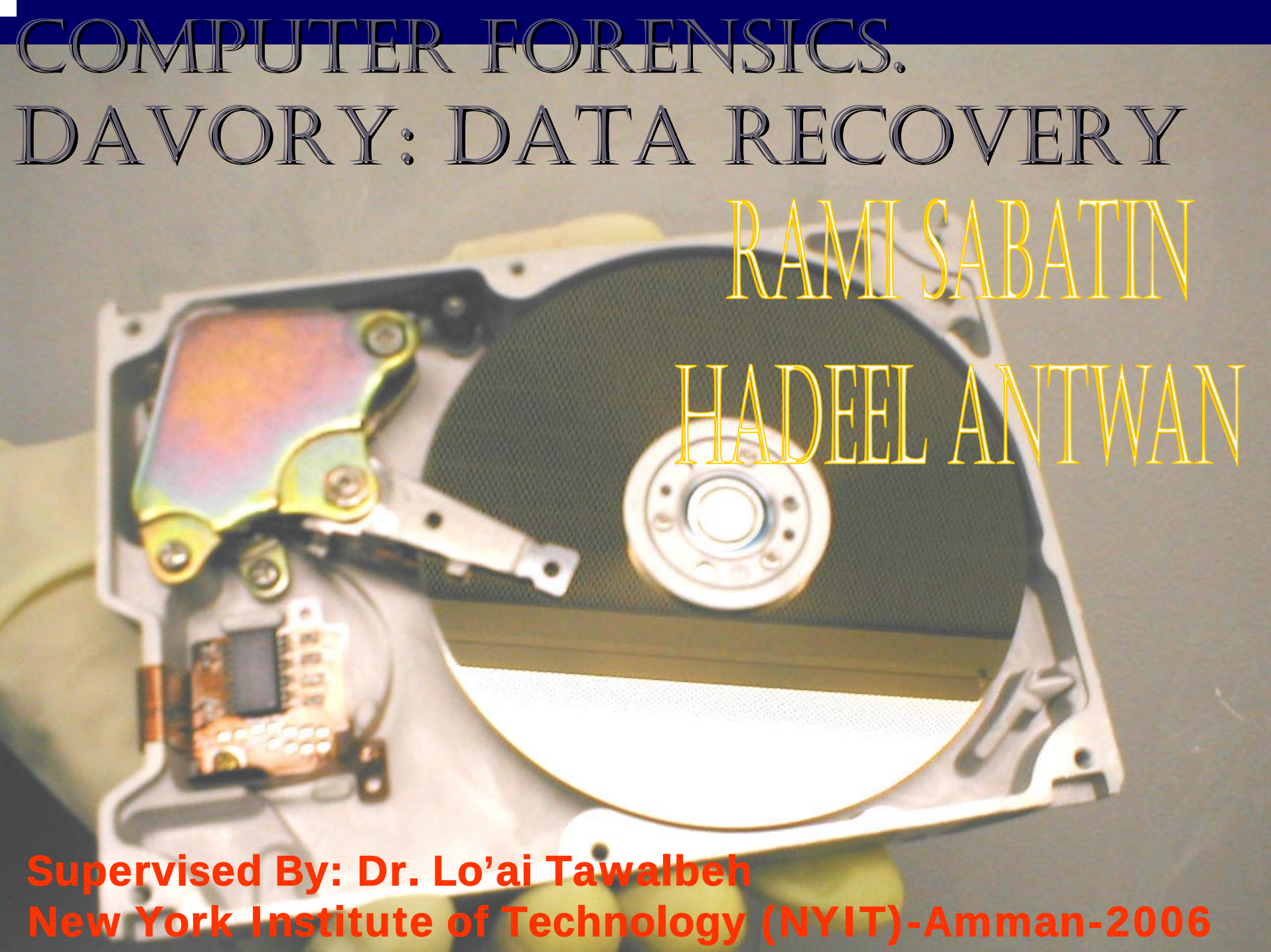
# COMPUTER FORENSICS.
# DAVORY: DATA RECOVERY




RAMI SABATIN

HADEEL ANTWAN

**Supervised By: Dr. Lo'ai Tawalbeh**

**New York Institute of Technology (NYIT)-Amman-2006**

# TOPICS

- Definition
- Recovery from what ??
- Davory SOFTWARE.
- Restore Software.

# INTRODUCTION

- There are many factors that make data loss :

Natural disaster.

Computer virus.

Data corruption.

Computer crime.

Human errors or bad use of Information.

Hint: "lost" data is not lost at all; it has simply become inaccessible to the user.

# DEFINITION

Data Recovery : The process of recovering deleted information from a storage media for forensic purposes.

Another Def:

is the process of salvaging data from damaged, failed, wrecked or inaccessible primary storage media when it cannot be accessed normally

# RECOVERY FROM WHAT

1) Deleted data
2) Overwritten data
3) Physical damage
4) Logical damage

# DELETED DATA

- When a file is deleted from an operating system such as Windows and removed from the recycle bin, the data is not gone. The O.S simply removes the pointer and does not touch the actual data.
- Then the space allocated for the file is then made available as free space, so new data may be written to that same space.
- Before this is done, the data is still intact and can be recovered by a variety of different data recovery software.

# OVERWRITTEN DATA

- Data is recorded onto magnetic media by writing a pattern binary (ones and zeroes).
- These patterns are read back by the disk and interpreted by the operating system as text, executables, pictures or whatever the data may represent.

# PETER GUTMANN CLAIMING

- Peter Gutmann suggests that even data overwritten can be recovered by using equipment and methods such as

-Electron microscopes

-Image analysis

because the changes that occur when new data is written can reveal previous information .

Note:It should also be noted that no data recovery company today can recover *overwritten* information.

# PHYSICAL DAMAGE

- wide variety of failures can cause physical damage to storage media.
- CD-ROMs can have their metallic substrate or dye layer scratched off;
- Hard disks can suffer any of several mechanical failures, such as head crashes and failed motors;
- tapes can simply break. Physical damage always causes at least some data loss

# LOGICAL DAMAGE

- Logical damage caused by power outages that prevent file system structures from being completely written to the storage medium .
- Power outages may lead to strange behavior like:

- Infinitely repeat directories
- Drives reporting negative amounts of free space
- System crashes, or an actual loss of data .

# MOST O.S COME WITH REPAIR TOOL

- Linux comes with the fsck utility.
- Mac OS X has Disk Utility.
- Microsoft Windows provides check disk .

# Two main techniques are used by repair programs

- consistency checking

Involves scanning the logical structure of the disk to make sure that it is consistent with its specification .

- Directory must have at least two entries:

dot (.) entry that points to itself

dot-dot (..) entry that points to its parent

# THE SECOND TECHNIQUE

- Is to assume very little about the state of the file system to be analyzed.
- Using any hints that any undamaged file system structures might provide.
- Rebuild the file system from scratch.
- This strategy involves scanning the entire drive and making note of all file system structures and possible file boundaries, then trying to match what was located to the specifications of a working file system

# DAVORY PROGRAM

- Davory undelete files and recovers files from logically corrupted or formatted drives
- Davory works not only on hard drives, floppy disks, CDs, and DVDs, but also on Compact Flash cards, Smart Media cards, memory sticks
- HINT: Davory cannot *repair corrupt* files.

# TWO WAYS TO RECOVER DATA USING DAVORY

- 1) Automatic recovery of files depends on filenames.
- 2) Automatic recovery of files depends on certain type.

# HOW IT WORK

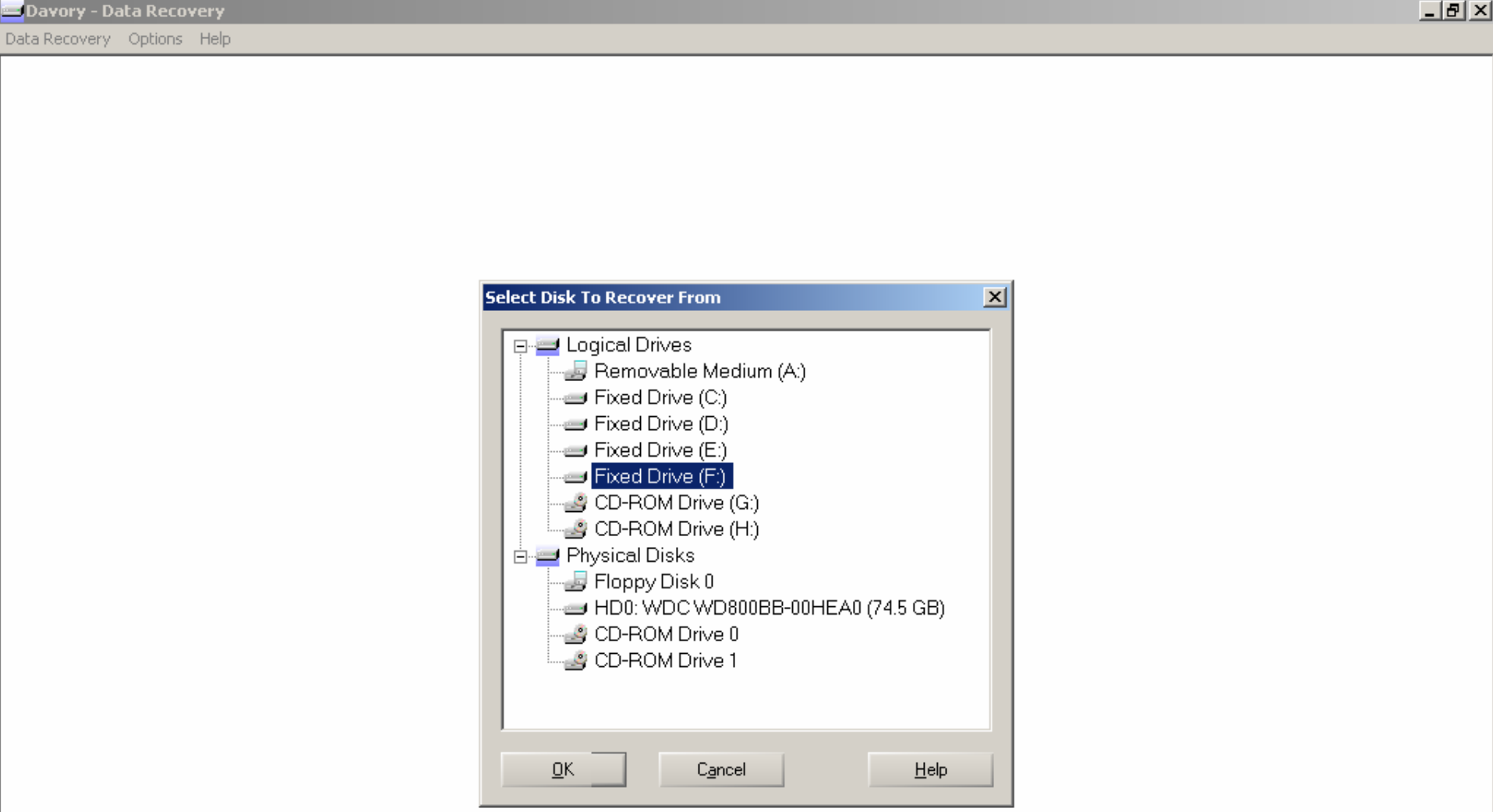
- Davory can be run directly from a floppy disk or CD.
- Davory does not recover files "in same place", it will recreates them on a different drive, so  original drive is not touched except for reading.

# SELECTING THE DISK

- selecting a logical drive ("drive letter" or "volume").
- Selecting a physical disk ("raw device") .

- Note:

  If the disk is not properly formatted, damaged, or if its file system is unknown to Windows, so Windows is unable to make it accessible as a drive letter, select the physical disk instead.




# THE WAY TO SELECT DISK

# LIMITATIONS

- Under Windows NT, 2000, and XP administrator rights are needed to access hard disks.
- Davory cannot operate on remote (network) drives.

# FILE RECOVERY BY NAME

- Works on FAT12, FAT16, FAT32, and NTFS logical drives/partitions.
- You may specify one or more filename patterns that cover all the files you wish to retrieve, e.g:

  Invoice*.pdf

  m*.xls

  Image*.gif

  *.tif

  *.Jpeg

# FILE RECOVERY BY NAME

- note that files that were moved to the recycle to permanent deletion are internally renamed by Windows.
- where only the filename extension remains the same.
- So if you wish to undelete files that were in the recycle bin before, specify only an asterisk before the dot
- "*.jpg"

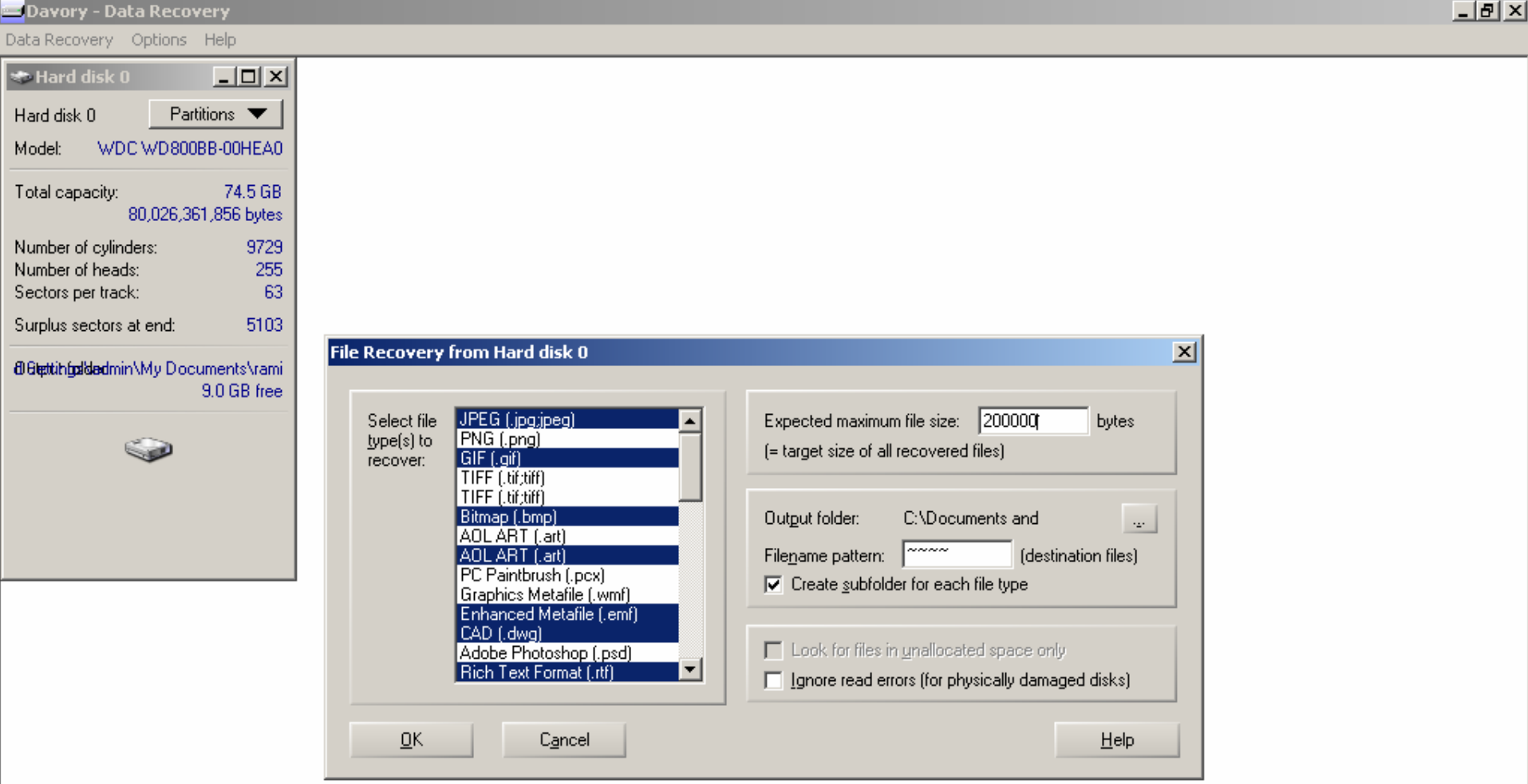
# FILE RECOVERY BY NAME

- Davory will recreate the original folder tree within the output folder and will place recovered files into their respective subfolders.
- Specifying a folder on the same drive where you are recovering from could easily overwrite disk space where deleted files reside that you still wish to recover! That way they would be lost forever.

- Unlike File Recovery by Type, "File Recovery by Name" will also restore the file date & time and its attributes.

# FILE RECOVERY BY TYPE

- Davory tries to detect the original correct size of JPEG, GIF, PNG, BMP, TIFF, AVI, WAV, ZIP, HTML, RTF, and MS Office files automatically.
- If this fails, the files are recovered the fixed maximum size that you specify
- You also specify an output folder where Davory should recreate the original file(s).
- Important: make sure this folder is on a different drive



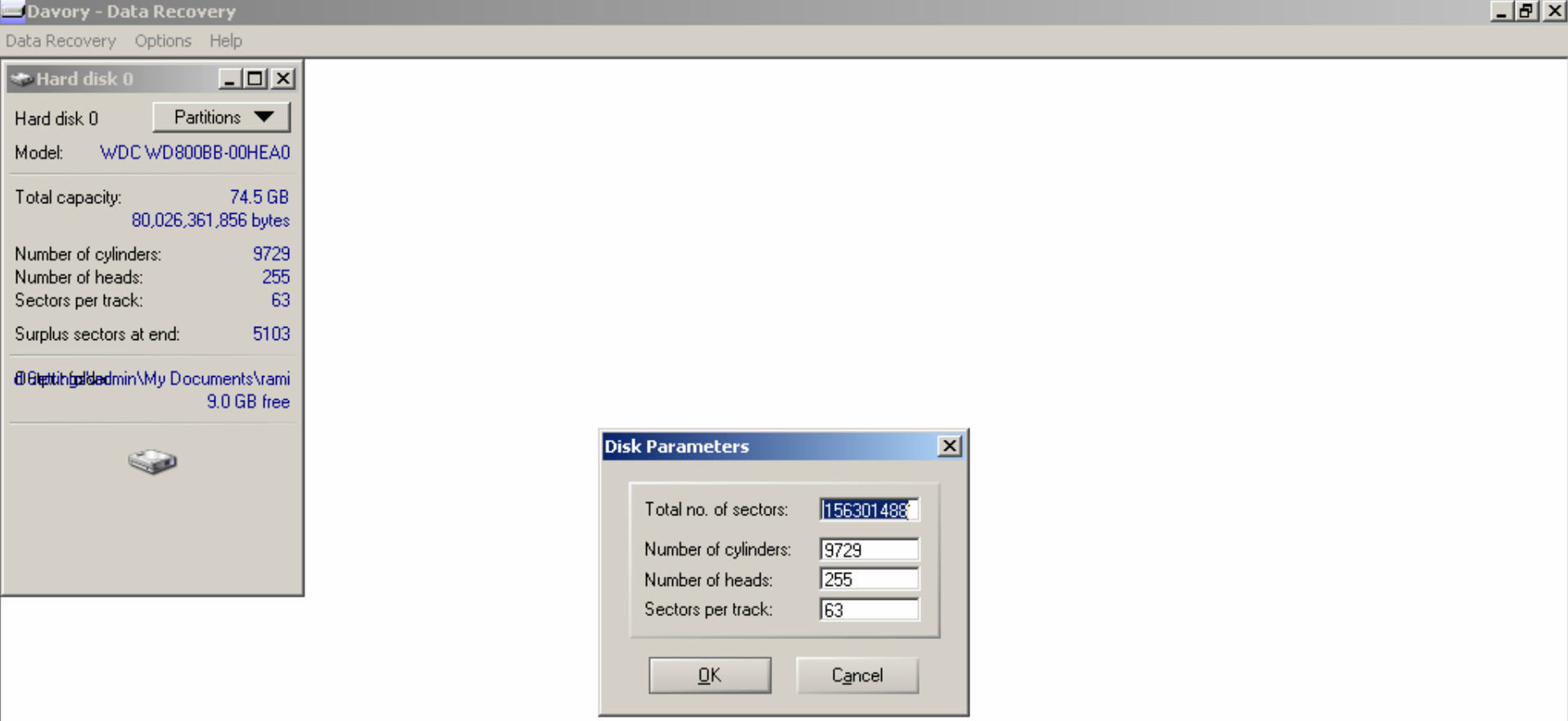

# THE WAY TO SELECT TYPE

# OPTIONS MENU

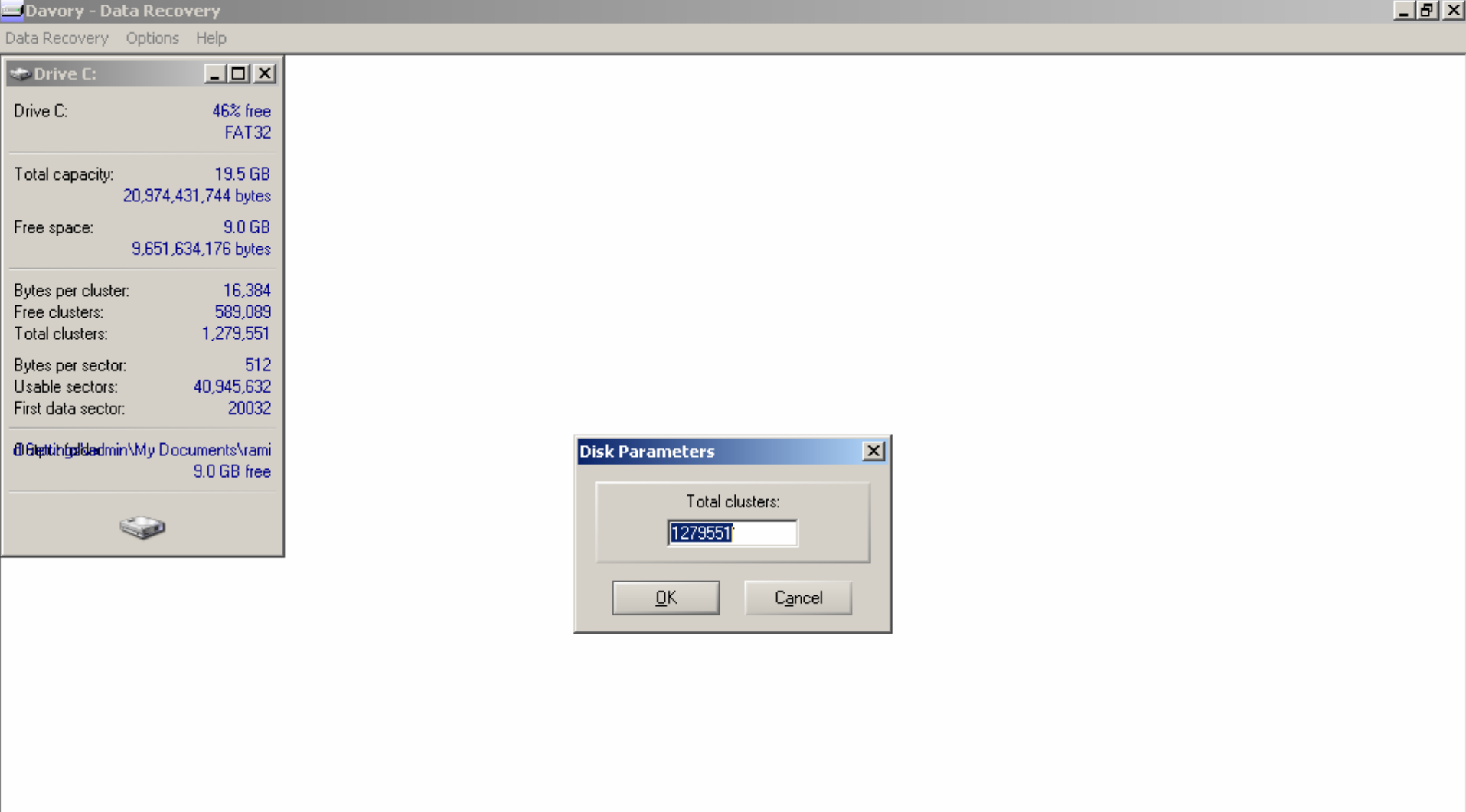
- Setup: Lets you switch between the English, the German, and the French user interface.
- Initialize: Use this command to restore the default settings of this program.
- Uninstall: Use this command to remove Davory from your system. This works properly even if you did not install Davory using the setup program.

# OPTIONS MENU

- Disk Parameters:
- Using this command on a physical disk, you may override the number of cylinders, heads, and sectors per track as recognized by Davory. This can be useful to access sectors at the end of the disk because isn't automatically detected by Davory
- Using this command on a logical drive to override the total number of clusters




# PHYSICAL DISK PARAMETERS




# LOGICAL DISK PARAMETERS

# RESTORE SOFTWARE

- The System Restore feature is built into Windows XP
- used to return your computer to an earlier state if you have a system failure or other major problem with your computer.
- System Restore takes snapshots of your computer system and saves them as **restore points** .
- These restore points mark configuration places to return to
- System Restore is both effective and user-friendly.

# HOW SYSTEM RESTORE WORKS

- System Restore automatically tracks changes to your computer
- Then, creates restore points before major changes are to occur.
- System Restore takes a full snapshot of the registry and some dynamic system files.

# Automatically Created Restore Points

- System Restore will automatically create a restore point before the following events:

  1)Application installations

  2)Auto Update installation :

  Update feature of Windows XP provide users to download critical Microsoft Windows® updates .

  *Once the update is downloaded the user chooses to install the update, the System Restore feature will create a restore point before the actual installation .

# Cont..

3)Restore operation

If a user, for example, accidentally chooses the wrong system state to restore back Then the restore operation itself will create a restore point for undo purposes.

4) Microsoft Backup Utility Recovery .

5) Unsigned driver installation .

6) Manual Restore points. At any time, users (administrator/owner users only) may create restore point.

# Cont..

- Scheduled restore points :

-System Restore provides users with the ability to restore to other specific days and times. It does this by creating a restore point every 24 hours of calendar time .

-Restore points are only created during idle time .

-Restore points saved and compressed Under(NTFS only).

# THE END