UAS

KEAMANAN INFORMASI

Disusun oleh:

PRASETYA BHAKTI NUSA

1310651002

JURUSAN TEKNIK INFORMATIKA

FAKULTAS TEKNIK

UNIVERSITAS MUHAMMADIYAH JEMBER

2015

ACCESS CONTROL

Integrity

Integritas berusaha untuk mencegah modifikasi yang tidak sah dari informasi. Dengan kata lain, integritas berusaha untuk mencegah akses tulis tidak sah ke data

Availability

Ketersediaan memastikan bahwa informasi yang tersedia bila diperlukan. Sistem harus dapat digunakan (tersedia) untuk penggunaan bisnis normal. Contoh dari serangan terhadap ketersediaan akan menjadi Denial-of-Service (DoS) serangan, yang berusaha untuk menolak layanan (atau availabil-.ity) dari sistem.

Disclosure, alteration, and destruction

CIA triad juga dapat dijelaskan oleh kebalikannya: Pengungkapan, Perubahan, dan. Destruction (DAD). Pengungkapan adalah pengungkapan yang tidak sah informasi; alter- asi adalah modifikasi yang tidak sah dari data, dan kehancuran yang membuat sistem. tidak tersedia. Sementara singkatan CIA kadang-kadang berubah, akronim DAD adalah. ditampilkan dalam urutan itu.

Identity and authentication, authorization, and accountability

Istilah "AAA" sering digunakan, menggambarkan landasan konsep Authentication,. Otorisasi, dan Akuntabilitas. Meninggalkan keluar dari AAA singkatan adalah Identifikasi,. yang diperlukan sebelum tiga "A" dapat mengikuti.

Identity and authentication

Identitas adalah klaim: jika nama Anda adalah "Orang X," Anda mengidentifikasi diri dengan mengatakan "Saya Orang X. "Identitas saja lemah karena tidak ada bukti. Anda juga dapat mengidentifikasi diri dengan mengatakan "Saya Orang Y." Membuktikan klaim identitas disebut authentication: Anda mengotentikasi klaim identitas, biasanya dengan menyediakan sepotong informasi atau sebuah benda yang hanya Anda dimiliki, seperti password atau paspor Anda.

Authorization

Otorisasi menjelaskan tindakan yang dapat performon sebuah systemonce Anda memiliki iDEN-.tified dan dikonfirmasi. Tindakan mungkin termasuk membaca, menulis, atau mengeksekusi file atau program.

Accountability

Akuntabilitas memegang pengguna jawab atas tindakan mereka. Ini biasanya menemani-plished dengan login dan menganalisis data audit. Menegakkan akuntabilitas membantu menjaga "Orang-orang jujur jujur." Untuk beberapa pengguna, mengetahui bahwa data login tidak cukup. untuk memberikan akuntabilitas: mereka harus tahu bahwa data yang dicatat dan diaudit dan itu. sanksi mungkin akibat dari pelanggaran kebijakan.

Nonrepudiation

Nonrepudiation berarti pengguna tidak dapat menyangkal (menolak) setelah dilakukan transaksi- ation. Ini menggabungkan otentikasi dan integritas: nonrepudiation mengotentikasi iDEN- tersebut. Tity dari pengguna yang melakukan transaksi dan memastikan integritas transaksi itu. Youmust memiliki kedua otentikasi dan integritas untuk memiliki nonrepudiation: membuktikan Anda. menandatangani kontrak untuk membeli mobil (otentikasi identitas Anda sebagai pembeli) tidak. berguna jika dealer mobil dapat mengubah harga dari $ 20.000 sampai $ 40.000 (melanggar integritas kontrak).

Least privilege and need to know

Keistimewaan paling berarti pengguna harus diberikan jumlah minimum akses. (Otorisasi) yang diperlukan untuk melakukan pekerjaan mereka, tapi tidak lebih. Paling istimewa diterapkan untuk kelompok benda. Perlu tahu lebih rinci dari paling istimewa: pengguna keharusan.
perlu tahu bahwa bagian tertentu dari informasi sebelum mengakses itu.

Subjects and objects

Sebuah subjek merupakan entitas yang aktif pada sistem data. Sebagian contoh pelajaran melibatkan orang mengakses file data. Namun, program komputer yang menjalankan adalah subyek. demikian juga Sebuah objek adalah data pasif dalam sistem. Benda dapat berkisar fromdatabases ke file teks. Hal penting untuk diingat tentang obyek adalah bahwa mereka pasif dalam sistem Mereka tidak memanipulasi benda-benda lain.

Defense-in-depth

Pertahanan-mendalam (juga disebut pertahanan berlapis) berlaku beberapa perlindungan (juga. disebut kontrol: tindakan yang diambil untuk mengurangi resiko) untuk melindungi aset. Setiap keamanan tunggal control mungkin gagal; dengan mengerahkan beberapa kontrol, Anda meningkatkan kerahasiaan integritas dan ketersediaan data Anda.

ACCESS CONTROL MODELS

Sekarang kita telah meninjau konsep kontrol akses landasan, kita bisa mendiskusikan.
berbeda model kontrol akses: model utama adalah akses Discretionary Control (DAC), Wajib Access Control (MAC), dan akses nondiscretionary control.

Discretionary access controls

Discretionary Access Control (DAC) memberikan pelajaran kontrol penuh dari benda-benda yang mereka miliki telah diberi akses ke, termasuk berbagi objek dengan mata pelajaran lain. Subyek diberdayakan dan mengendalikan data mereka. Sistem operasi standar UNIX dan Windows menggunakan DAC untuk sistem berkas: subjek dapat memberikan akses mata pelajaran lain untuk file mereka mengubah atribut mereka, mengubah mereka, atau menghapusnya.

Mandatory access controls

Wajib Access Control (MAC) adalah sistem-ditegakkan kontrol akses berdasarkan sub. izin ject dan label objek. Subjek dan objek memiliki izin dan label, masing-masing, seperti rahasia, rahasia, dan rahasia. Sebuah subjek mungkin mengakses objek hanya jika izin subjek sama dengan atau lebih besar dari label objek. Subyek tidak dapat berbagi objek dengan mata pelajaran lain yang tidak memiliki izin yang tepat atau "menulis" objek untuk tingkat klasifikasi yang lebih rendah (seperti sejak rahasia untuk rahasia). Sistem MAC biasanya terfokus pada menjaga kerahasiaan data.

Nondiscretionary access control

Peran Berbasis Access Control (RBAC) mendefinisikan bagaimana informasi diakses pada sistem berdasarkan peran subjek. Peran A bisa menjadi perawat, administrator cadangan, bantuan teknisi meja, dll Subyek dikelompokkan menjadi peran dan peran masing-masing didefinisikan memiliki izin akses berdasarkan peran, bukan individu. RBAC adalah jenis kontrol akses nondiscretionary karena pengguna tidak memiliki kebijaksanaan mengenai kelompok benda mereka diizinkan untuk mengakses dan tidak mampu untuk mentransfer objek untuk mata pelajaran lainnya. Kontrol akses tugas berbasis model kontrol akses nondiscretionary lain, berkaitan dengan RBAC.

Rule-based access controls

Sebuah sistem kontrol akses berbasis aturan menggunakan serangkaian aturan yang ditetapkan, pembatasan,dan filter untuk mengakses objek dalam suatu sistem. Aturan-aturan dalam bentuk "Jika / kemudian" pernyataan. Contoh dari perangkat kontrol akses berbasis aturan adalah proxy firewall yang memungkinkan pengguna untuk berselancar di Web dengan konten yang disetujui yang telah ditetapkan hanya (Jika pengguna berwenang untuk berselancar di Web dan situs pada daftar yang disetujui, kemudian memungkinkan akses). Situs lain dilarang dan aturan ini diberlakukan di seluruh semua dikonfirmasi pengguna.

Centralized access control

Kontrol akses terpusat berkonsentrasi kontrol akses di satu titik logis untuk sistem atau organisasi. Alih-alih menggunakan database kontrol akses lokal, sistem mengotentikasi melalui server otentikasi pihak ketiga. Kontrol akses terpusat dapat digunakan untuk menyediakan Single Sign-On (SSO), di mana subjek dapat mengotentikasi sekali, dan kemudian mengakses beberapa sistem. Kontrol akses terpusat dapat terpusat menyediakan tiga "A" dari kontrol akses: Otentikasi, Otorisasi, dan Akuntabilitas.

Access control lists

Daftar kontrol akses (ACL) digunakan di seluruh banyak kebijakan keamanan IT, prosedur-prosedur-, dan teknologi. Daftar kontrol akses adalah daftar objek; setiap entri menggambarkan mata pelajaran yang dapat mengakses objek tersebut. Akses upaya subjek untuk obyek yang tidak memiliki entri yang cocok pada ACL akan ditolak.

Access provisioning lifecycle

Setelah model kontrol akses yang tepat telah dipilih dan digunakan, akses provisi siklus hidup harus dijaga dan diamankan. Sementara banyak organisasi folpraktik terbaik rendah untuk mengeluarkan akses, banyak kekurangan proses formal untuk memastikan seumur hidup akses disimpan aman sebagai karyawan dan kontraktor bergerak dalam sebuah organisasi. IBM menjelaskan aturan siklus hidup identitas berikut:

• "Password pemeriksaan kepatuhan kebijakan

• Memberitahu pengguna untuk mengubah password mereka sebelum mereka berakhir

• Mengidentifikasi hidup perubahan siklus seperti rekening yang tidak aktif selama lebih dari 30 hari berturut-turut

• Mengidentifikasi akun baru yang belum digunakan formore dari 10 hari

• Mengidentifikasi akun yang calon untuk dihapus karena mereka telah ditangguhkan selama lebih dari 30 hari

• Ketika kontrak berakhir mengidentifikasi semua account milik mitra bisnis atau karyawan kontraktor dan mencabut hak akses

User entitlement, access review, and audit

Akses agregasi terjadi sebagai pengguna individu memperoleh lebih banyak akses ke banyak sistem ini dapat terjadi secara sengaja, sebagai fungsi Single Sign-On (SSO). Hal ini juga dapat terjadi tidak sengaja pengguna sering mendapatkan hak baru (juga disebut hak akses) karena mereka mengambil peran atau tugas baru. Hal ini dapat mengakibatkan otorisasi merayap: pengguna mendapatkan lebih banyak hak tanpa penumpahan yang lama. Kekuatan hak-hak ini dapat com-pound dari waktu ke waktu, mengalahkan kontrol seperti hak istimewa setidaknya dan pemisahan tugas. Hak pengguna harus secara rutin ditinjau dan diaudit. Proses harus bangan oped yang mengurangi atau menghilangkan hak tua yang baru diberikan.

2.

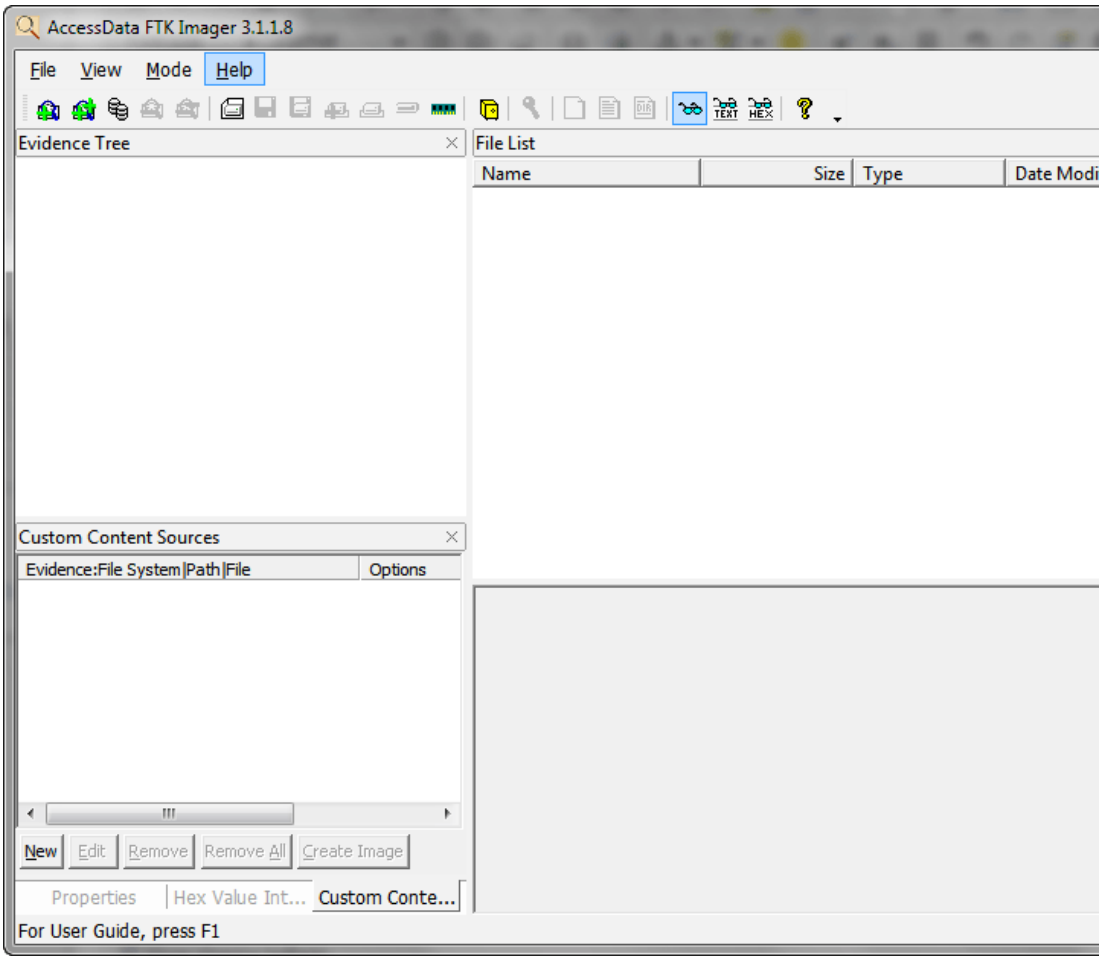
Menggunakan FTK Imager untuk menjamin keaslian Data Elektronik

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

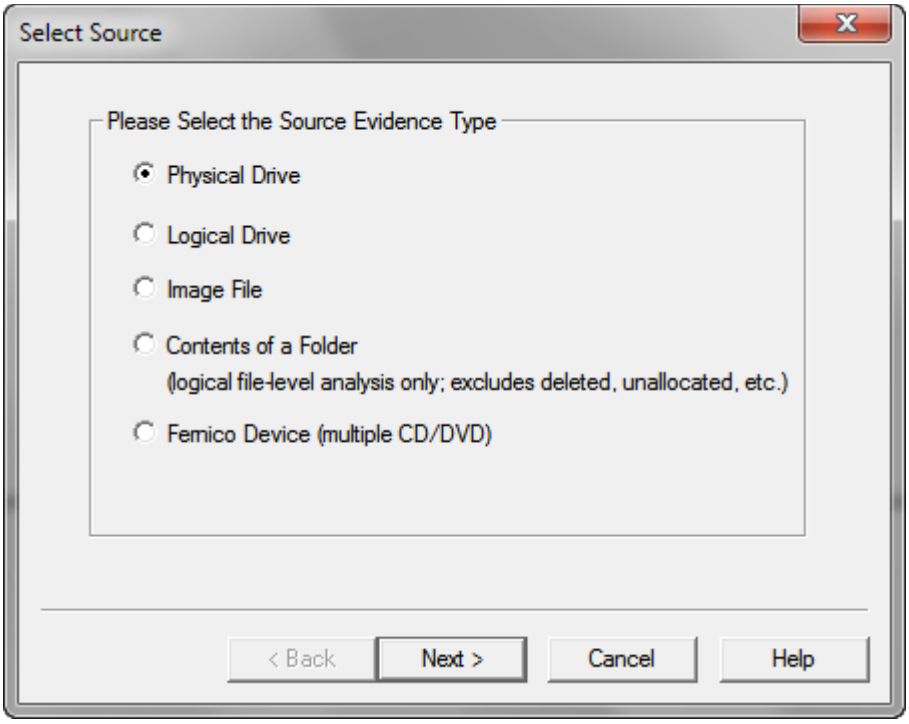
Oleh karena itu ada beberapa cara yang bisa kita lakukan untuk menjamin keaslian data tersebut :

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



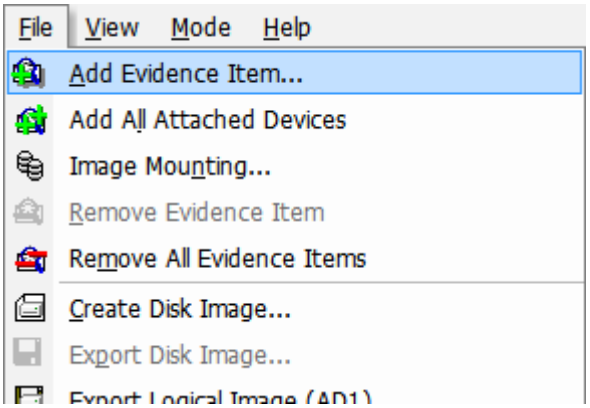
Untuk membuat Hash value maupun direktory listing kita bisa lakukan dengan membuat Image dari CDRom tersebut. FTK imager mengenal beberapa sumber dari Image yaitu :



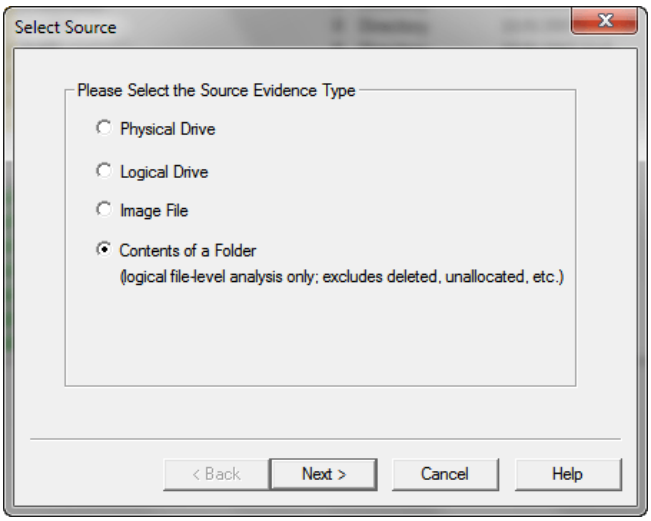
1. Physical Drive, biasanya berupa harddisk atau flash disk, disini kita bicara mengenai drive secara fisik, jadi kalau kapasitas ada 500 gb maka image kita juga akan memiliki size sebesar 500 gb (kecuali kita compress), jadi kita akan mengclone harddisk secara fisik , tidak perduli apakah ada isinya 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:

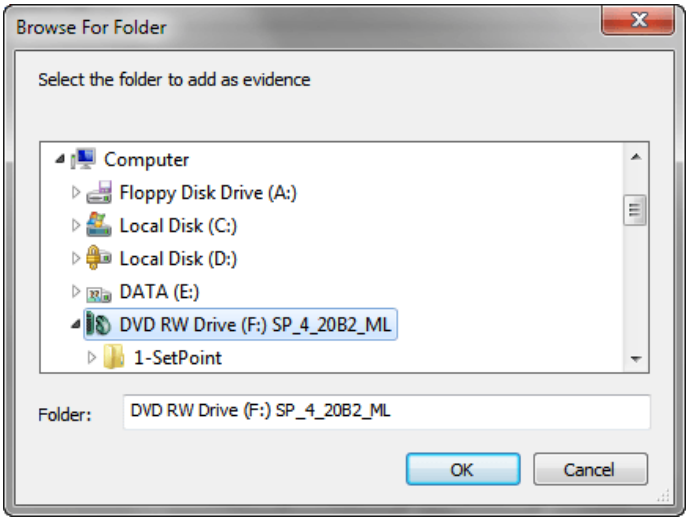
- Kita backup/cloning dulu secara fisik CDROM tadi menjadi 2 atau lebih Copy (bisa dengan Nero atau software burning lainnya)
- Kita Add Evidence ke FTK Imager



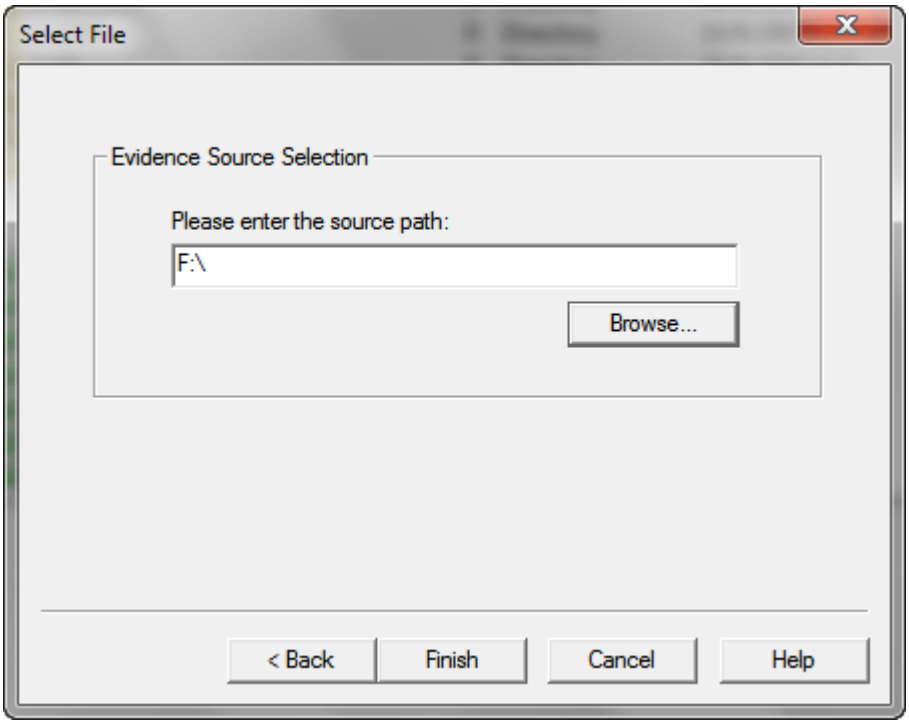
- Kita isi dengan Contents of a folder



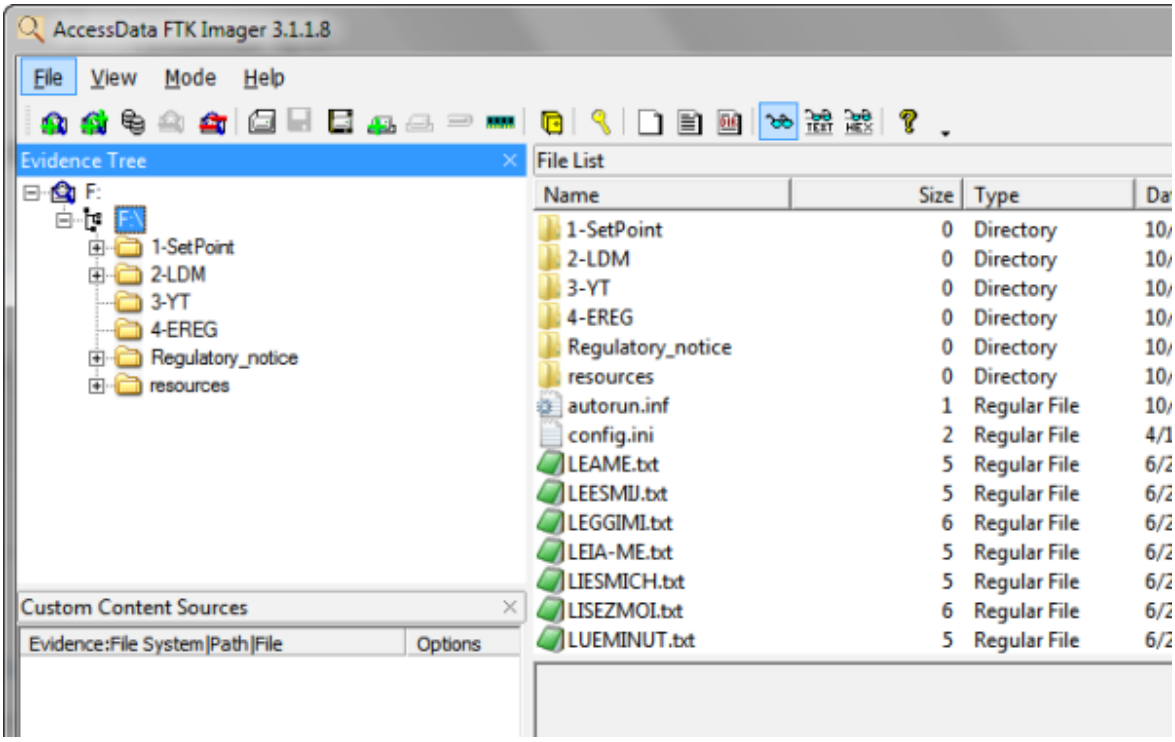
- Kita Next lalu Browse CD-ROM kita



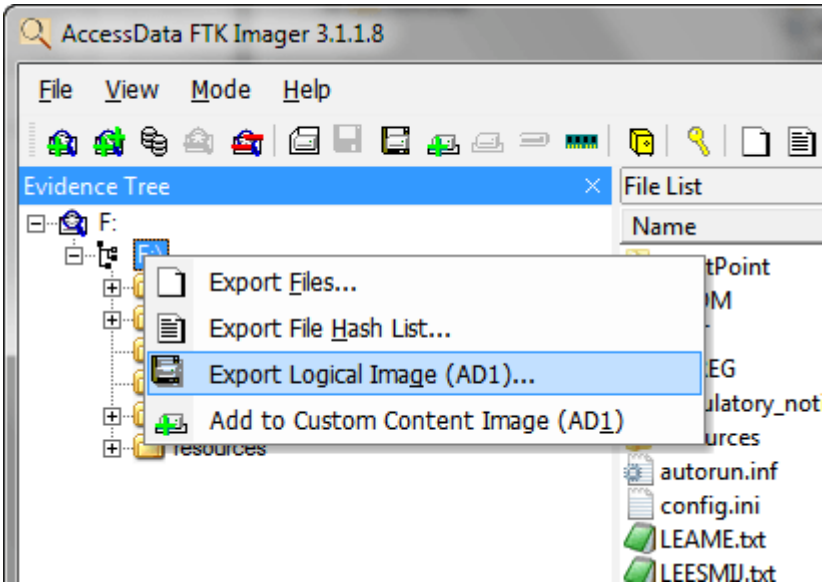
- Lalu Klik Finish



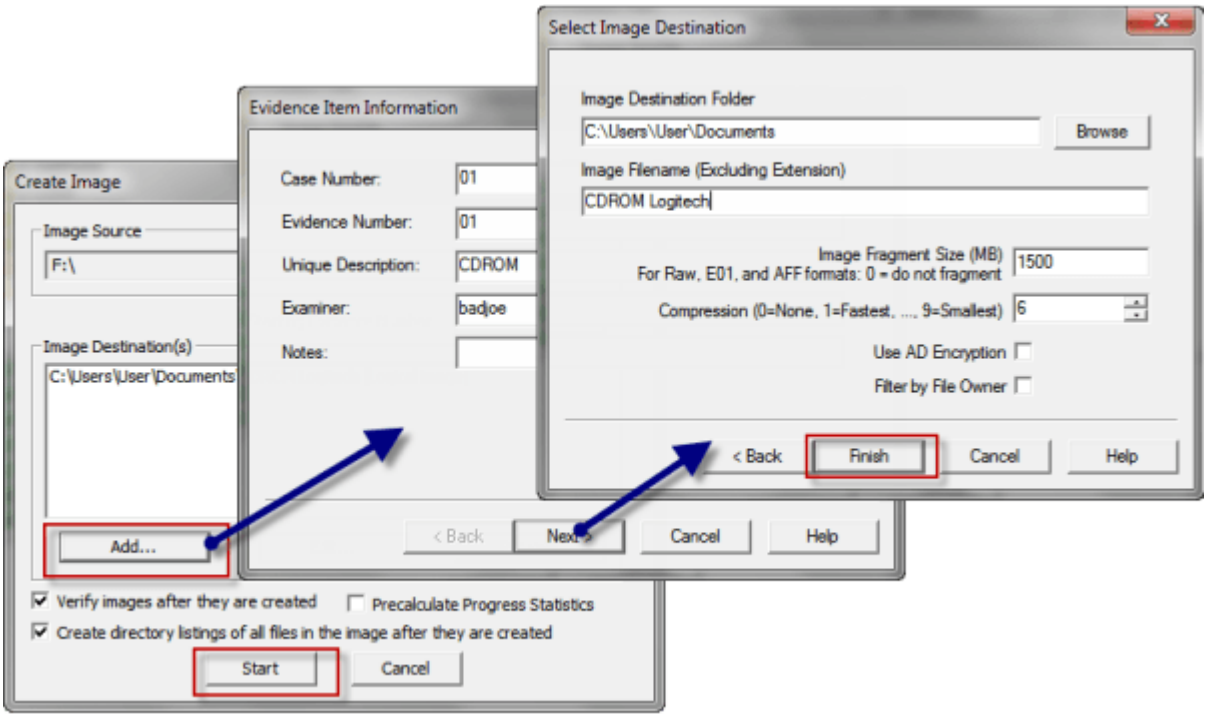
- Ini hasilnya di FTK Imager



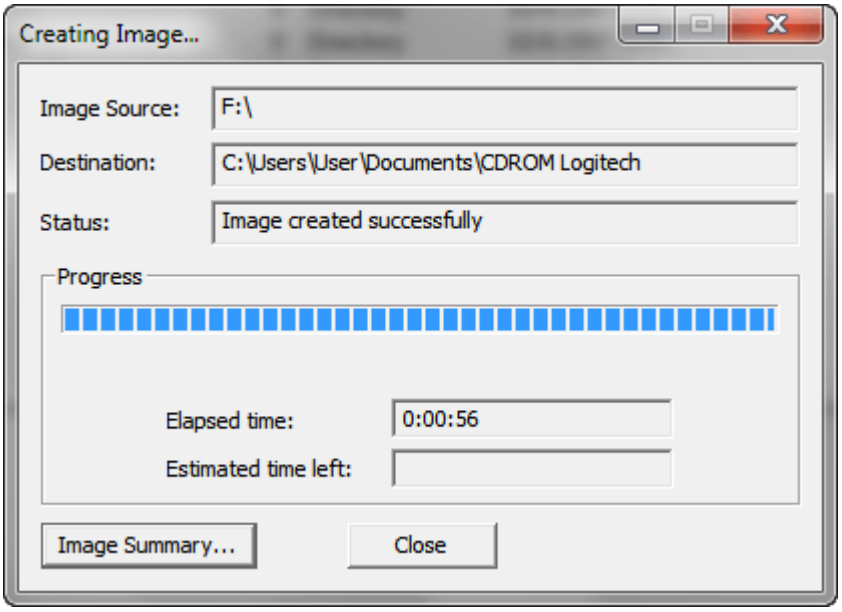
- Untuk membuat Imagenya Kita Klik kanan di F:, lalu pilih Export Logical Image



- 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



- Ini jika sudah selesai



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

```
Created By AccessData® FTK® Imager 3.1.1.8

Case Information:
Acquired using: ADI3.1.1.8
Case Number: 01
Evidence Number: 01
Unique Description: CDROM
Examiner: badjoe
Notes:

---------------------------------------------------------------

Information for C:\Users\User\Documents\CDROM Logitech.ad1:
[Computed Hashes]
 MD5 checksum:    7ed8883418b06d2cc403c16afa72ec5d
 SHA1 checksum:   64a5dfe000fce781d2bd89c6be6c87ebbca4641d

Image information:
 Acquisition started:   Sat Dec 01 12:04:33 2012
 Acquisition finished:  Sat Dec 01 12:05:29 2012
 Segment list:
  C:\Users\User\Documents\CDROM Logitech.ad1

Image Verification Results:
 Verification started:  Sat Dec 01 12:05:30 2012
 Verification finished: Sat Dec 01 12:05:30 2012
 MD5 checksum:    7ed8883418b06d2cc403c16afa72ec5d : verified
 SHA1 checksum:   64a5dfe000fce781d2bd89c6be6c87ebbca4641d : verified
```

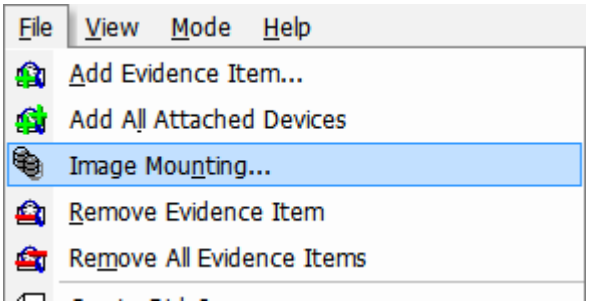
file listing dan file summary yang kita dan WP tandatangani bisa kita lampirkan sebagai KKP

Mounting File Image

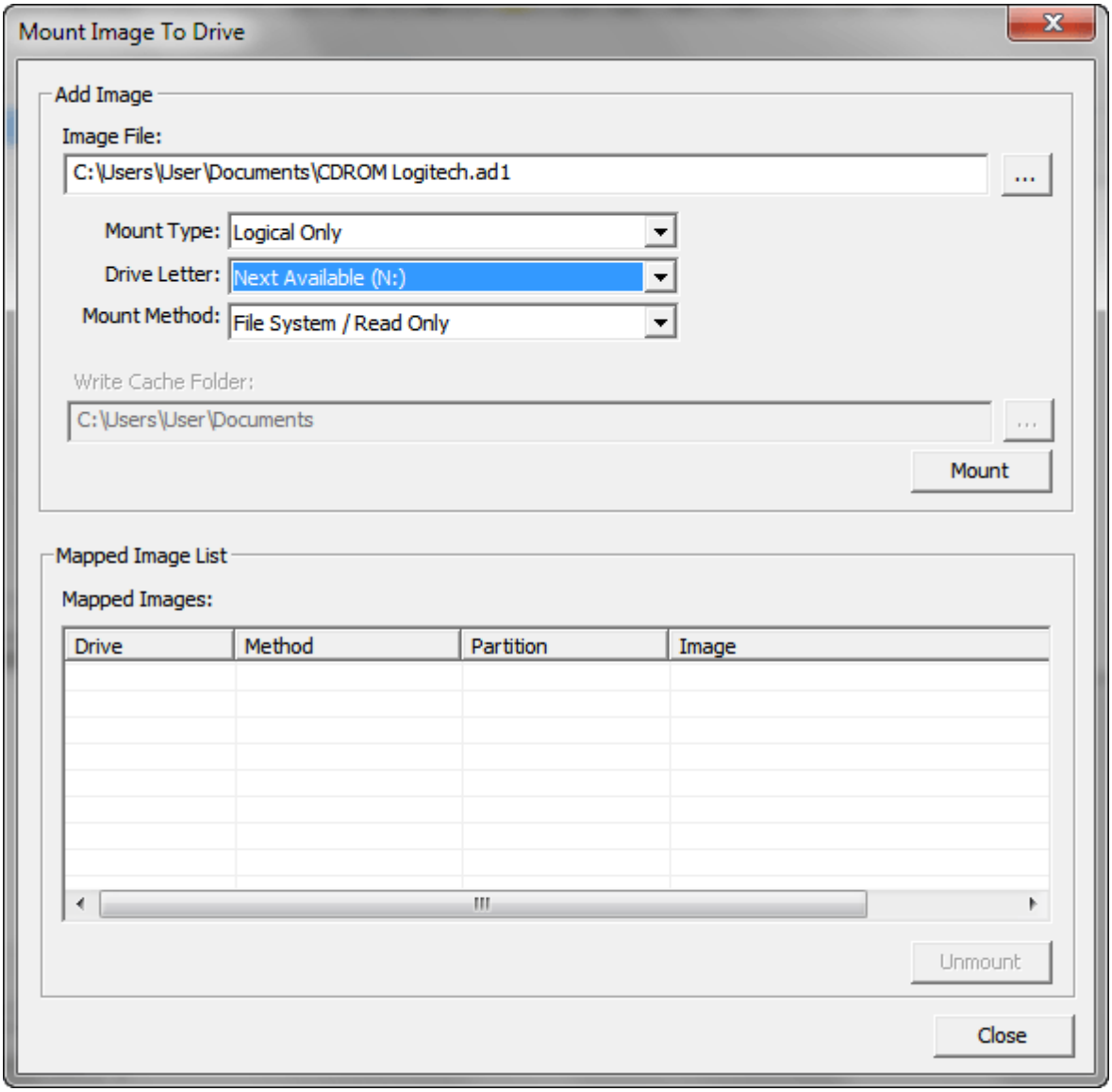
File image berupa satu file dng extension ad1, agar bisa dilihat isinya maka harus kita mounting atau taruh disuatu drive agar terlihat semua isinya. ini berguna karena kita lebih aman bekerja dengan file cloning/imagenya saja, sementara CDROM aslinya bisa kita safe ditempat yang aman

Langkah-2 nya :

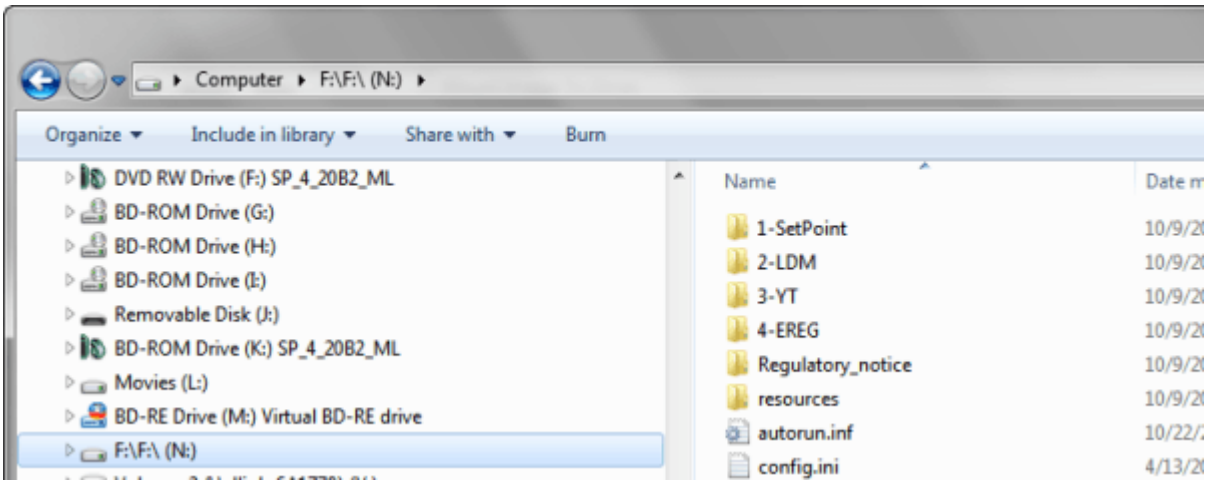
- Klik File –> Image Mounting



- pilih filenya



- Klik Mount, ini hasilnya



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