 di tumpukan CDROM kita misalnya. Image file biasanya hanya mengambil bagian drive/CDROM yang ada datanya saja untuk menghemat tempat
4. Contents of A folder, berupa folder dan isinya termasuk sub folder, kalau kita mau mengambil datanya saja dari suatu drive/CDROM/Flashdisk maka kita gunakan ini karena lebih menghemat tempat
5. Fernico Device (Multiple CD), ini berupa alat untuk mengcloning banyak CD, tidak kita perdalam disini

Misalnya kita menerima data berupa CDROM maka langkah2nya adalah sbb:

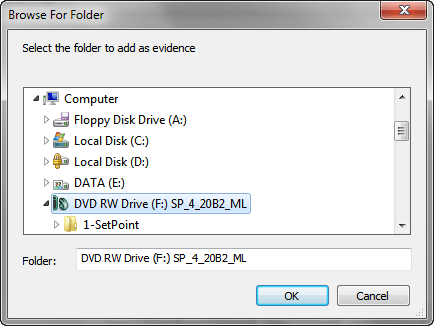
* Kita backup/cloning dulu secara fisik CDROM tadi menjadi 2 atau lebih Copy (bisa dengan Nero atau software burning lainnya)
* Kita Add Evidence ke FTK Imager

[](http://i0.wp.com/eoditor.com/wp-content/uploads/2012/11/FTKImager04.png)

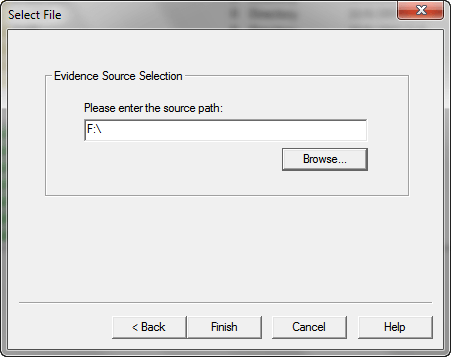
* Kita isi dengan Contents of a folder

[](http://i0.wp.com/eoditor.com/wp-content/uploads/2012/11/FTKImager02.png)

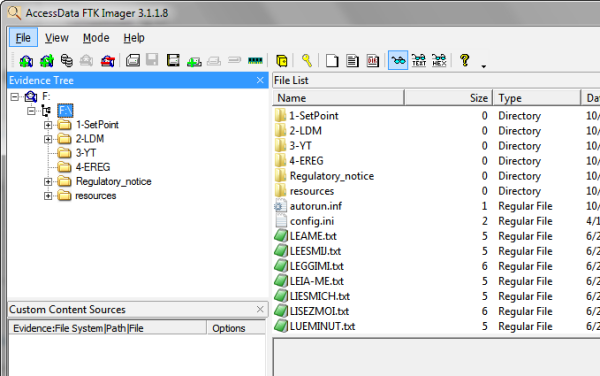
* Kita Next lalu Browse CD-ROM kita

[](http://i0.wp.com/eoditor.com/wp-content/uploads/2012/11/FTKImager05.png)

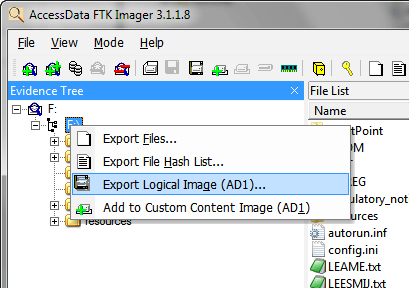
* Lalu Klik Finish

[](http://i2.wp.com/eoditor.com/wp-content/uploads/2012/11/FTKImager05a.png)

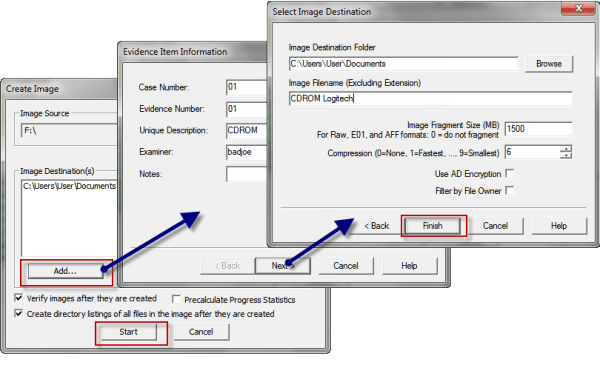
* Ini hasilnya di FTK Imager

[](http://i0.wp.com/eoditor.com/wp-content/uploads/2012/11/FTKImager06.png)

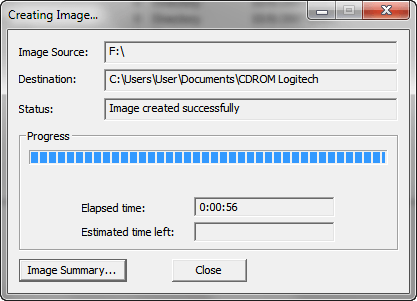
* Untuk membuat Imagenya Kita Klik kanan di F:, lalu pilih Export Logical Image

[](http://i0.wp.com/eoditor.com/wp-content/uploads/2012/11/FTKImager07.png)

* akan muncul windows baru, klik **add,** isi data evidence, next lalu isi  nama file imagenya, lalu finish
* Klik start untuk memulai Image, ini perlu waktu tergantung besarnya data dan compresi yang digunakan
* Untuk keamanan bisa juga diencrypt

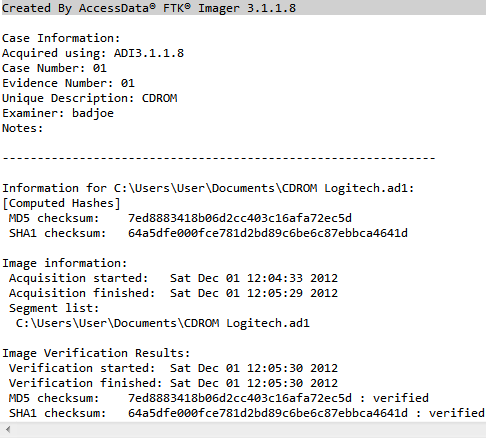
**[](http://i0.wp.com/eoditor.com/wp-content/uploads/2012/11/FTKImager08.png)**

* Ini jika sudah selesai

[](http://i0.wp.com/eoditor.com/wp-content/uploads/2012/11/FTKImager09.png)

FTK Imager akan menciptakan 3 file yaitu Image file (\*.ad1) , file listing file (\*.csv) dan Summary file (\*. txt)

* ini adalah file summary yang berisi hash valuenya dan dinyatakan identik dengan aslinya

[](http://i0.wp.com/eoditor.com/wp-content/uploads/2012/11/FTKImager11.png)

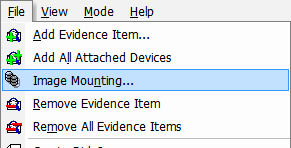
file listing dan file summary yang kita dan WP tandatangani bisa kita lampirkan sebagai KKP

## Mounting File Image

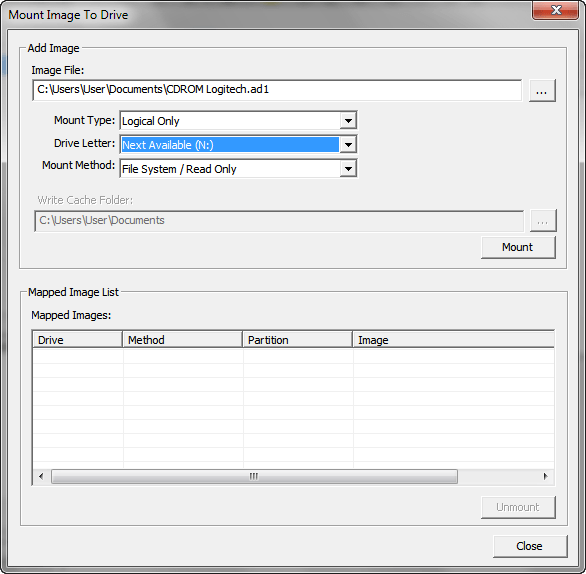
File image berupa satu file dng extension ad1, agar bisa dilihat isinya maka harus kita mounting atau taruh disuatu drive agar terlihat semua isinya. ini berguna karena kita lebih aman bekerja dengan file cloning/imagenya saja, sementara CDROM aslinya bisa kita safe ditempat yang aman

Langkah-2 nya :

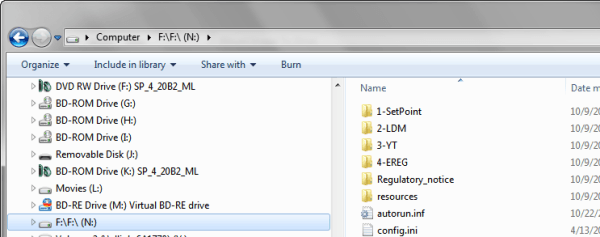
* Klik File –> Image Mounting

[](http://i0.wp.com/eoditor.com/wp-content/uploads/2012/11/FTKImager12.png)

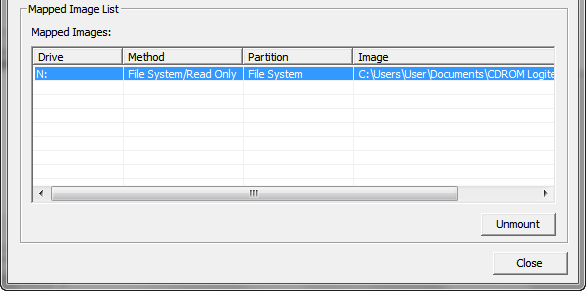
* pilih filenya

[](http://i0.wp.com/eoditor.com/wp-content/uploads/2012/11/FTKImager13.png)

* Klik Mount, ini hasilnya

[](http://i2.wp.com/eoditor.com/wp-content/uploads/2012/11/FTKImager14.png)

* Untuk meng-unmount kita klik lagi image mounting , pilih drive N, lalu klik Unmounth

[](http://i1.wp.com/eoditor.com/wp-content/uploads/2012/11/FTKImager15.png)