JAIN DEEMED-TO-BE UNIVERSITY
SCHOOL OF COMPUTER SCIENCE AND IT

COMPUTER FORENSIC AND INVESTIGATION

16BCA5CD11

Credits: 4

(ISMA) – 5th SEM

Module-2

LECTURE : 4

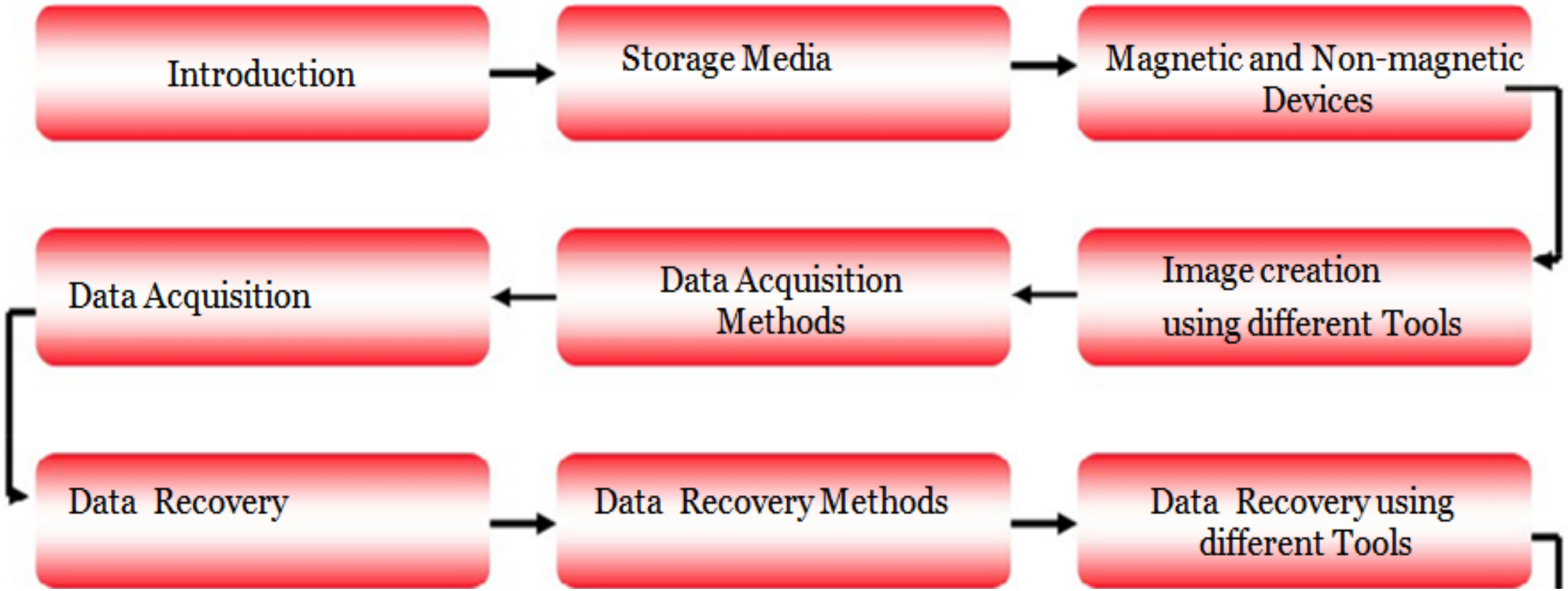
PRACTICAL: 0

TUTORIAL : 0

DISCIPLINE SPECIFIC ELECTIVE (DSE) - 2

Ajay Shriram Kushwaha

Agenda


Introduction
Storage Media
Magnetic and Non-magnetic Devices
Image creation using different Tools
Data Acquisition Methods
Data Acquisition
Data Recovery
Data Recovery Methods
Data Recovery using different Tools

Storage Media

ExpressCare module

CD or DVD

Internal hard disk

External hard disk

Microfilm

Miniature hard disk

Storage

USB flash drive

PC card

Smart card

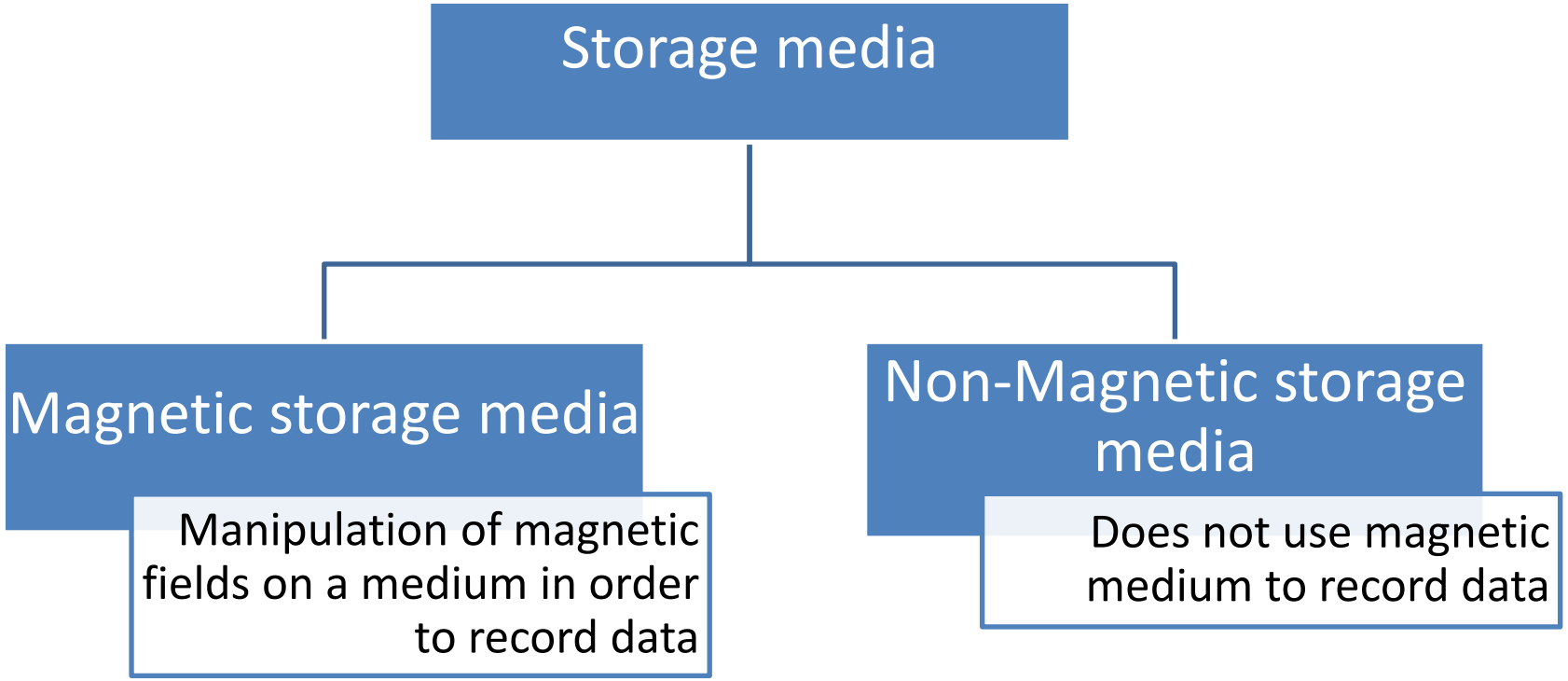
Flash memory card

A variety of storage media

Types of Storage Media Devices

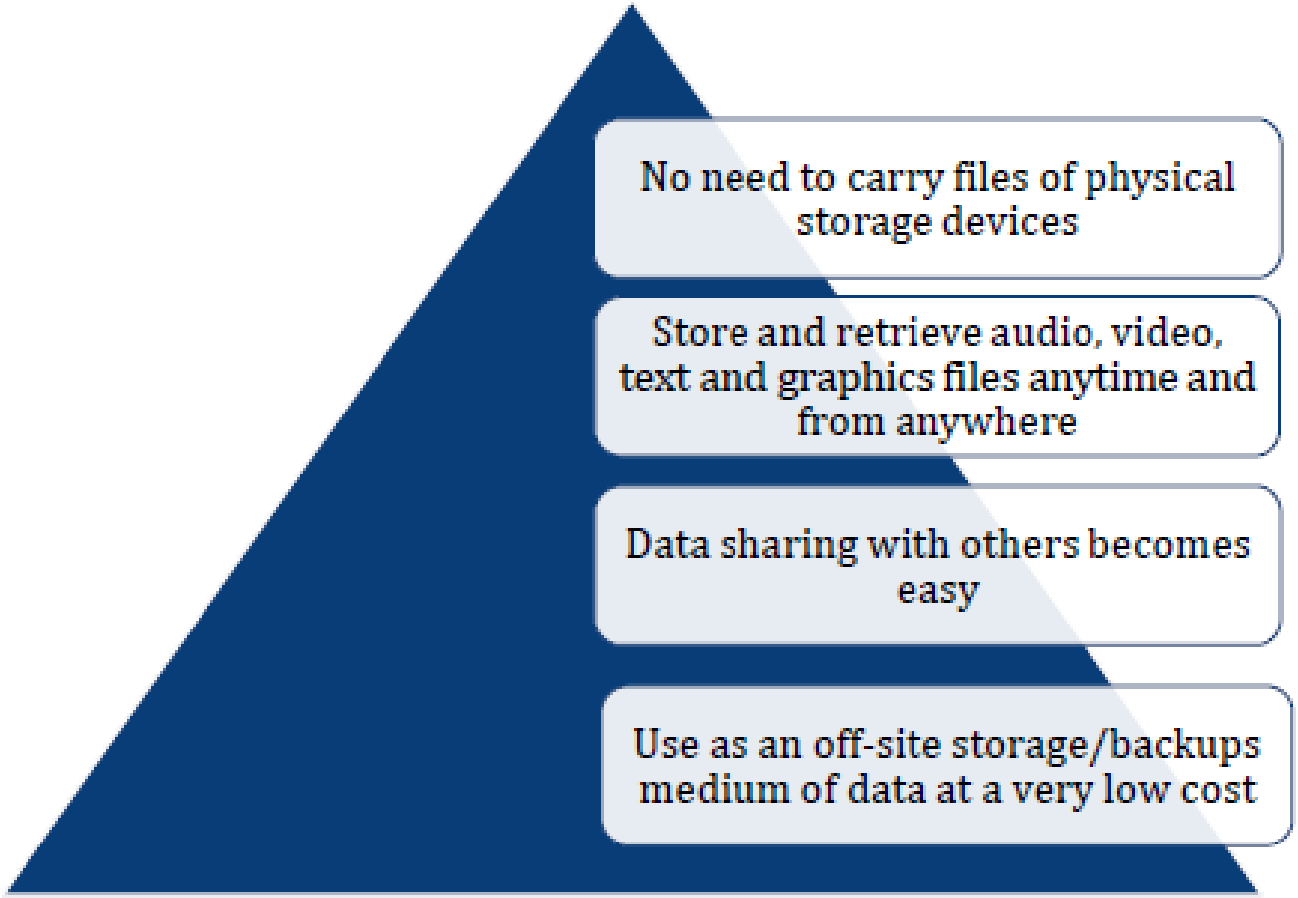
Storage Media

In a computer, storage is the place where data is held in an electromagnetic or optical form for access by a computer processor



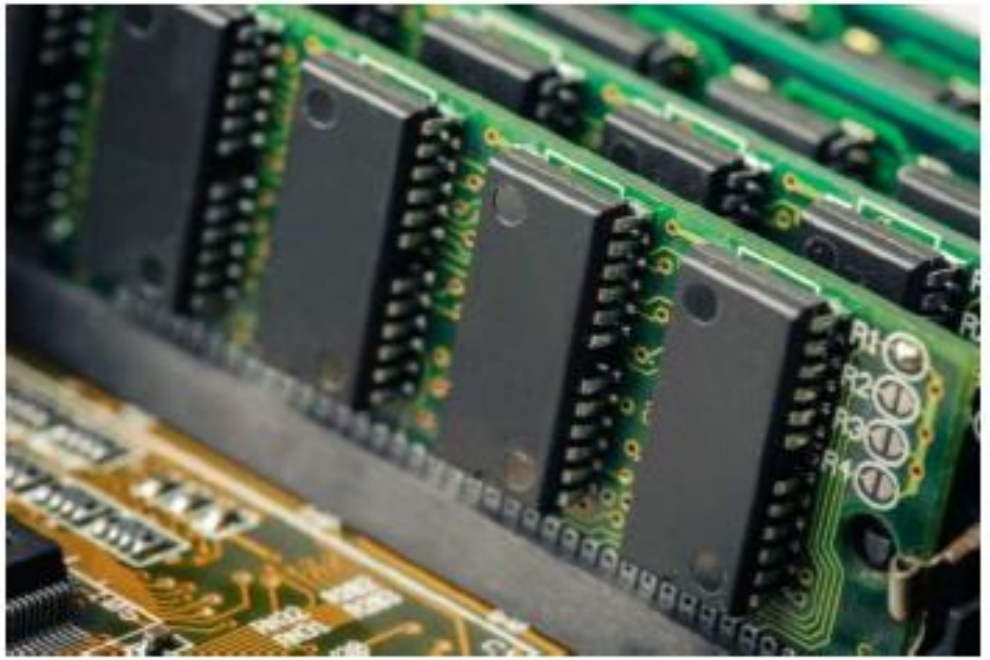
Cloud Based Storage

Advantages



Random Access Memory

RAM is a very fast and volatile storage media as the data within will be lost when powered off.



Random Access Memory

Magnetic Medium

Magnetic storage devices uses different encoding patterns of magnetization on a specific magnetic material to store data.




Hard disc	Floppy Disc	Tape drives	Magnetic stripes

Example : Magnetic Storage Media

Tape drives

Contains a magnetically-coated plastic ribbon and is capable of storing large volume of data at a low cost

Tape drives

Contains a magnetically-coated plastic ribbon and is capable of storing large volume of data at a low cost

Examples

- Magnetic storage media
  - HDD (Hard Disk Drive)
  - Floppy Drive
  - Data Tape storage

- Non-Magnetic storage media
  - SSD (Solid State Drive)
  - USB drive
  - CD

Hard Disks

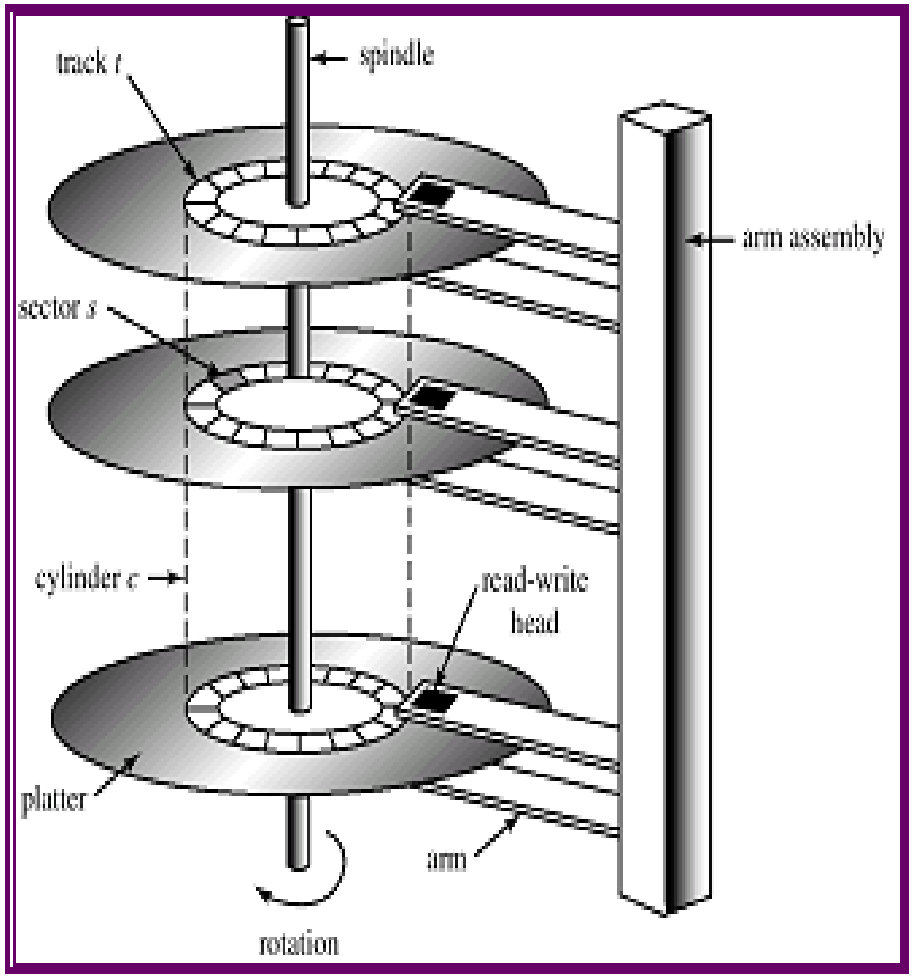
Hard Disks

- The **Hard drive** is the computer's main storage media device that permanently stores all data on the computer
- The data is recorded magnetically on to the hard disk
- The main component of hard disk
  - Cylinder
  - Head
  - Platters
- A high speed spindle platter is used as a recording media and the data is stored on the tacks of the sector

Hard Disks

Components of Hard Drive

- Actuator: Moves read and write arm
- Read/Write Arm: Swings rear and write head back and forth across platter
- Spindle: Central spindle allows platter to rotate at high speed
- Magnetic Platter: Stores information in binary form
- Plug Connection: Link hard drive to circuit board in persona computer
- Read/Write Head: Tiny magnet on the end of read and write arm
- Circuit board: On underside controls the flow of data to and from the platter
- Flexible connector: Carries data from circuit board to read/write head and platter
- Small Spindle: Allows read/write arm to swing across platter



Read/Write Operations

- Data's are stored with ordered manner in circular paths called **Tracks.**
- Tracks will be fragmented to store data is called **sectors.**
- Map of Sectors**:** Will be stored in **FAT**(File Allocation table)which will have the used space of hard drive and free space.
- By referring to the FAT the **Read/Write head** will do the process accordingly.

Drawbacks & Comparison

- Amount of time takes to read/write head to get itself to the right part of disk for accessing in huge
- Hard drive head crash leads to failure of R/W operation in hard drive
- Heavy power consumption

Parameters	HDD	SSD
Access Time	10ms	0.1ms
Read Speed	50-100	200-500
Weight	500g	50g
Power	6w	2-3W

Non-Magnetic Storage

- Solid-state drive (SSD)
- Flash memory card
- USB flash drive
- Optical media (DVD, CD and BlueRay)
- Punch cards

Solid State Drive

- NAND logic gates
- Non-volatile Storage devices
- Used to store persistence data on solid-state flash memory
- Has an array of semiconductor memory organized as a disk drive, using integrated circuits (ICs) rather than magnetic or optical storage media
- Performance is fast
- Lower latency
- Supports all format

Optical Storage Devices

Optical storage is a term from engineering referring to the storage of data on an optically readable medium

Types of optical storage devices

- CD (Compact disk)

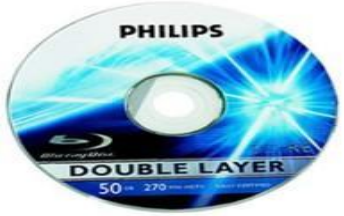
  - Up to 700 MB of Storage

- DVD (Digital Versatile Disk)

  - Up to 4.7 GB of Storage

- Blu-ray Disk

  - UP to 25 GB of Storage



USB Storage

USB Drive Working Principle

- Pen drive usually consists of a PCB (printed circuit board) with a USB connector, power circuitry and a number of integrated circuits (ICs).
- One of the IC in the PCB provides an interface between the memory and the USB connector.
- The next IC is a NAND flash memory where all the files are stored.
- Pen drive or the USB flash drive uses the PCB as the means of transferring the data and power from the USB
- Controller chip is considered to be the brain of pen drive

Components

- USB Connector: It acts as an interface between the NAND flash memory chip and the computer to which the pen drive is plugged
- USB mass storage controller (or the controller chip): This chip helps to retrieve the information from the pen drive and it also helps in recording/reading the information on the NAND flash memory. It is basically a microcontroller with on-chip RAM and ROM
- **Test points:** They are electric pins used to stimulate and exercise the pen drive during assembly process.
- **NAND flash memory chip:** Helps in the storage of files and all data's. Also it allows the erasing the information so that we can delete files and put new files into the pen drive.
- Crystal Oscillator: It is a piece of quartz crystal designed to vibrate at a very particular frequency.
- LED: Used to indicate if the flash drive is working properly.
- Write-protect switch: An optional component used to safeguard the information saved on the flash drive
- **Space to put a second NAND flash memory chip:** Additional slot to put another memory chip which can increase the storage capacity.

Data Acquisition

Data Acquisition

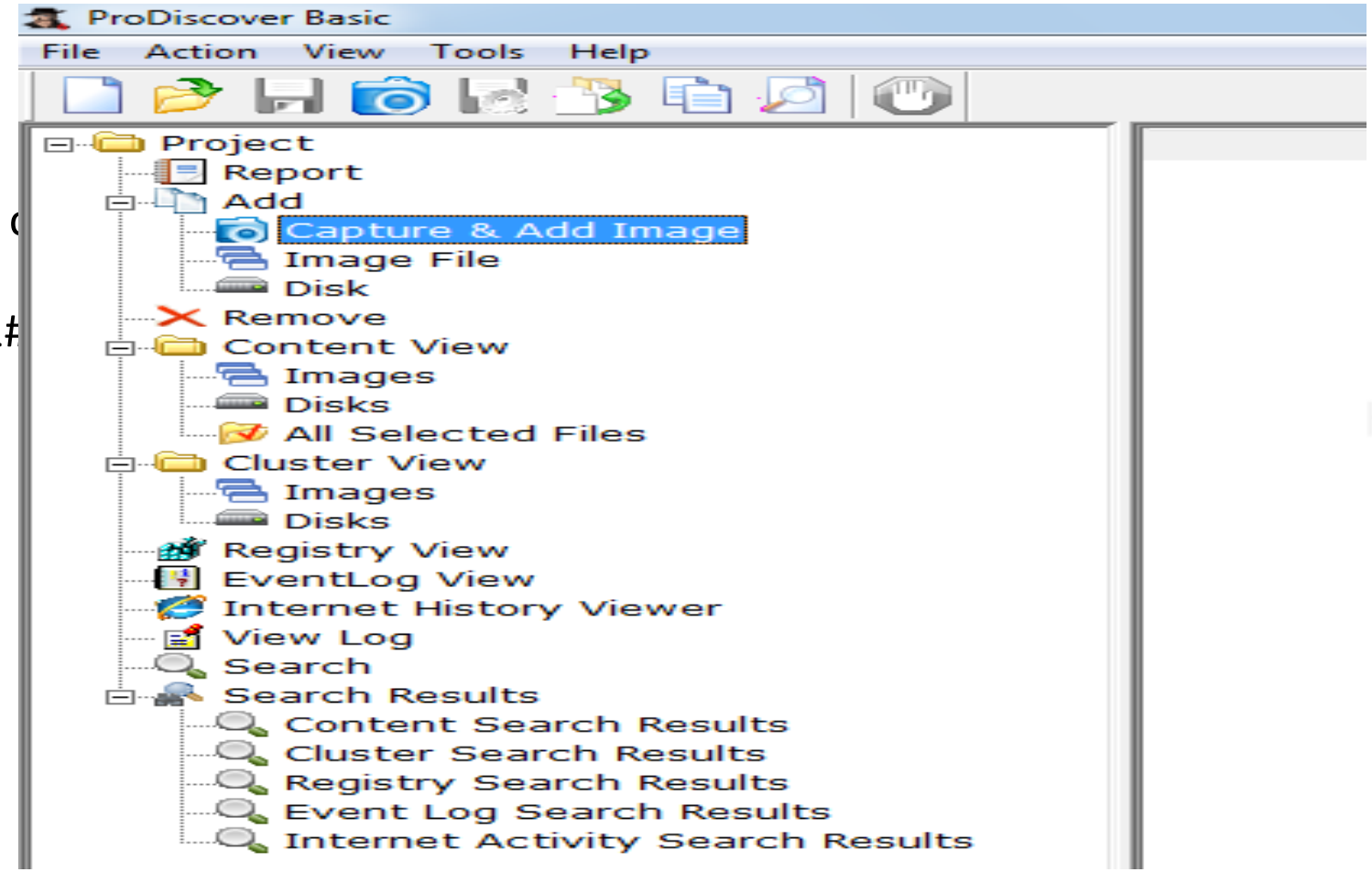
Data acquisition is the process of imaging or obtaining control of data and adding it to a collection of evidence.

- **Types of acquisitions**
  - **Static acquisitions** and **live acquisitions**
- Four methods
  - Bit-stream disk-to-image file
  - Bit-stream disk-to-disk
  - Logical disk-to-disk or disk-to-disk data
  - Sparse data copy of a file or folder

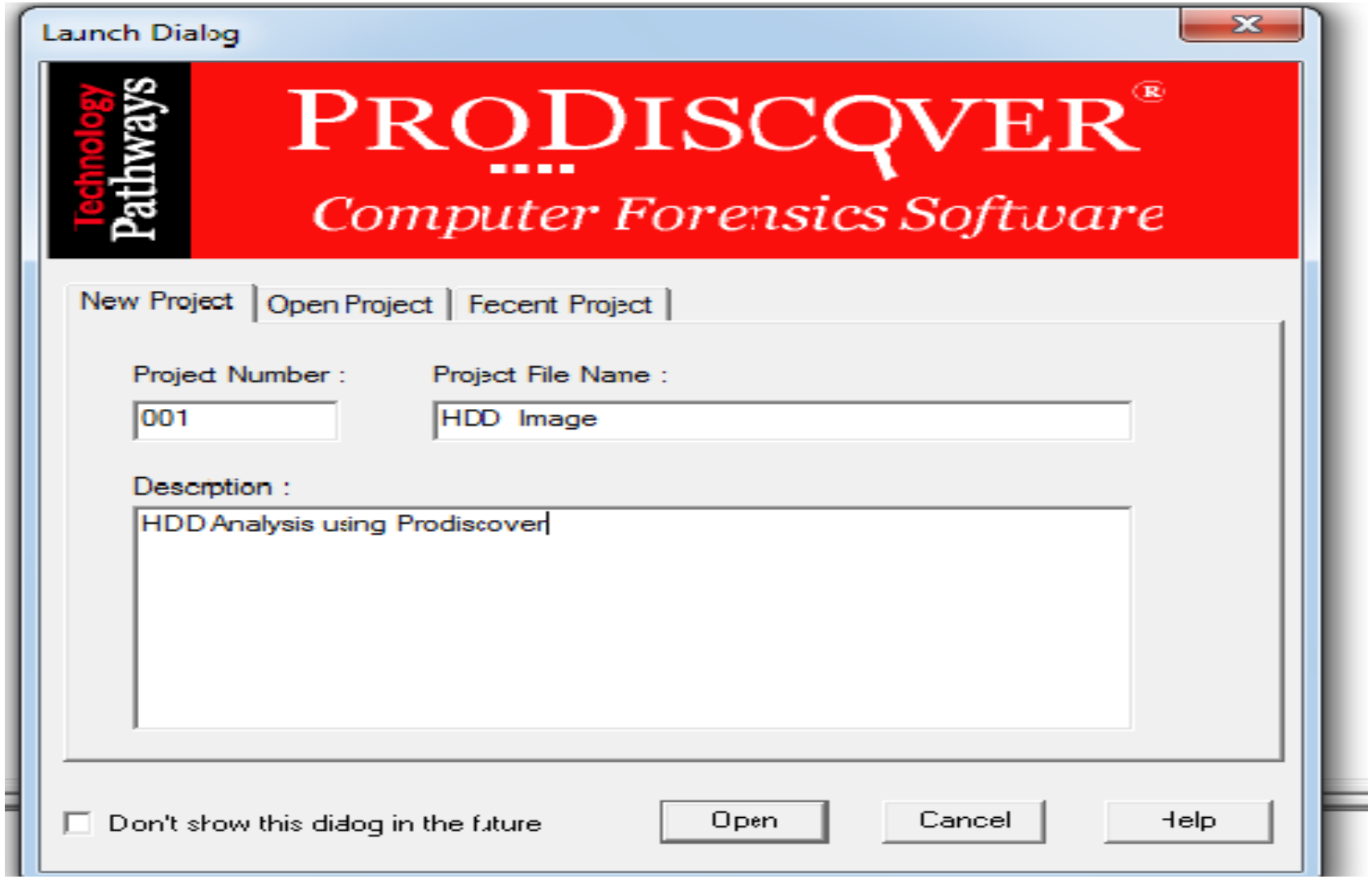
How to create Disk Image with different Tools

To c

R1#


ProDiscover Basic
File
Action
View
Tools
Help
Project
Report
Add
Capture & Add Image
Image File
Disk
Remove
Content View
Images
Disks
All Selected Files
Cluster View
Images
Disks
Registry View
EventLog View
Internet History Viewer
View Log
Search
Search Results
Content Search Results
Cluster Search Results
Registry Search Results
Event Log Search Results
Internet Activity Search Results

here


Launch Dialog
Technology Pathways
PRODISCOVER®
Computer Forensics Software
New Project
Open Project
Fecent Project
Project Number :
001
Project File Name :
HDD Image
Description :
HDD Analysis using Prodiscover
Don't show this dialog in the future
Open
Cancel
Help

- Click on capture and Add Image

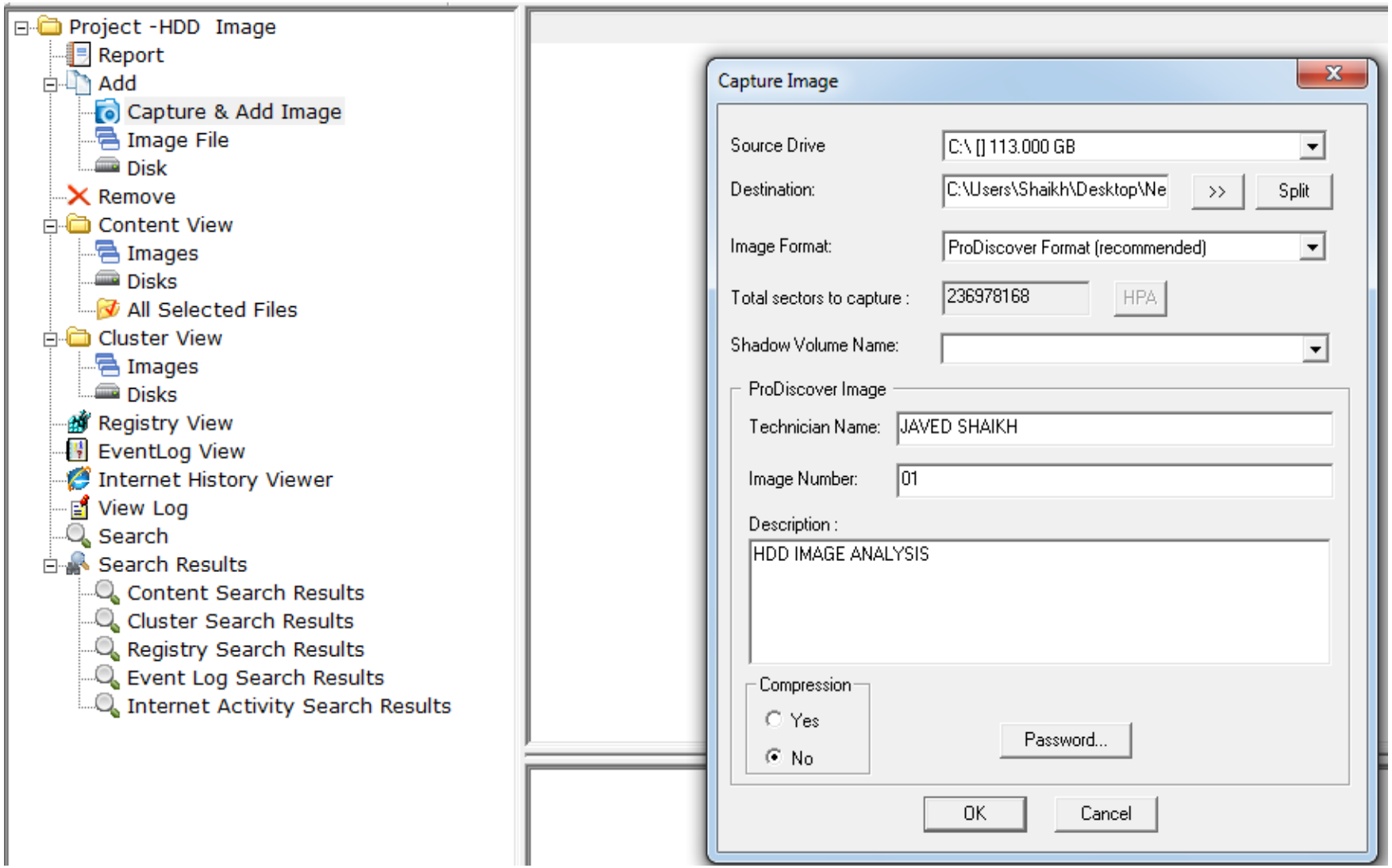


Image Creation using FTK Imager

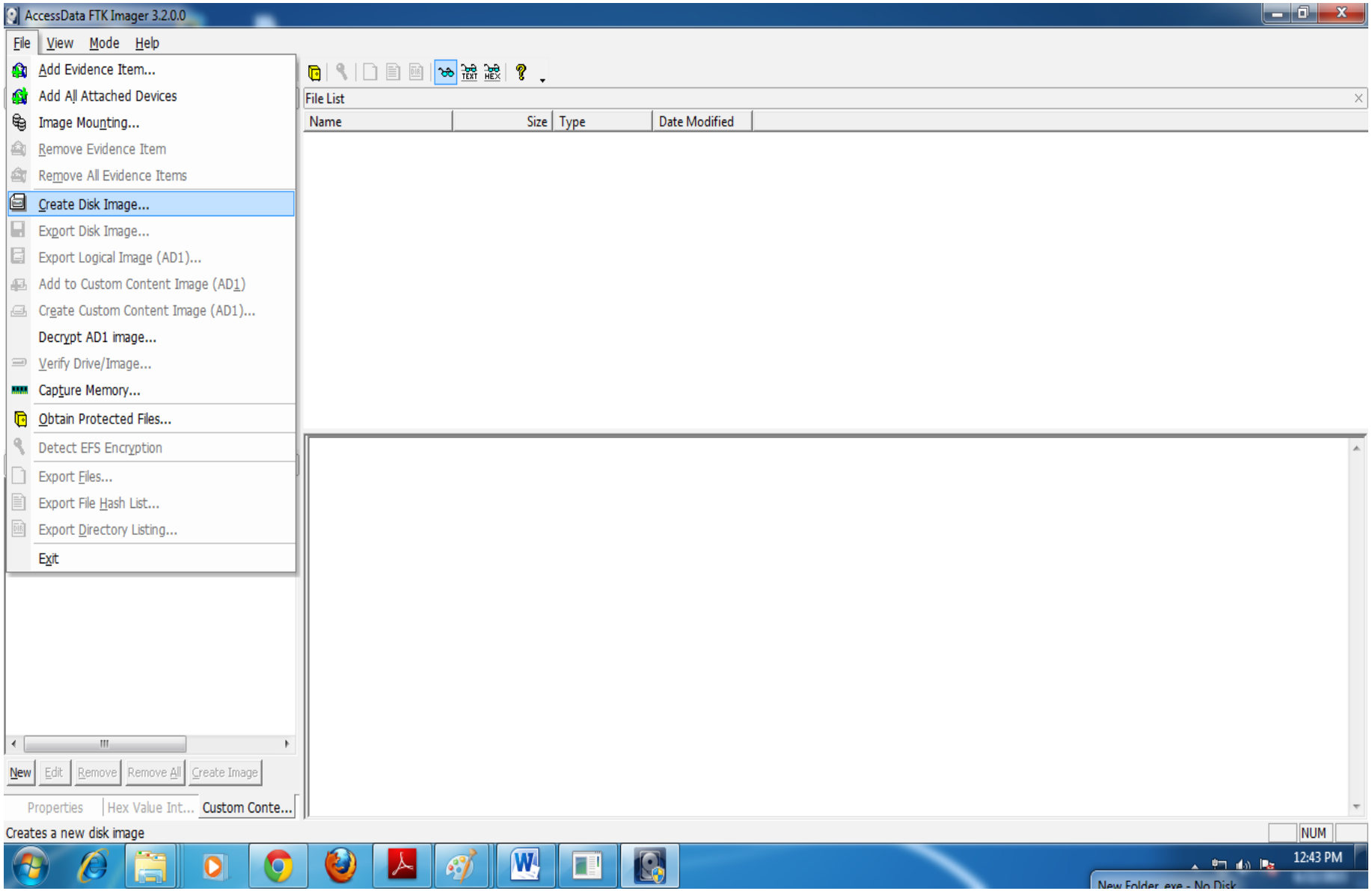
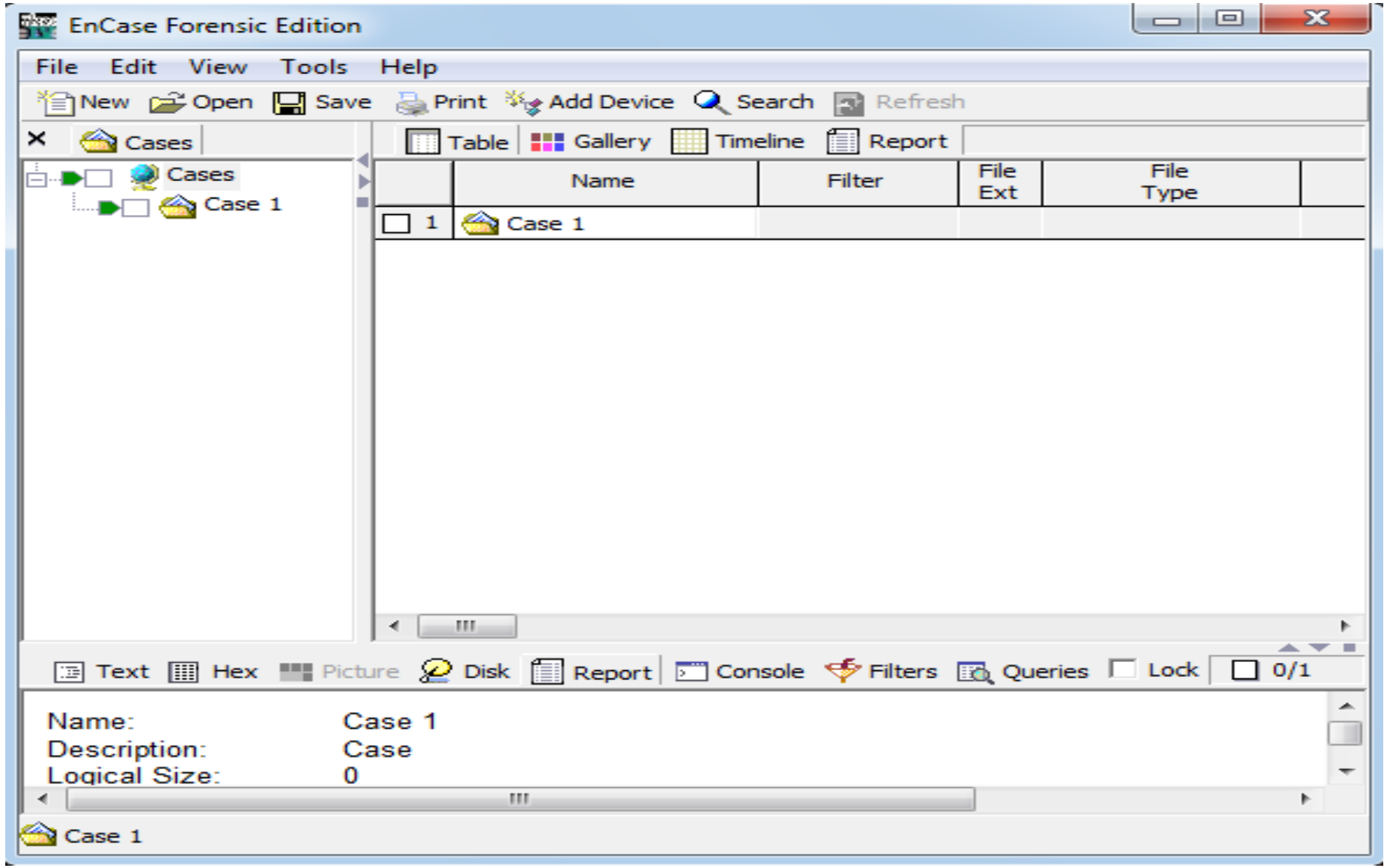


Image Creation using Encase



Data Recovery & its methods

What is Data Recovery?

- The forensic acquisition in full or in part of data stored on non-functioning storage media through the use of sophisticated equipment and techniques for the purpose of presenting the data in a legal forum

- Retrieving deleted/inaccessible data from electronic storage media (hard drives, removable media, optical devices, etc...)

- Typical causes of loss include:
  - Electro-mechanical Failure
  - Natural Disaster
  - Computer Virus
  - Data Corruption
  - Computer Crime
  - Human Error

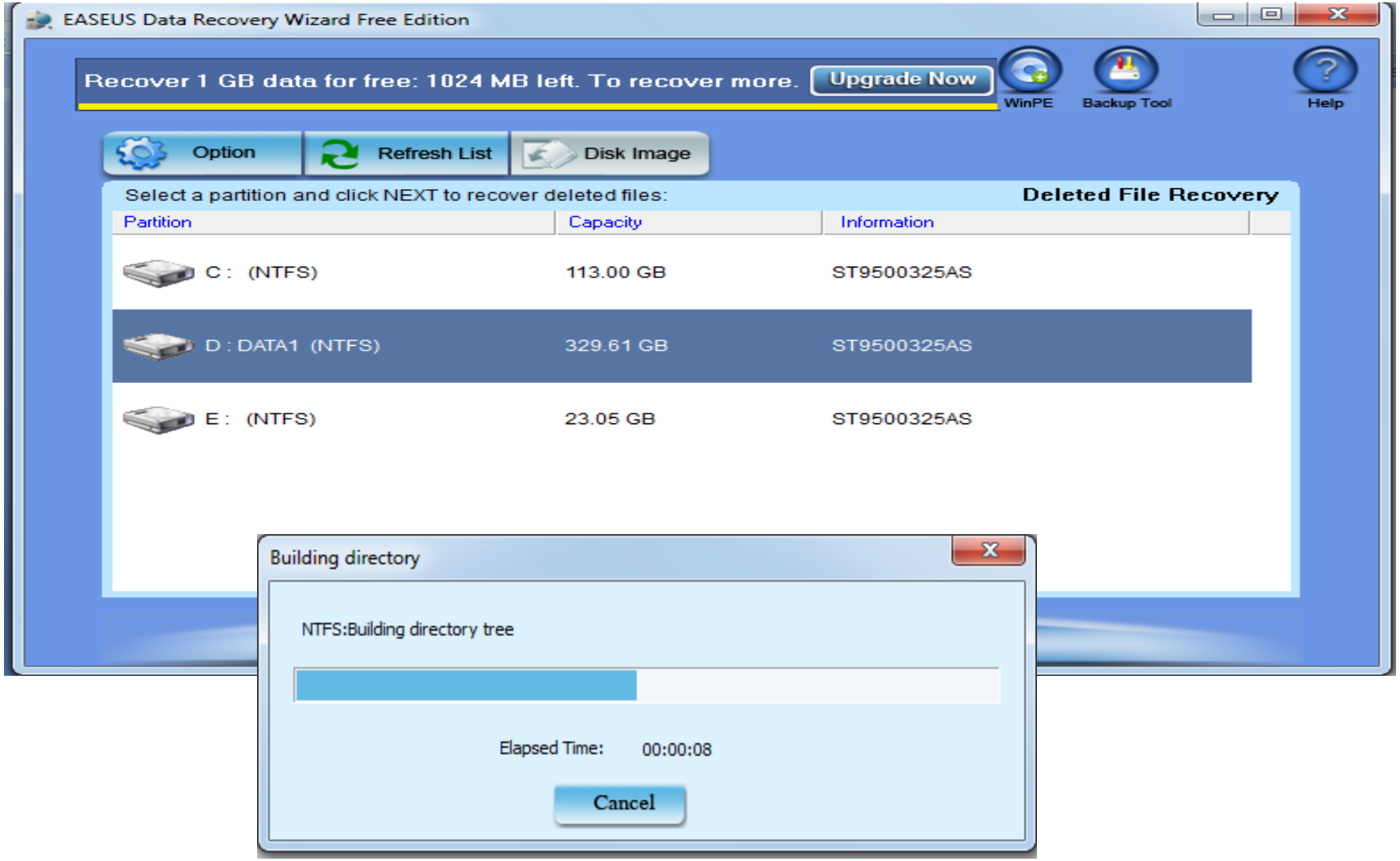
Recovery Methods

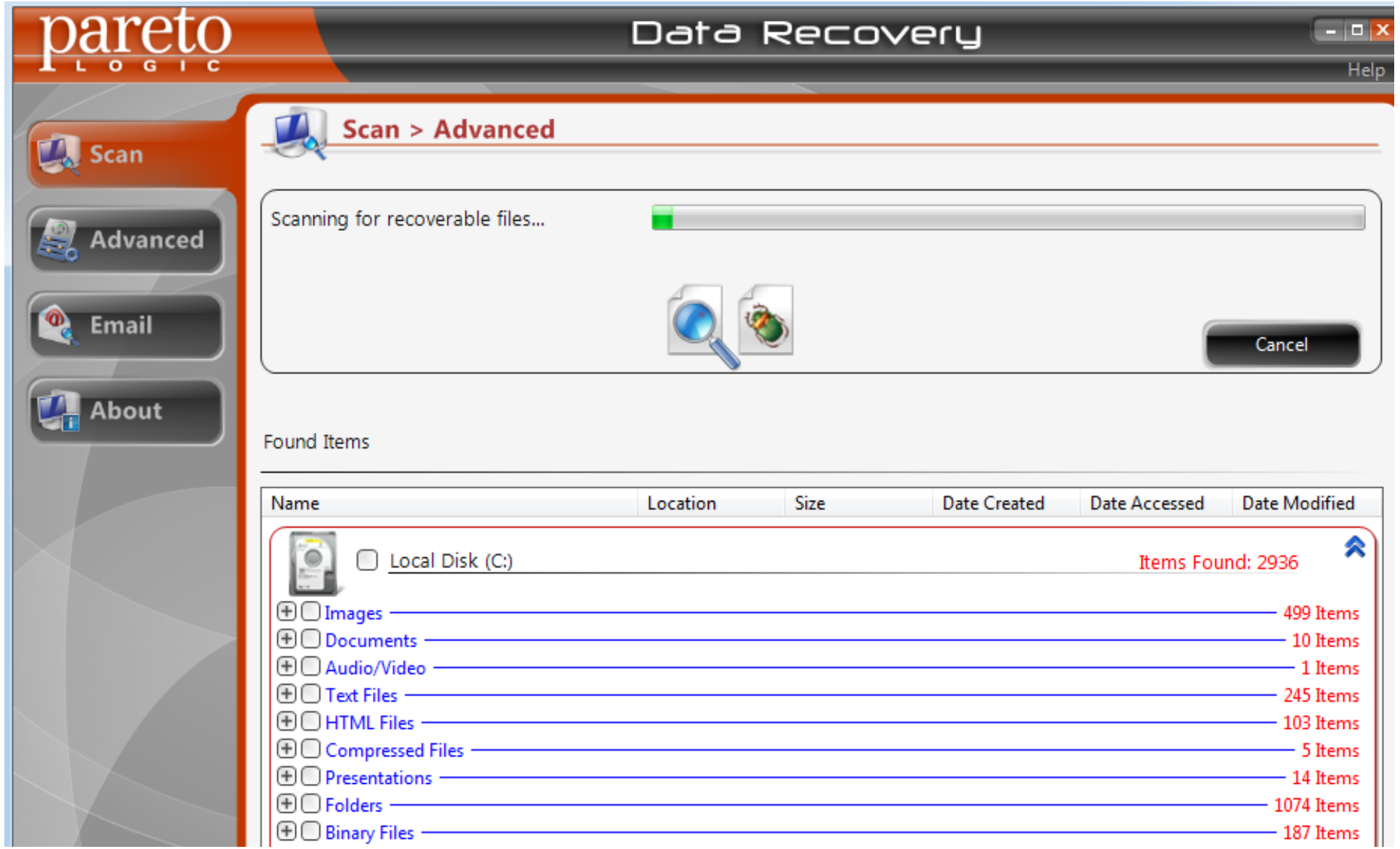
- Hidden files
- Recycle bin
- Unerase wizards
- Assorted commercial programs
- Ferrofluid
  - Coat surface of disk
  - Check with optical microscope
  - Does not work for more recent hard drives

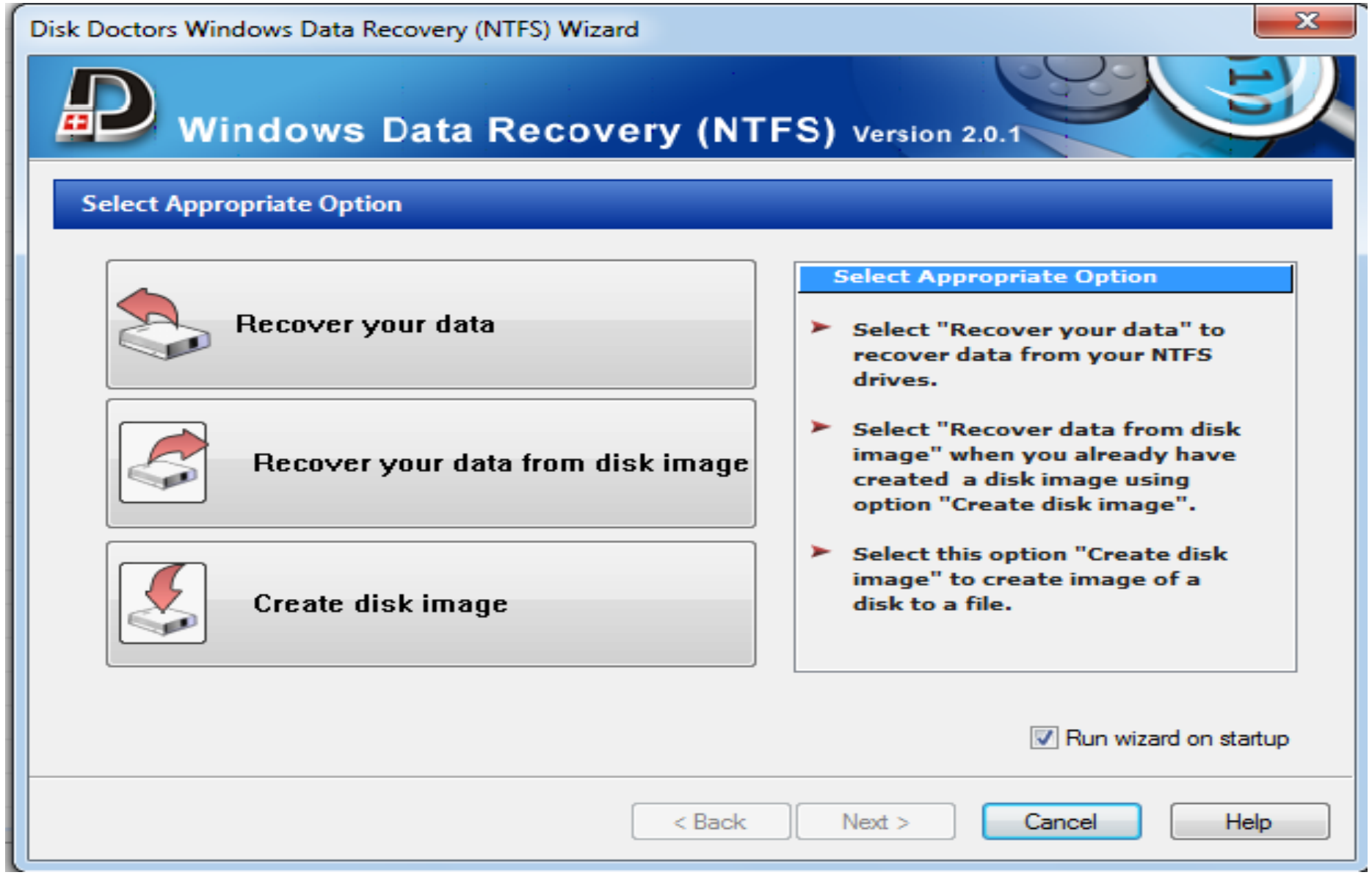
Tools for Data Recovery


EASEUS Data Recovery Wizard Free Edition
EASEUS Data Recovery Wizard Free
WinPE
Backup Tool
Language
Help
Recover 1 GB data for free: 1024 MB left. To recover more.
Upgrade Now
Choose a mode to start recovery:
Deleted File Recovery
Complete Recovery
Partition Recovery
Data Recovery Wizard Free Edition V5.5.1
Data Recovery Wizard helps you to recover data due to deletion, format, partition loss, software crash, virus attack, etc.

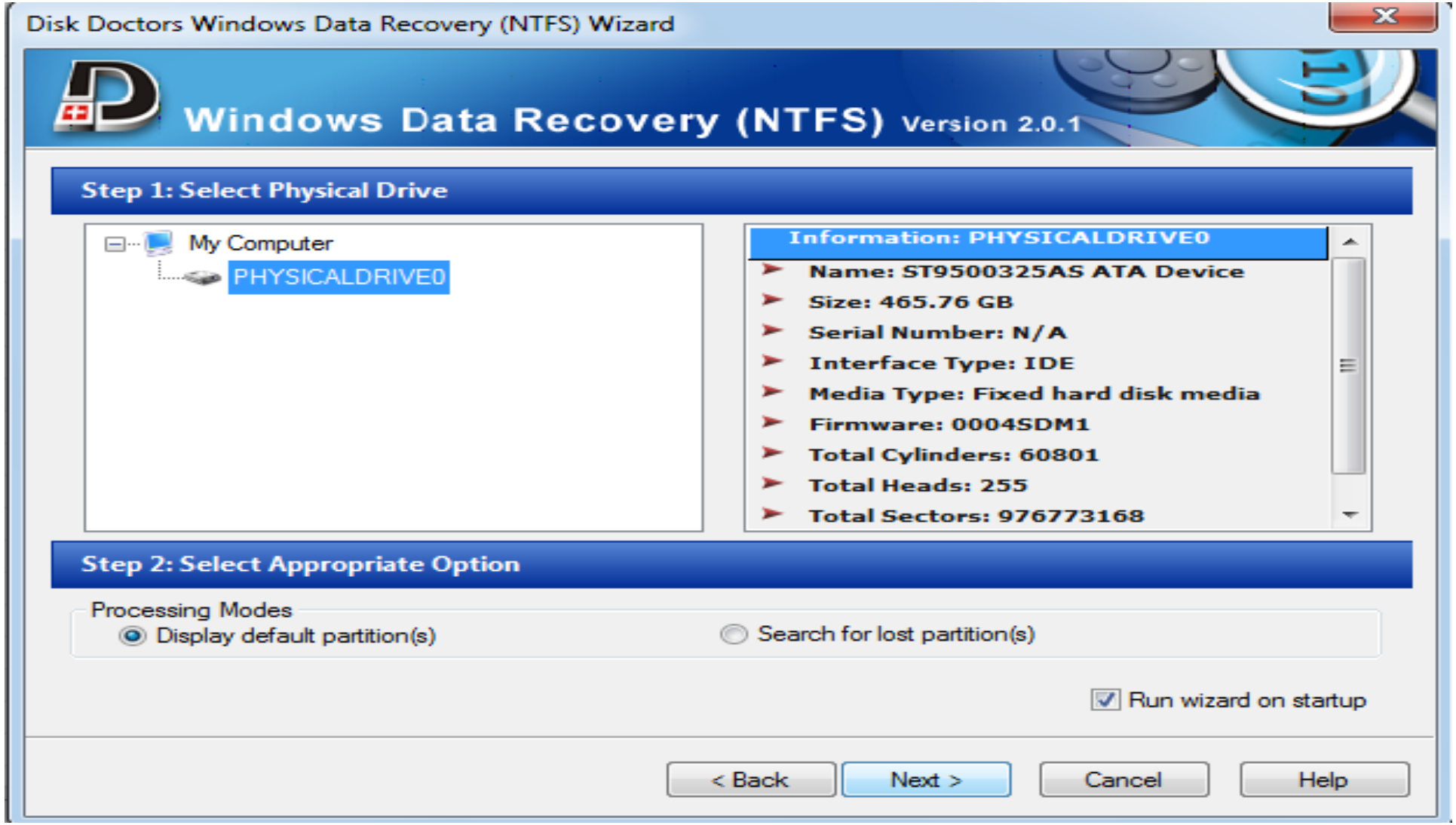
- Select Drive



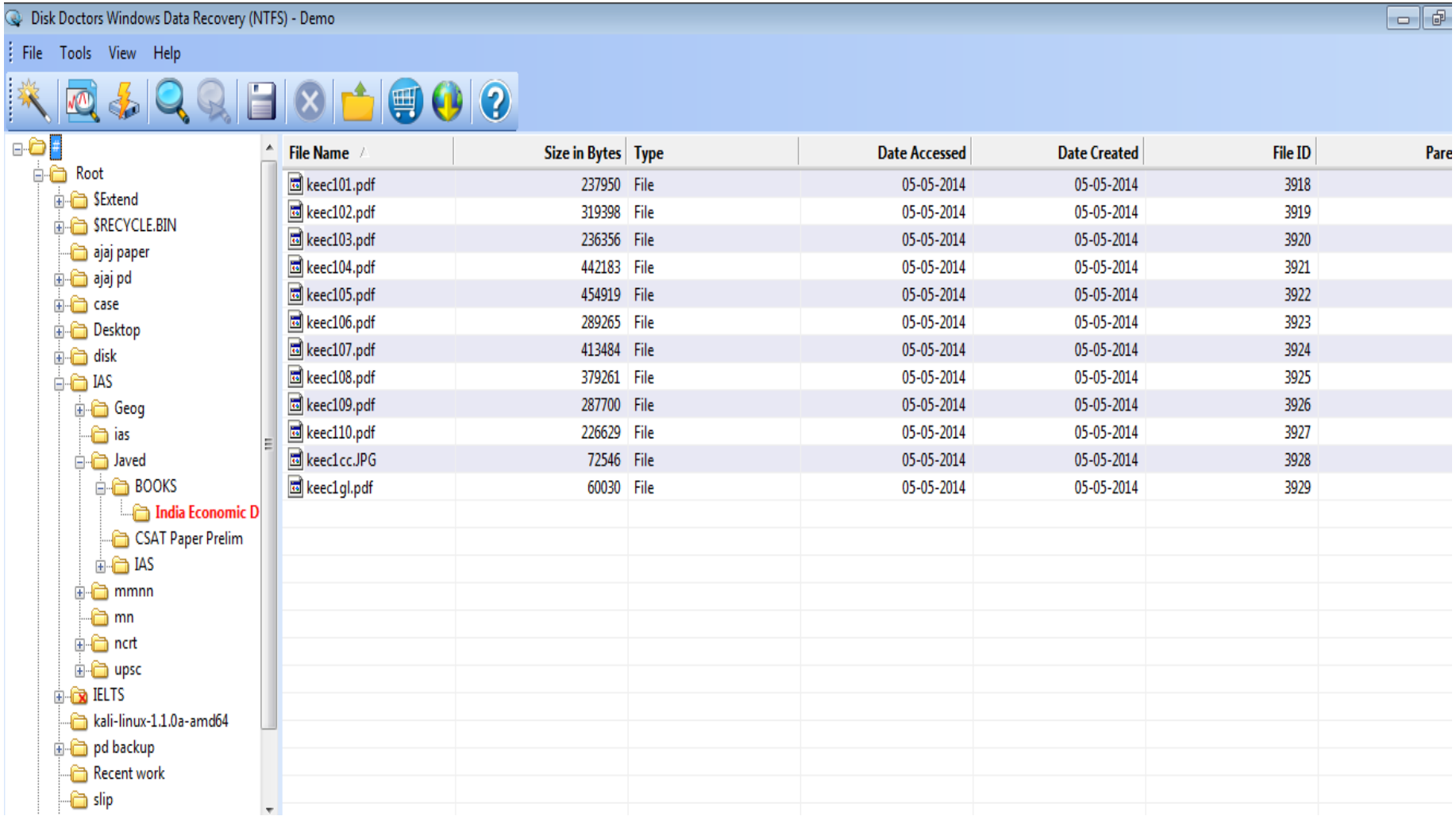

pareto LOGIC
Data Recovery
Help
Scan
Advanced
Email
About
Scan > Advanced
Scanning for recoverable files...
Cancel
Found Items
Name
Location
Size
Date Created
Date Accessed
Date Modified
Local Disk (C:)
Items Found: 2936
Images 499 Items
Documents 10 Items
Audio/Video 1 Items
Text Files 245 Items
HTML Files 103 Items
Compressed Files 5 Items
Presentations 14 Items
Folders 1074 Items
Binary Files 187 Items


Disk Doctors Windows Data Recovery (NTFS) Wizard
Windows Data Recovery (NTFS) Version 2.0.1
Select Appropriate Option
Recover your data
Recover your data from disk image
Create disk image
Select Appropriate Option
Select "Recover your data" to recover data from your NTFS drives.
Select "Recover data from disk image" when you already have created a disk image using option "Create disk image".
Select this option "Create disk image" to create image of a disk to a file.
Run wizard on startup
< Back
Next >
Cancel
Help

- Click on Recover your data, on right side you will find the specification



- Analyzed the file tree



File Name	Size in Bytes	Type	Date Accessed	Date Created	File ID	Pare
keec101.pdf	237950	File	05-05-2014	05-05-2014	3918	
keec102.pdf	319398	File	05-05-2014	05-05-2014	3919	
keec103.pdf	236356	File	05-05-2014	05-05-2014	3920	
keec104.pdf	442183	File	05-05-2014	05-05-2014	3921	
keec105.pdf	454919	File	05-05-2014	05-05-2014	3922	
keec106.pdf	289265	File	05-05-2014	05-05-2014	3923	
keec107.pdf	413484	File	05-05-2014	05-05-2014	3924	
keec108.pdf	379261	File	05-05-2014	05-05-2014	3925	
keec109.pdf	287700	File	05-05-2014	05-05-2014	3926	
keec110.pdf	226629	File	05-05-2014	05-05-2014	3927	
keec1cc.JPG	72546	File	05-05-2014	05-05-2014	3928	
keec1gl.pdf	60030	File	05-05-2014	05-05-2014	3929	

Volatile Memory

- **Volatile memory** is computer storage that only maintains its data while the device is powered. Most **RAM** (random access **memory**) used for primary storage in personal computers is **volatile memory**.

Memdump(Farmer & Venema,1999) is a free tool that runs on many different systems, including windows,Linux,and salaris.It is easy to download,compile,and use, and is very straightforward in its functinality;it simply creates a bit-by-bit copy of the volatile memory on a system.

KnTTools(GMG Systems, Inc.,2007) is a memory acquisition and analysis tool that was created for use with windows systems. The Acquisition component,KnTDD can capture the physical memory and store it to a removable drive or send it over the network for archival on a separate machine.

FAT Kit, Developed by Petroni, Walters, Fraser , and Arbaugh.,2006), is a popular memory forensic tool that automates the process of extracting interesting data from volatile memory. FAT Kit is its ability to detect malicious code that residing in volatile memory.

The windows Memory Forensic Toolkit(WMFT) Supports the analysis of memory images from machines running windows 2000, windows 2003, and windows XP. There is also a Linux version available, but its functionality is currently somewhat limited in comparison with the windows version.

Summary

- Roles & Responsibilities
- Characters involved in governance
- Different roles by Management level
- Relationship of outcome with management directives
- Role of IT Strategy Committee and Steering Committee
- IT Balanced Scorecard
- Val-IT Framework and COBIT
- Importance of Governance in establishing a sustainable Security Culture in the organization

Feel Free to ask for Any query

Ajay Shriram Kushwaha