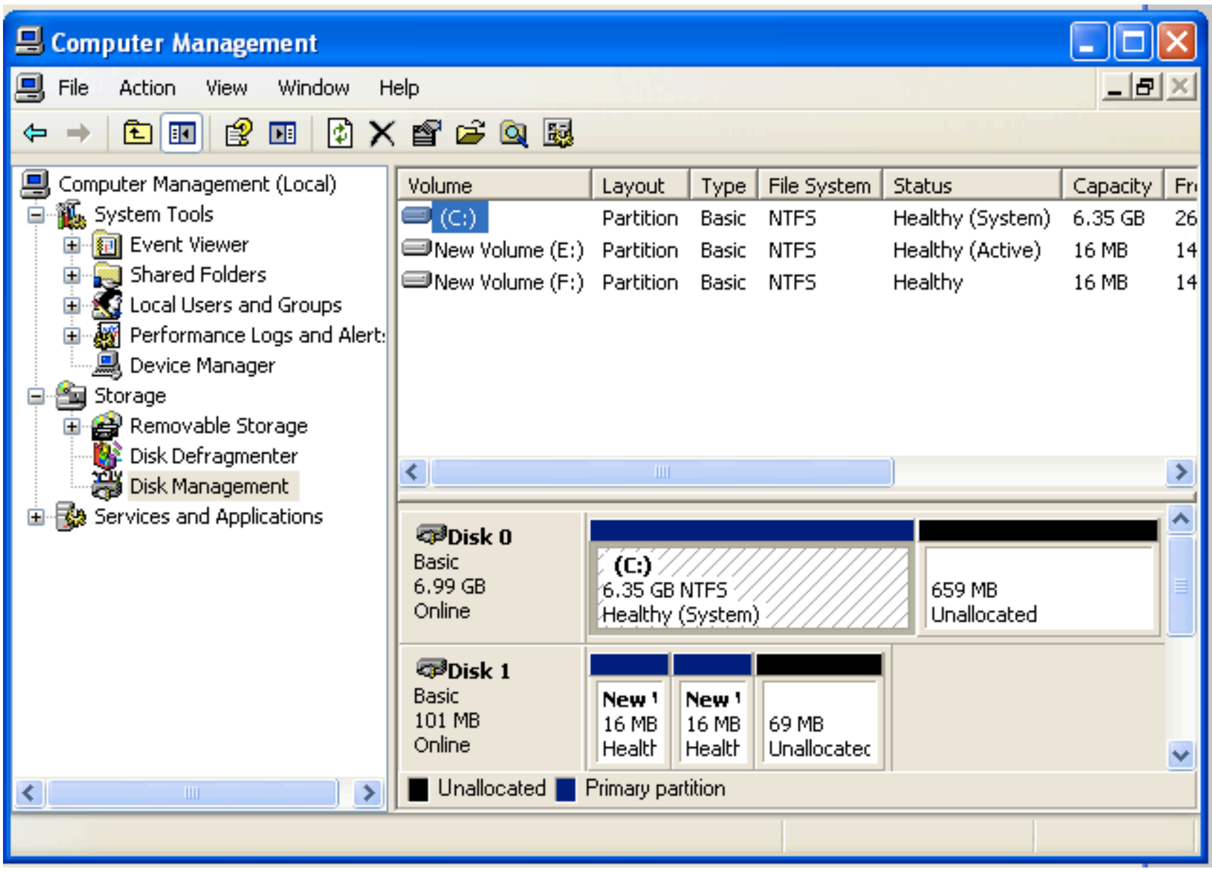
Project 14: Pengenalan FTK (15 pts.)

Kebutuhan Project

- Komputer Windows XP virtual, yang sudah dibuat sebelumnya.
- Virtual hard disk kedua berukuran kecil, yang sudah digunakan pada project 2 sebelumnya (berukuran 100M, jika sudah tidak ada buat kembali di virtual box seperti pada project 2 dengan ukuran 100M).

Membuat Clean Disk (Disk yang benar-benar kosong)

1. Untuk langkah ini saudara harus memiliki virtual hard berukuran kecil (100M) yang terhubung di VM, yang sudah di buat pada project sebelumnya. Jika tidak ada, buat terlebih dahulu atau masukkan USB flash drive. Tidak masalah di dalamnya terdapat data atau tidak.
   a. Click **Start**, klik kanan "**My Computer**", dan click **Manage**.
   b. Maka akan terlihat disk berukuran kecil yang bernama "Disk 1", seperti terlihat di bawah ini.



Volume	Layout	Type	File System	Status	Capacity	Fr
(C:)	Partition	Basic	NTFS	Healthy (System)	6.35 GB	26
New Volume (E:)	Partition	Basic	NTFS	Healthy (Active)	16 MB	14
New Volume (F:)	Partition	Basic	NTFS	Healthy	16 MB	14

Disk 0
Basic
6.99 GB
Online

(C:)
6.35 GB NTFS
Healthy (System)

659 MB
Unallocated

Disk 1
Basic
101 MB
Online

New
16 MB
Healt

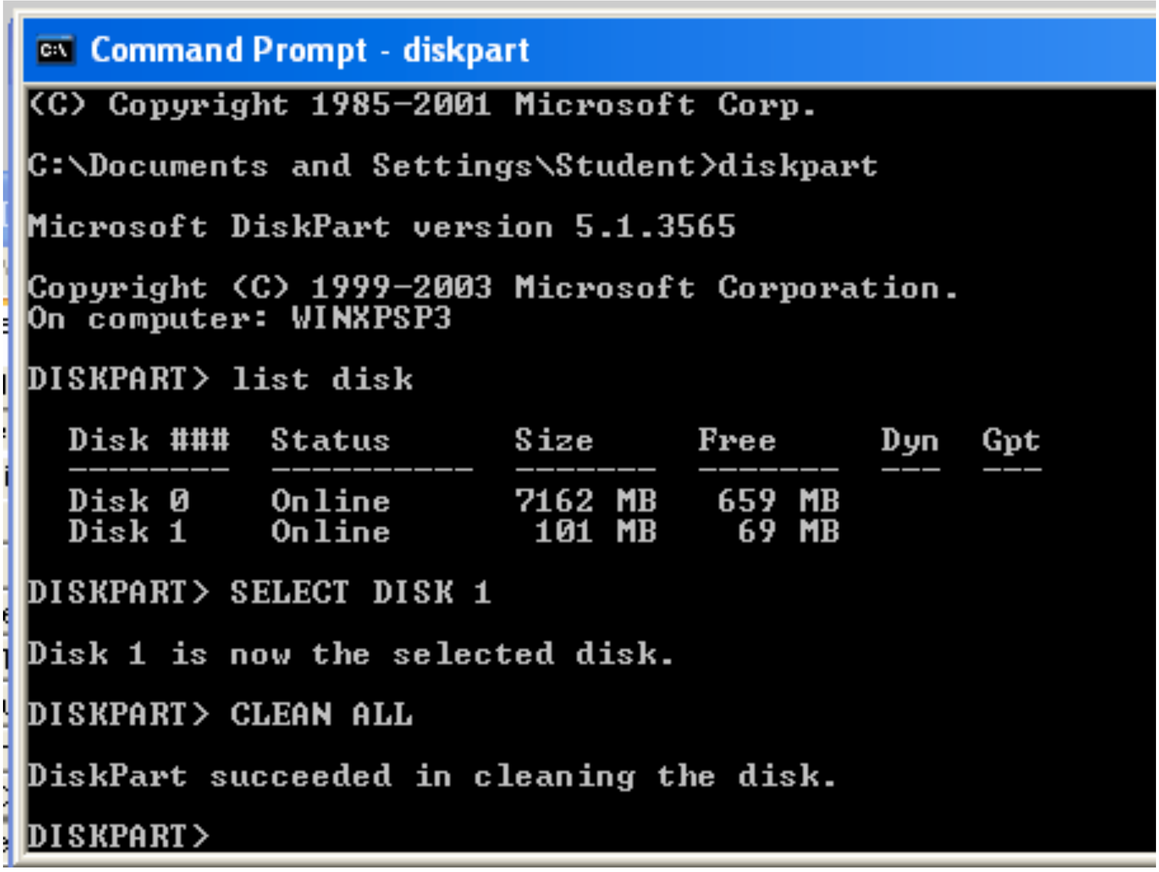
New
16 MB
Healt

69 MB
Unallocatec

■ Unallocated ■ Primary partition

   c. Untuk membuka Command Terminal, Click **Start**, **Run**. Ketikkan CMD dan tekan Enter.
   d. Jalankan perintah berikut untuk membersihkan disk ke dua. Hati-hati jangan salah disk!

```
DISKPART
LIST DISK
SELECT DISK 1
CLEAN ALL
```



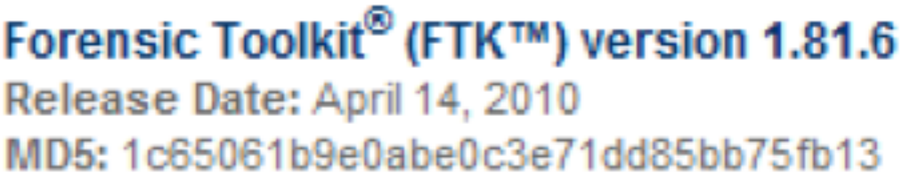
```
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Student>diskpart

Microsoft DiskPart version 5.1.3565

Copyright (C) 1999-2003 Microsoft Corporation.
On computer: WINXPSP3

DISKPART> list disk

  Disk ###  Status      Size     Free     Dyn  Gpt
  --------  ----------  -------  -------  ---  ---
  Disk 0    Online      7162 MB   659 MB
  Disk 1    Online       101 MB    69 MB

DISKPART> SELECT DISK 1

Disk 1 is now the selected disk.

DISKPART> CLEAN ALL

DiskPart succeeded in cleaning the disk.

DISKPART>
```

Mendownload FTK

2. Untuk project ini kia gunakan FTK versi free demo mode. Bisa di downloafd dari elearning. File dengan nama "FTK-Forensic_Toolkit-1.81.6.exe".

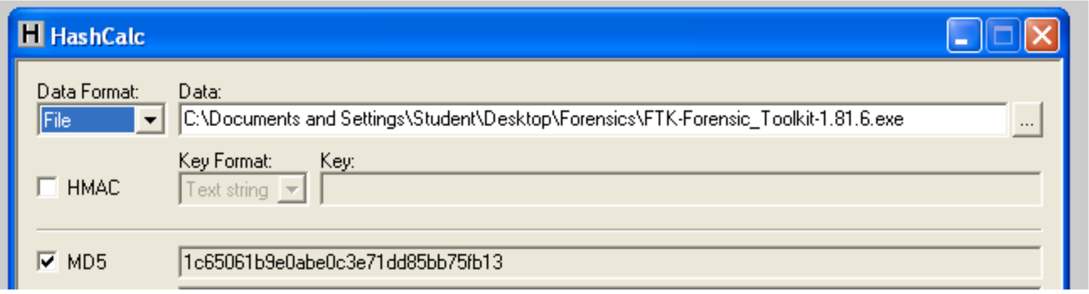
Verifikasi Hash

Berikut ini nilai Hashnya :



Forensic Toolkit® (FTK™) version 1.81.6
Release Date: April 14, 2010
MD5: 1c65061b9e0abe0c3e71dd85bb75fb13

3. Untuk mengetes file, bisa gunakan Hashcalc. Jika tidak ada bisa di download di: http://www.slavasoft.com/hashcalc/
   a. Buka Hashcalc.
   b. Seret file "**FTK-Forensic_Toolkit-1.81.6.exe**" ke Hashcalc window.
   c. Maka akan terlihat nilai hah, yang berakhiran fb13, seperti di bawah ini:



HashCalc

Data Format: File

Data: C:\Documents and Settings\Student\Desktop\Forensics\FTK-Forensic_Toolkit-1.81.6.exe

□ HMAC Key Format: Text string Key:

☑ MD5 1c65061b9e0abe0c3e71dd85bb75fb13

Install FTK

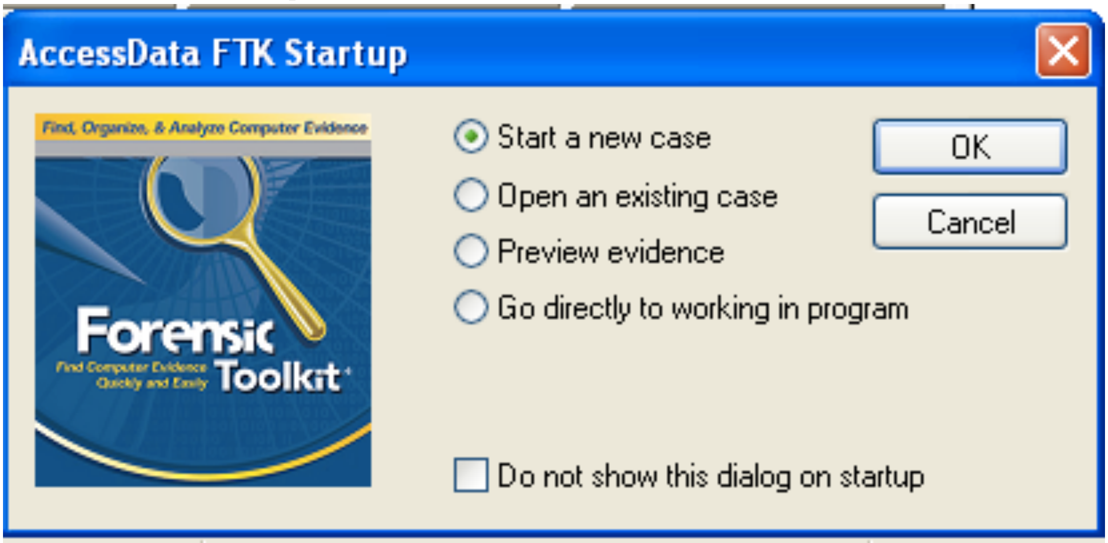
4. Double-click file "**FTK-Forensic_Toolkit-1.81.6.exe**" dan install software dengan pilihan default.

Menjalankan FTK

5. Setelah di instal, FTK akan berjalan.
   a. Ketika ada kotak pesan Error box "No security device was found...", click **No**.
   b. Ketika ada kotak pesan Error box "The KFF Hash library file was not found...", click **OK**.
   c. Ketika muncul kotak box pops yang menjelaskan keterbatasan versi demo, click **OK**.

Menjalankan New Case

6. Pada kotak "AccessData FTK Startup", biarkan pilihan default "**Start a new case**", seperti di bawah ini, dan click **OK**.



AccessData FTK Startup

● Start a new case

○ Open an existing case

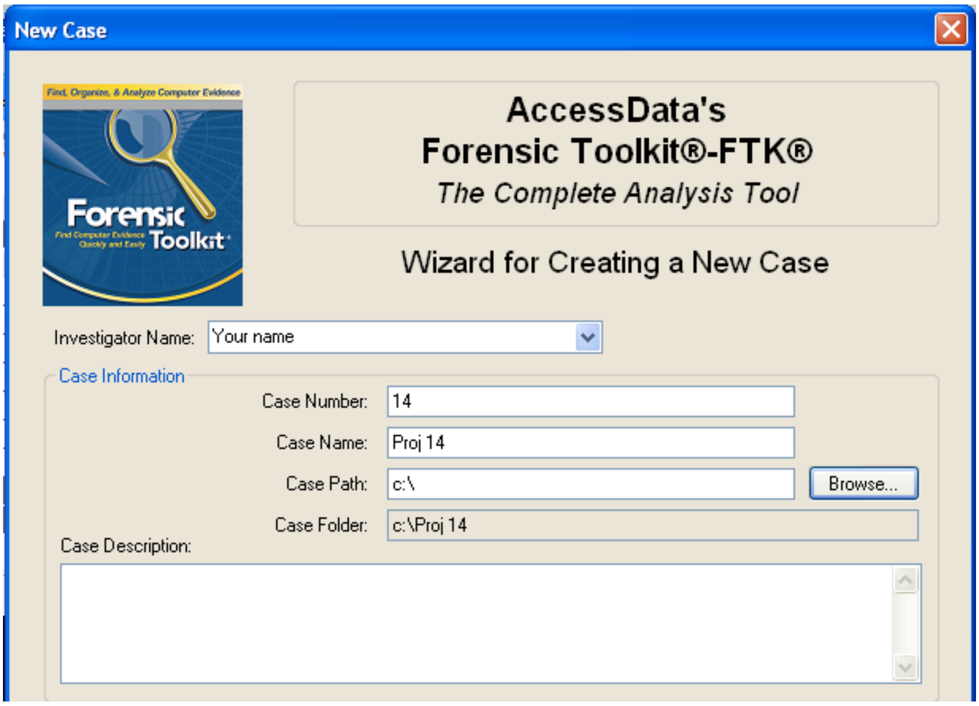
○ Preview evidence

○ Go directly to working in program

□ Do not show this dialog on startup

OK
Cancel
Find, Organize, & Analyze Computer Evidence
Forensic Toolkit
Find Computer Evidence Quickly and Easily

   a. Pada jendela screen yang bertuliskan "Wizard for Creating a New Case", Isi fields seperti berikut, ganti "Your Name" dengan nama masing-masing. Click **Next**.



New Case

AccessData's
Forensic Toolkit®-FTK®
The Complete Analysis Tool

Wizard for Creating a New Case

Investigator Name: Your name

Case Information

Case Number: 14

Case Name: Proj 14

Case Path: c:\

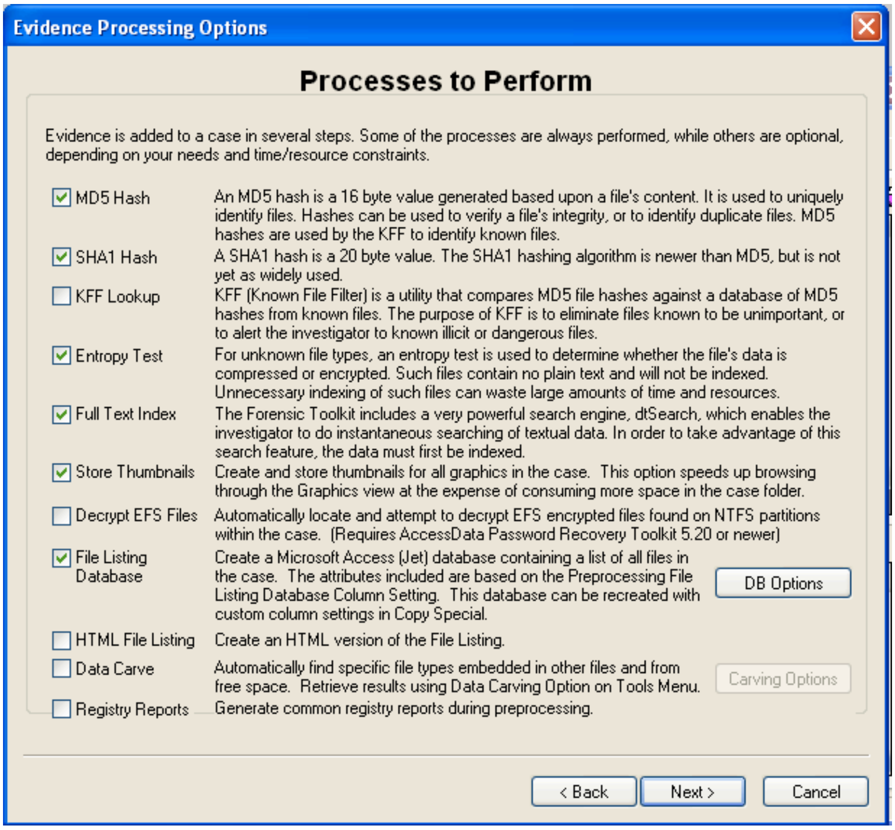
Case Folder: c:\Proj 14

Case Description:

b. Pada jendela screen yang berisi "Forensic Examiner Information", biarkan fields tetap kosong dan click **Next**.

c. Pada screen yang berisi "Case Log Options", biarkan pilihan default, yang akan mencatat semua. Click **Next**.

d. Pada screen yang bertuliskan "Processes to Perform", buang deselect "KFF Lookup" and "Decrypt EFS Files", karena fitur ini tidak tersedia pada versi demo, seperti di bawah ini. Click **Next**.



Evidence Processing Options

Processes to Perform

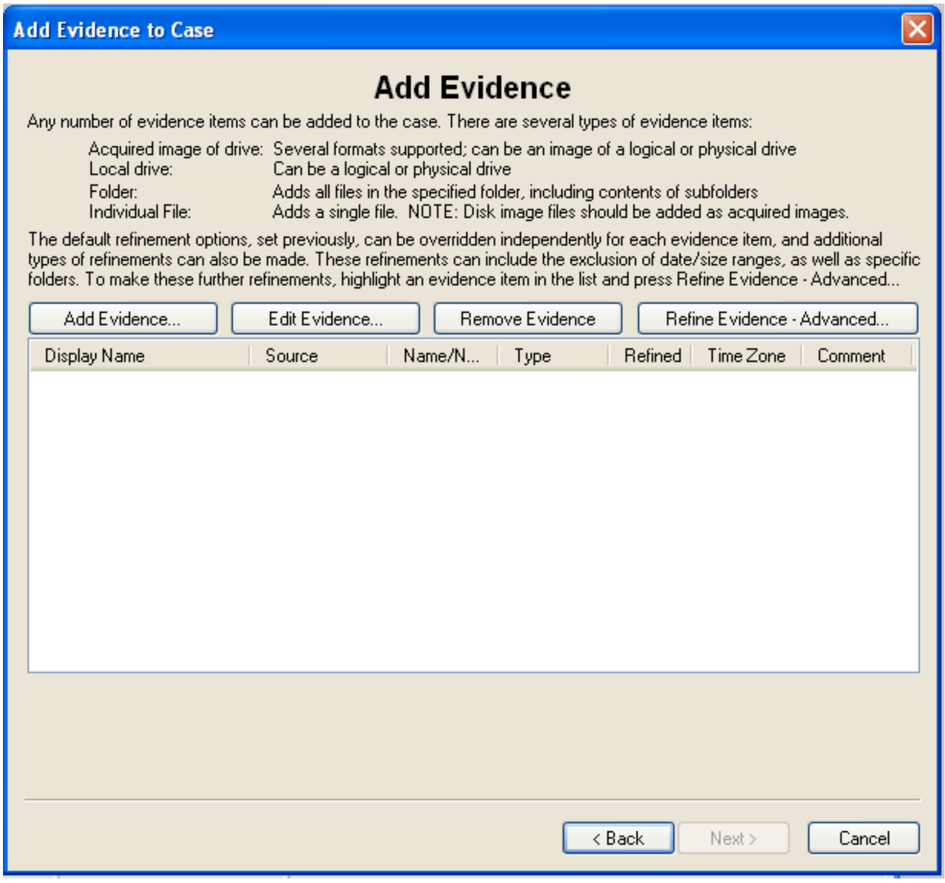
Evidence is added to a case in several steps. Some of the processes are always performed, while others are optional, depending on your needs and time/resource constraints.

☑ MD5 Hash	An MD5 hash is a 16 byte value generated based upon a file's content. It is used to uniquely identify files. Hashes can be used to verify a file's integrity, or to identify duplicate files. MD5 hashes are used by the KFF to identify known files.
☑ SHA1 Hash	A SHA1 hash is a 20 byte value. The SHA1 hashing algorithm is newer than MD5, but is not yet as widely used.
☐ KFF Lookup	KFF (Known File Filter) is a utility that compares MD5 file hashes against a database of MD5 hashes from known files. The purpose of KFF is to eliminate files known to be unimportant, or to alert the investigator to known illicit or dangerous files.
☑ Entropy Test	For unknown file types, an entropy test is used to determine whether the file's data is compressed or encrypted. Such files contain no plain text and will not be indexed. Unnecessary indexing of such files can waste large amounts of time and resources.
☑ Full Text Index	The Forensic Toolkit includes a very powerful search engine, dtSearch, which enables the investigator to do instantaneous searching of textual data. In order to take advantage of this search feature, the data must first be indexed.
☑ Store Thumbnails	Create and store thumbnails for all graphics in the case. This option speeds up browsing through the Graphics view at the expense of consuming more space in the case folder.
☐ Decrypt EFS Files	Automatically locate and attempt to decrypt EFS encrypted files found on NTFS partitions within the case. (Requires AccessData Password Recovery Toolkit 5.20 or newer)
☑ File Listing Database	Create a Microsoft Access (Jet) database containing a list of all files in the case. The attributes included are based on the Preprocessing File Listing Database Column Setting. This database can be recreated with custom column settings in Copy Special.
☐ HTML File Listing	Create an HTML version of the File Listing.
☐ Data Carve	Automatically find specific file types embedded in other files and from free space. Retrieve results using Data Carving Option on Tools Menu.
☐ Registry Reports	Generate common registry reports during preprocessing.

e. Pada screen yang bertuliskan "Refine Case-Default", biarkan pilihan default "Include All Items". Click **Next**.

f. Pada screen yang bertuliskan "Refine Index -Default", biarkan pilihan default. Click **Next**.

g. Akan terlihat layar "Add Evidence", seperti berikut ini.



Add Evidence to Case

Add Evidence

Any number of evidence items can be added to the case. There are several types of evidence items:

Acquired image of drive:	Several formats supported; can be an image of a logical or physical drive
Local drive:	Can be a logical or physical drive
Folder:	Adds all files in the specified folder, including contents of subfolders
Individual File:	Adds a single file. NOTE: Disk image files should be added as acquired images.

The default refinement options, set previously, can be overridden independently for each evidence item, and additional types of refinements can also be made. These refinements can include the exclusion of date/size ranges, as well as specific folders. To make these further refinements, highlight an evidence item in the list and press Refine Evidence - Advanced...

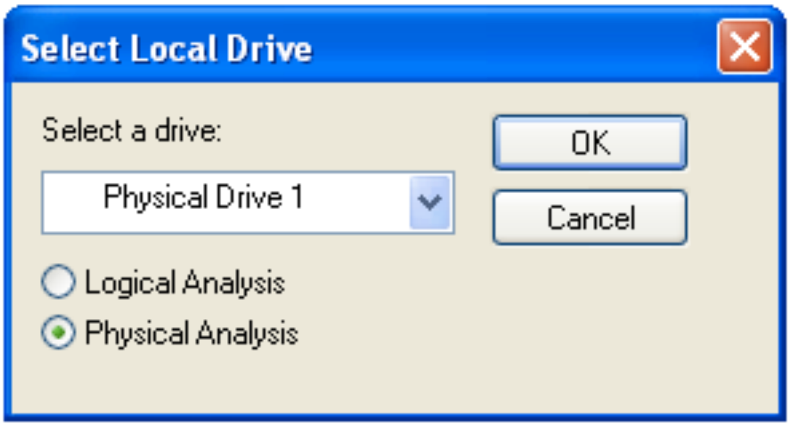
Display Name	Source	Name/N...	Type	Refined	Time Zone	Comment

Menambahkan Evidence ke Case

7. Pada kotak "Add Evidence", click tombol "**Add Evidence...**".

   a. Pada kotak "Add Evidence to Case", pilih "**Local Drive**", dan click **Continue**.

   b. Pada kotak "Select Local Drive", click "**Physical Analysis**" dan pilih drive "Physical Drive 1", seperti terlihat di bawah ini. Click **OK**.



Select Local Drive

Select a drive: Physical Drive 1

○ Logical Analysis
● Physical Analysis

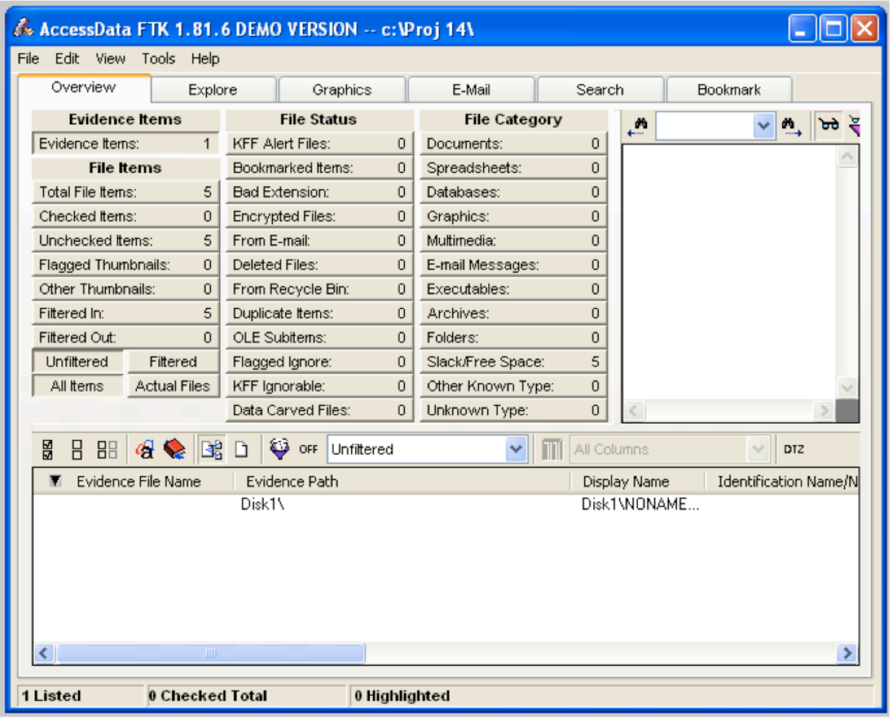
c. Pada kotak "Evidence Information", click **OK**.

d. Pada kotak "Add Evidence", click **Next**.

e. Pada kotak "New Case Setup is Now Complete", click **Finish**.

f. Saat kotak "Processing File" tampil. Tunggu sampai selesai ---Tidak akan memakan waktu lama jika ukuran filenya kecil.

g. Maka akan terlihat tampilan seperti di bawah ini, yang memperlihatkan "Evidence Items: 1" pada kiri atas jendela.



Evidence Items		File Status		File Category	
Evidence Items:	1	KFF Alert Files:	0	Documents:	0
File Items		Bookmarked Items:	0	Spreadsheets:	0
Total File Items:	5	Bad Extension:	0	Databases:	0
Checked Items:	0	Encrypted Files:	0	Graphics:	0
Unchecked Items:	5	From E-mail:	0	Multimedia:	0
Flagged Thumbnails:	0	Deleted Files:	0	E-mail Messages:	0
Other Thumbnails:	0	From Recycle Bin:	0	Executables:	0
Filtered In:	5	Duplicate Items:	0	Archives:	0
Filtered Out:	0	OLE Subitems:	0	Folders:	0
Unfiltered	Filtered	Flagged Ignore:	0	Slack/Free Space:	5
All Items	Actual Files	KFF Ignorable:	0	Other Known Type:	0
		Data Carved Files:	0	Unknown Type:	0

Unfiltered

Evidence File Name	Evidence Path	Display Name	Identification Name/N
	Disk1\	Disk1\NONAME...	

1 Listed | 0 Checked Total | 0 Highlighted

Simpan Screen Image

8. Pastikan terlihat pesan "Evidence Items: 1".

   a. Capture keseluruhan desktop dengan PrntScn.
   HARUS DISUBMIT KESELURUHAN DESKTOP UNTUK MENDAPATKAN POIN MAKSIMAL!

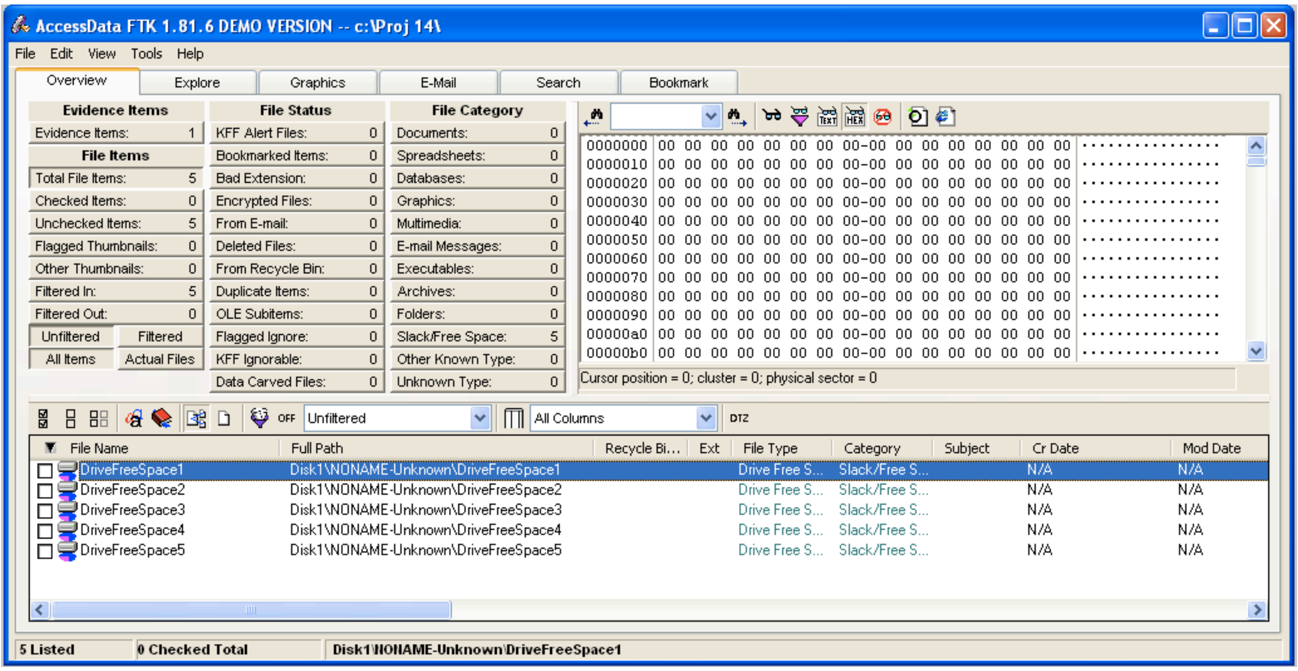
   b. Simpan dengan nama "**Nama Kamu_ 14**".

Jendela FTK

9. Lihat kiri atas jendela FTK. Pada bagian "File Items", FTK akan menampilkan 'Total File Items" adalah 5. Padahal keseluruha disk tersebut kosong?

   a. Untuk melihatnya, click tombol "Total File Items:". Panel bagian bawah akan memperlihatkan lima items, yang dinamai "DriveFreeSpace1","DriveFreeSpace2","DriveFreeSpace3", dll.

   b. Pada panel kiri bawah jendela FTK, click "DriveFreeSpace1". Sudut kanan atas memperlihatkan hexadecimal view yang terdiri dari byte-byte pada file, seperti terlihat di bawah ini.



AccessData FTK 1.81.6 DEMO VERSION -- c:\Proj 14\

File Edit View Tools Help
Overview Explore Graphics E-Mail Search Bookmark

Evidence Items		File Status		File Category	
Evidence Items:	1	KFF Alert Files:	0	Documents:	0
File Items		Bookmarked Items:	0	Spreadsheets:	0
Total File Items:	5	Bad Extension:	0	Databases:	0
Checked Items:	0	Encrypted Files:	0	Graphics:	0
Unchecked Items:	5	From E-mail:	0	Multimedia:	0
Flagged Thumbnails:	0	Deleted Files:	0	E-mail Messages:	0
Other Thumbnails:	0	From Recycle Bin:	0	Executables:	0
Filtered In:	5	Duplicate Items:	0	Archives:	0
Filtered Out:	0	OLE Subitems:	0	Folders:	0
Unfiltered	Filtered	Flagged Ignore:	0	Slack/Free Space:	5
All Items	Actual Files	KFF Ignorable:	0	Other Known Type:	0
		Data Carved Files:	0	Unknown Type:	0

```
0000000  00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ................
0000010  00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ................
0000020  00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ................
0000030  00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ................
0000040  00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ................
0000050  00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ................
0000060  00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ................
0000070  00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ................
0000080  00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ................
0000090  00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ................
00000a0  00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ................
00000b0  00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ................
```

Cursor position = 0; cluster = 0; physical sector = 0

OFF Unfiltered All Columns DTZ

File Name	Full Path	Recycle Bi...	Ext	File Type	Category	Subject	Cr Date	Mod Date
□ DriveFreeSpace1	Disk1\NONAME-Unknown\DriveFreeSpace1			Drive Free S...	Slack/Free S...		N/A	N/A
□ DriveFreeSpace2	Disk1\NONAME-Unknown\DriveFreeSpace2			Drive Free S...	Slack/Free S...		N/A	N/A
□ DriveFreeSpace3	Disk1\NONAME-Unknown\DriveFreeSpace3			Drive Free S...	Slack/Free S...		N/A	N/A
□ DriveFreeSpace4	Disk1\NONAME-Unknown\DriveFreeSpace4			Drive Free S...	Slack/Free S...		N/A	N/A
□ DriveFreeSpace5	Disk1\NONAME-Unknown\DriveFreeSpace5			Drive Free S...	Slack/Free S...		N/A	N/A

5 Listed | 0 Checked Total | Disk1\NONAME-Unknown\DriveFreeSpace1

c. Tampilannya sama seperti HxD utility yang digunakan pada project sebelumnya. Bisa dilihat, file kosong – bukan merupakan file sebenarnya, karena tidak ada header atau footer atau file name atau data di dalamnya. FTK hanya memecah empty space up ke dalam chunks (bagian) yang disebut 'Files" untuk menanganinya.

d. Untuk melihat disk benar-benar kosong, lihat ke "File Status" dan "File Category" kolom di bagian kiri atas jendela FTK. Bisa dilihat FTK tidak bisa menemukan data yang berguna pada format disk—benar-benar kosong.

Mengirimkan Project

10. Kirim melalui elearning.