Data Recovery

By

PRAJIN PRAKASH

No:40

Reg.No:11131982

What is Data?

- Computer data is information processed or stored by a computer.

- This information may be in the form of text documents, images, audio clips, software programs, or other types of data. Computer data may be processed by the computer's **CPU** and is stored in files and **folders** on the the computer's **hard disk**

What is Data recovery ?

it is the process of salvaging **data** from damaged, failed, corrupted, or inaccessible secondary storage media when it cannot be accessed normally. Recovery may be required due to physical damage to the storage device or logical damage to the file system

The essence of data recovery

- Data recovery means retrieving lost, deleted, unusable or inaccessible data that lost for various reasons.
- Data recovery not only restores lost files but also recovers corrupted data.
- There are software and hardware reasons that cause data loss, while we can recover data by software and hardware ways.

The scope of data recovery

- There are so many forms and phenomenon on data problem, we can divide the objects or scope of data recovery according to different symptoms

The scope of data recovery

System problem

- Can not enter the system or the system is abnormal or computer closes down.
- Key file of system is lost or corrupted, there is some bad track on hard disk, the hard disk is damaged, MBR or DBR is lost, or the CMOS setting is incorrect and so on.

Bad track of hard disk

- logic and physical bad track.
- Logic bad track is mainly caused by incorrect operation, and it can be restored by software.
- While physical bad track is caused by physical damage, which is real damage, we can restore it by changing the partition or sector.

The scope of data recovery

Partition problem

- partition cannot be identified and accessed, or partition is identified as unformatted, partition recovery tools such as Partition Table Doctor can be used to recover data.

Files loss

If files are lost because of deletion, format or Ghost clone error, files restoring tools such as Data Recovery Wizard can be used to recover data.

The scope of data recovery

Password loss

- If files, system password, database or account is lost, some special decryption tools that correspond to certain data form such as Word, WinZip can be used.

Files repair

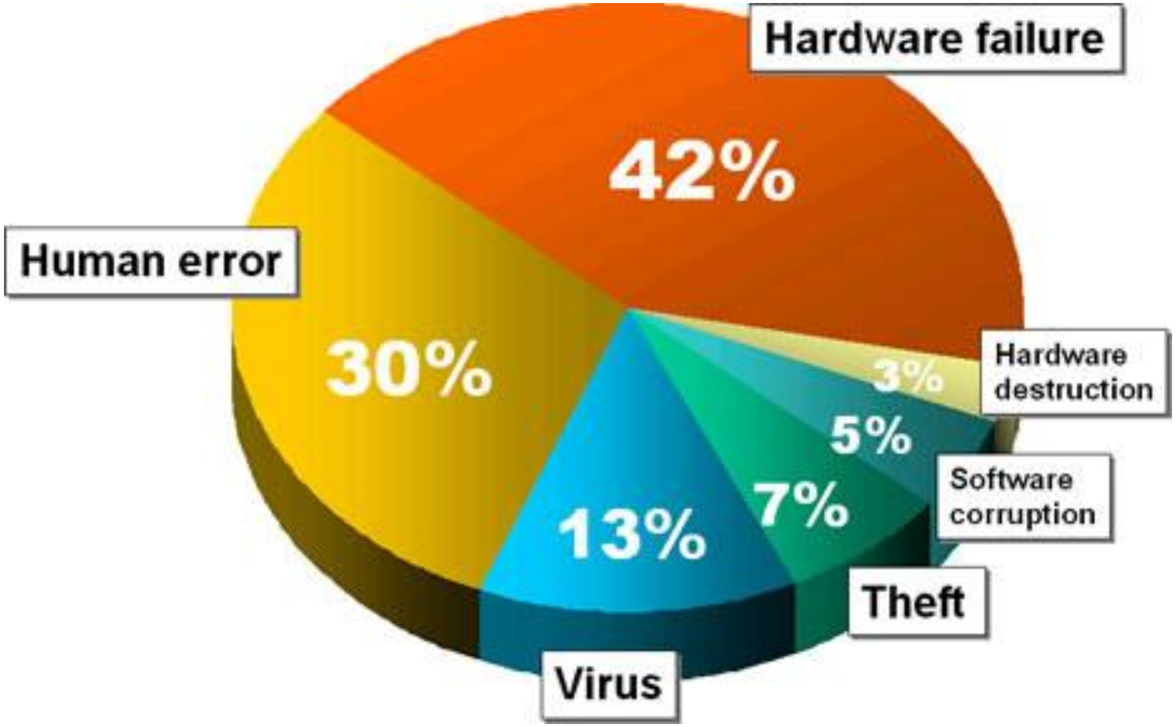
- For some reasons, some files can not be accessed or used, or the contents are full of troubled characters, the contents are changed so as they can not be read. In this condition, some special files restoring tools can be tried to restore the files.

The principle of data recovery

Data recovery is a process of finding and recovering data, in which there may be some risk, for no all situations can be anticipated or prearranged. It means maybe there will be some unexpected things happen. So we need reduce the danger in data recovery to the lowest:

- Backup all the data in your hard disk
- Prevent the equipment from being damaged again
- Don’t write anything to the device on which you want to recover data
- Try to get detailed information on how the data lost and the losing process
- Backup the data recovered in time.

Data loss

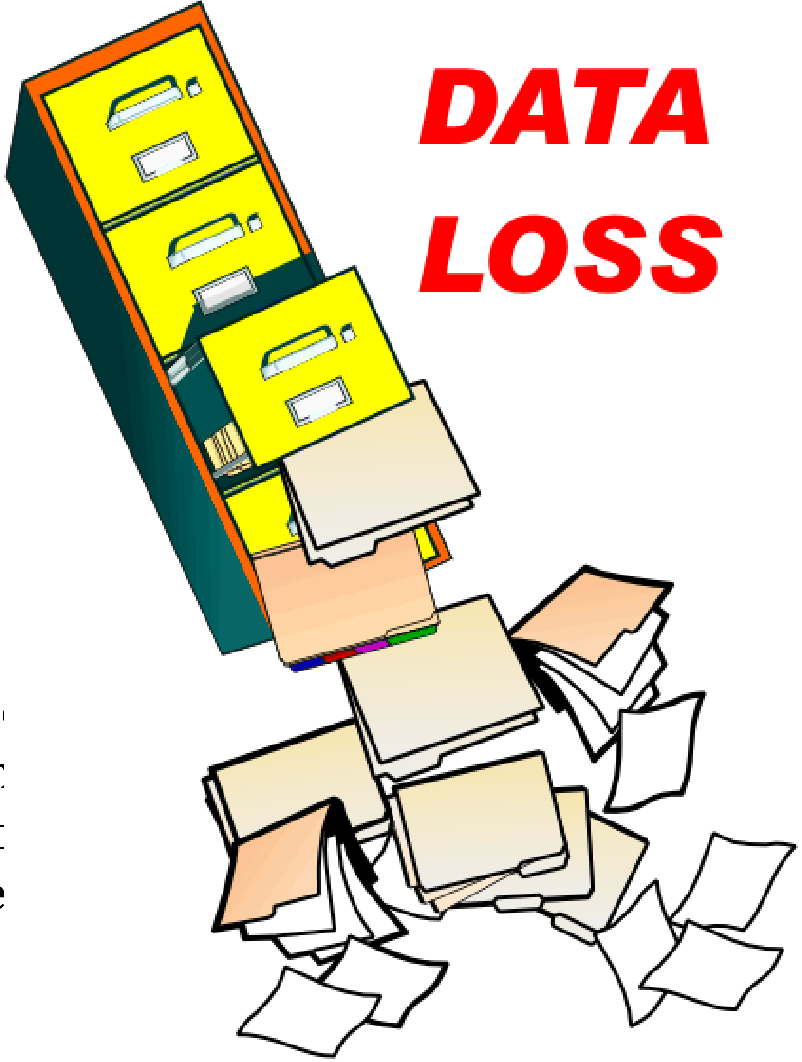


FILE NOT FOUND!

Software reason

- Virus, format, mis-partition, mis-clone, mis-operation, network deletion, power-cut during operati all may be the software reasons. Th symptoms are usually mis-operatio read error, can not find or open file report no partition, not formatted, password lost and troubled characters

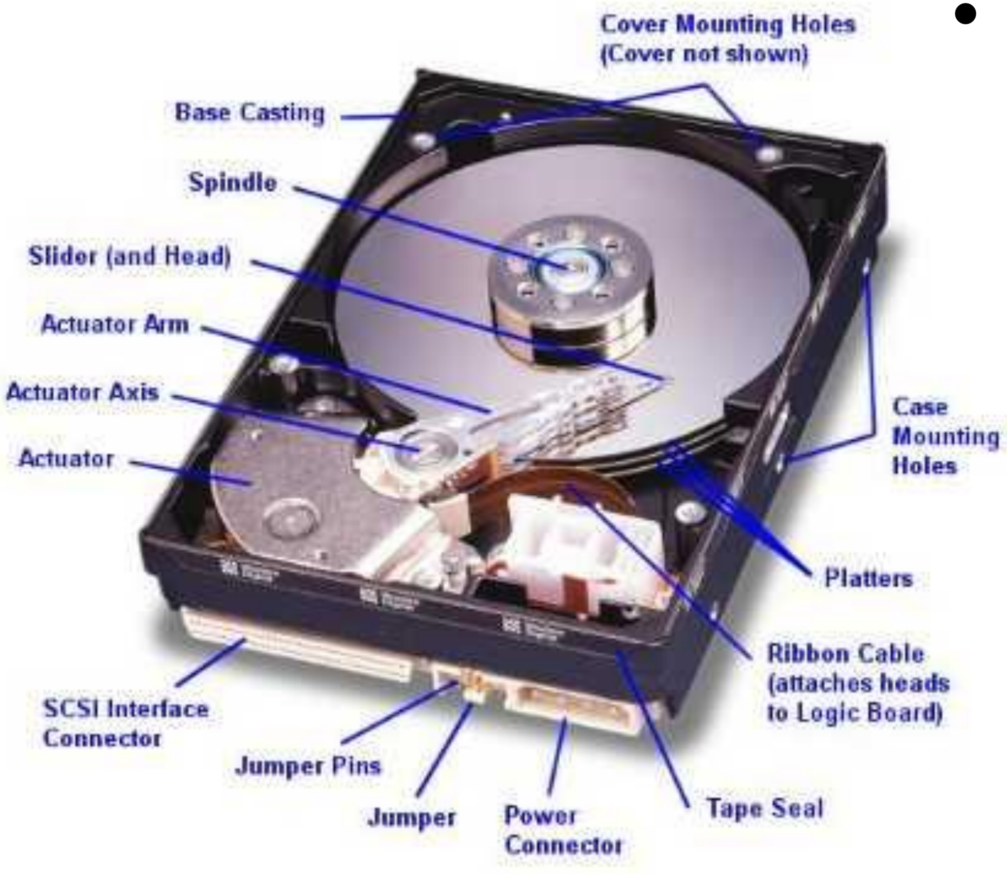
  use software tools to recover it. So called soft recovery means data can be recovered by software



Data loss

- **Hardware reason**
  - Sometimes data loss is because of hardware, such as bad sector in hard disk, power cut, head damage, circuit panel problem, etc.
  - The speed of hardware become slow, cannot operate successfully; cannot read data, etc

Hard disk

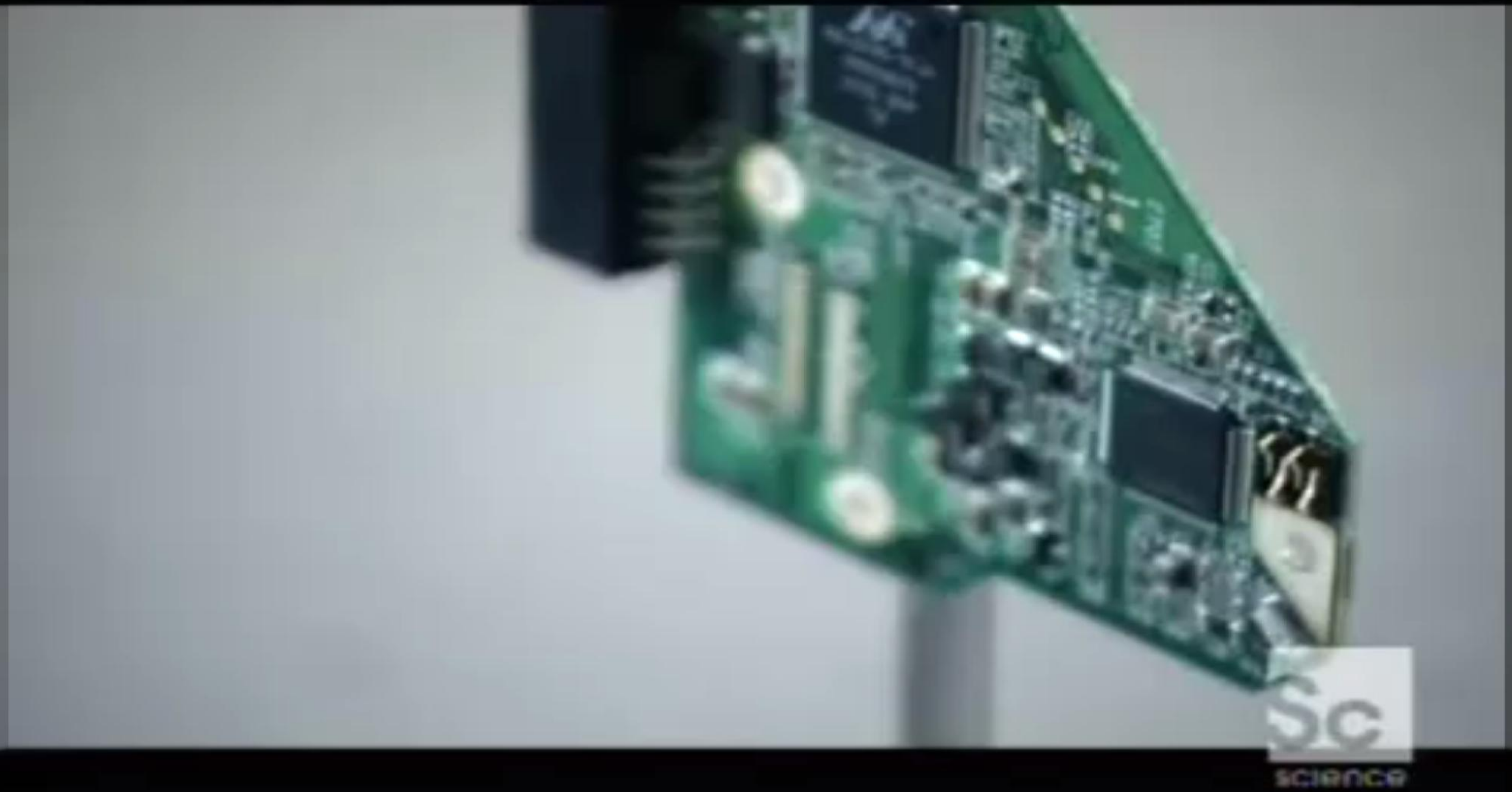


- Physical structure

HD consists of platter, control circuit board and interface parts.

A hard disk is a sealed unit containing a number of platters in a stack. Hard disks may be mounted in a horizontal or a vertical position. In this description, the hard drive is mounted horizontally.

Parts of hard disk



Data organization

- Primary formatting of hard disk

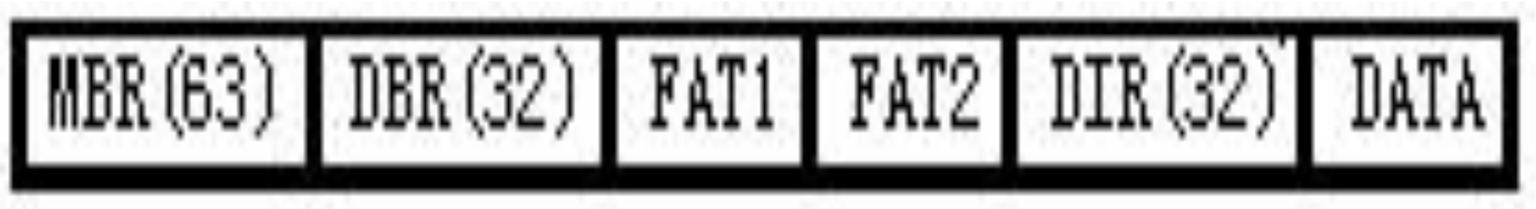
  When hard disk is firstly made in the factory, it usually is "blank". Only after partitioning tracks and sectors, we can save data on hard disk

- Advanced formatting of hard disk High-level format

Assign logical serial numbers for sectors (serial numbers in partition) from cylinder that assigned by each logical drive

Data storage region of HD

Data in hard disk divided into 5



- **MBR :**master boot directory . The first physical sector. Bios or special firmware stored.
- **DBR :** dos boot directory. First sector that visit by os .store boot program and BPB (BIOS perimeter block).
- **FAT :** it is a file system . Relatively uncomplicated.
- **DIR :** means directory also called FDT. DIR is placed after FAT2
- **DATA :**store the data

File systems

Management of fat32 file system

Root directory management in FAT32 partition

- All files/folders in FAT32 have corresponding file entries record in FDT, each file entry records important information of the file/folder the file system of operating system searches and localizes corresponding file/folder according to the file information in FDT of each partition. Under FAT32, size of each FDT is 32 bytes.
- FAT32 root directory management includes management of files with short and long filename, and management of direcotories under root directory..

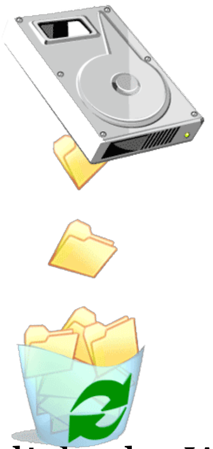
Sub directory management

Management of sub-directory in FAT32

- a parental directory may have many sub-directories, while a sub-directory has only one parental directory. Under the sub-directory of root directory, we may create more inferior sub-directories, thus forming a directory tree. For directories under root directory, its entrance still exists in root directory. .

File deletion

When deleting a file, the system only makes a deletion mark on this file’s directory entry, marking clusters it covers in FAT as “empty”; clusters in DATA remains original file’s contents. When writing in data again, the original file content might be covered by new information.

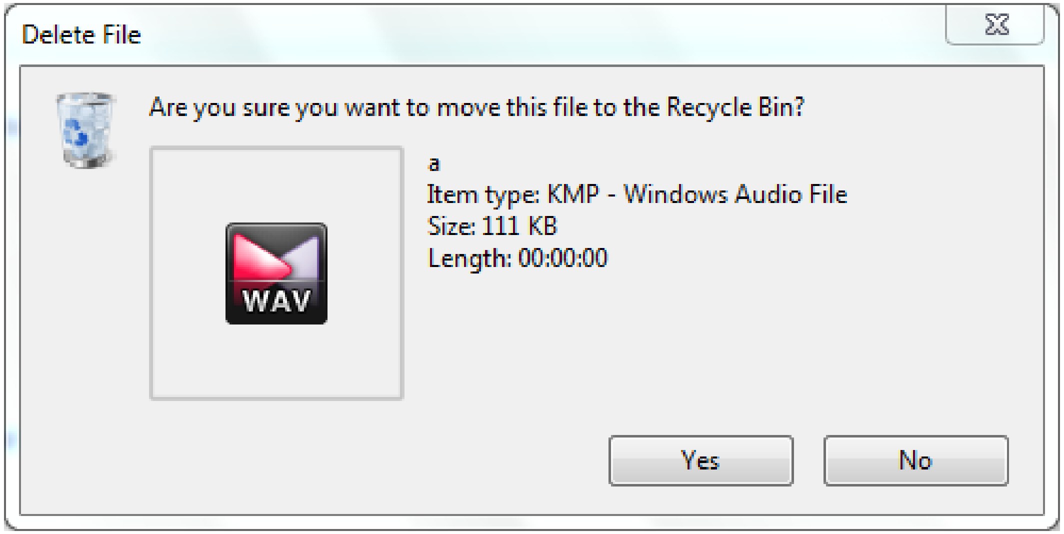


There is a Recycle Bin in Windows,
The recycling bin is only some space on the hard disk; the Windows system automatically
establishes a folder "**RECYCLED**" (under root directory of each disk partition) with hiding attribute to save temporarily deleted files. Only when deleting or executing “Clear” command, these files then can be completely deleted (as to operating system). As "the recycling bin" we see on the desktop, it is only a shortcut. Then we will introduce fast deletion and complete deletion separately.

File deletion

Fast deletion

Fast deletion of files is just to put them into Recycle Bin. In this situation, the data can be recovered.



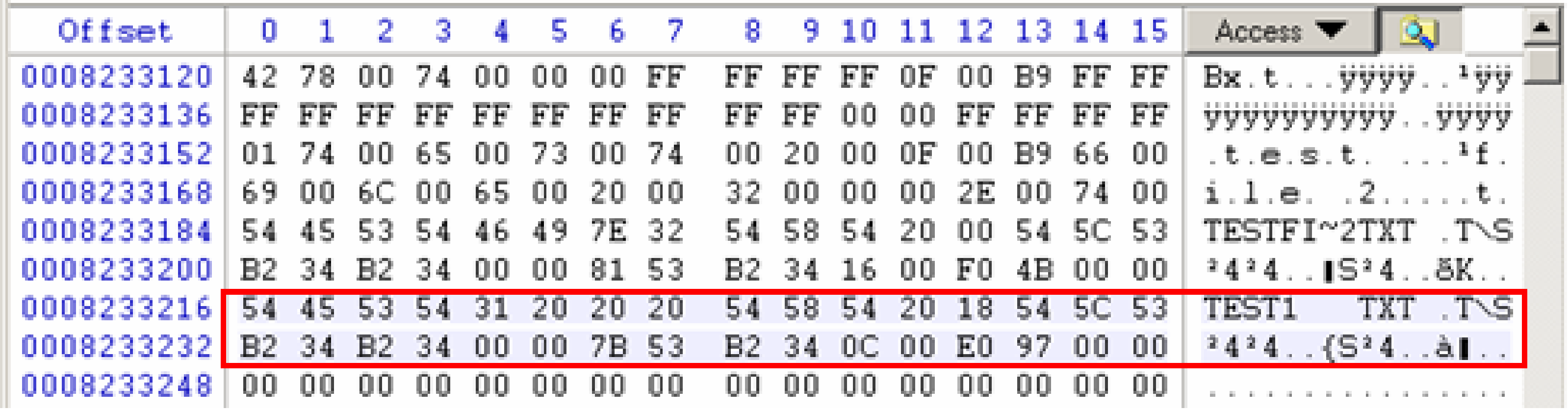
Are you sure you want to move this file to the Recycle Bin?

a
Item type: KMP - Windows Audio File
Size: 111 KB
Length: 00:00:00

Comparing the changes of FDT, FAT and DATA between before and after deletion, we can find the rules.

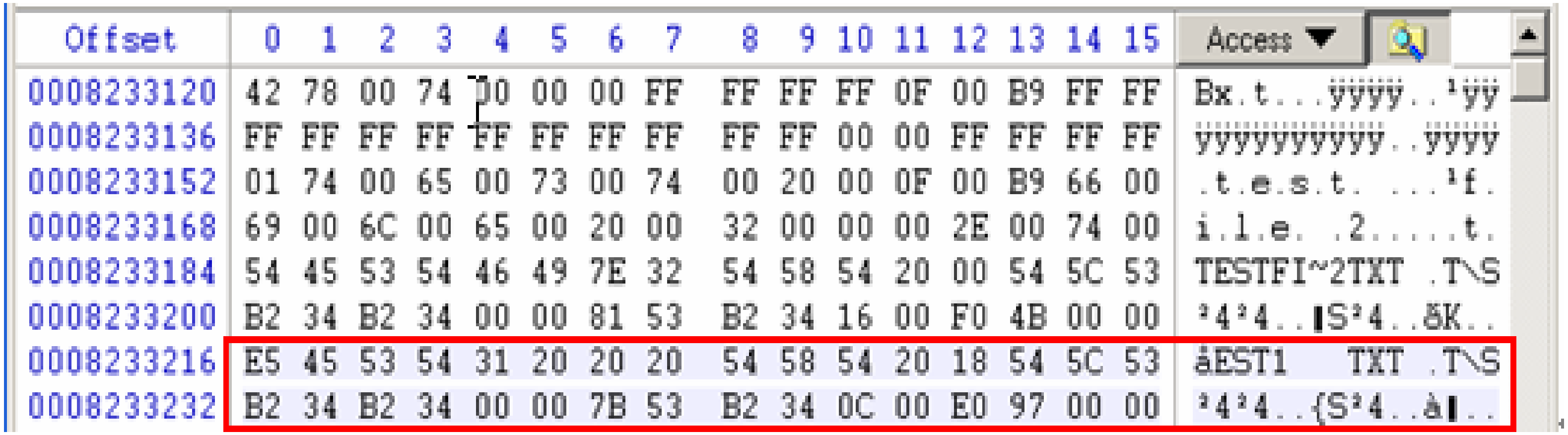
File deletion

FDT before deleting “test1.txt”:



```
Offset      0  1  2  3  4  5  6  7   8  9 10 11 12 13 14 15   Access ▼
0008233120  42 78 00 74 00 00 00 FF  FF FF FF 0F 00 B9 FF FF  Bx.t...ÿÿÿÿ..¹ÿÿ
0008233136  FF FF FF FF FF FF FF FF  FF FF 00 00 FF FF FF FF  ÿÿÿÿÿÿÿÿÿÿ..ÿÿÿÿ
0008233152  01 74 00 65 00 73 00 74  00 20 00 0F 00 B9 66 00  .t.e.s.t. ...¹f.
0008233168  69 00 6C 00 65 00 20 00  32 00 00 00 2E 00 74 00  i.l.e. .2.....t.
0008233184  54 45 53 54 46 49 7E 32  54 58 54 20 00 54 5C 53  TESTFI~2TXT .T\S
0008233200  B2 34 B2 34 00 00 81 53  B2 34 16 00 F0 4B 00 00  ²4²4..▮S²4..ðK..
0008233216  54 45 53 54 31 20 20 20  54 58 54 20 18 54 5C 53  TEST1   TXT .T\S
0008233232  B2 34 B2 34 00 00 7B 53  B2 34 0C 00 E0 97 00 00  ²4²4..{S²4..à▮..
0008233248  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
```

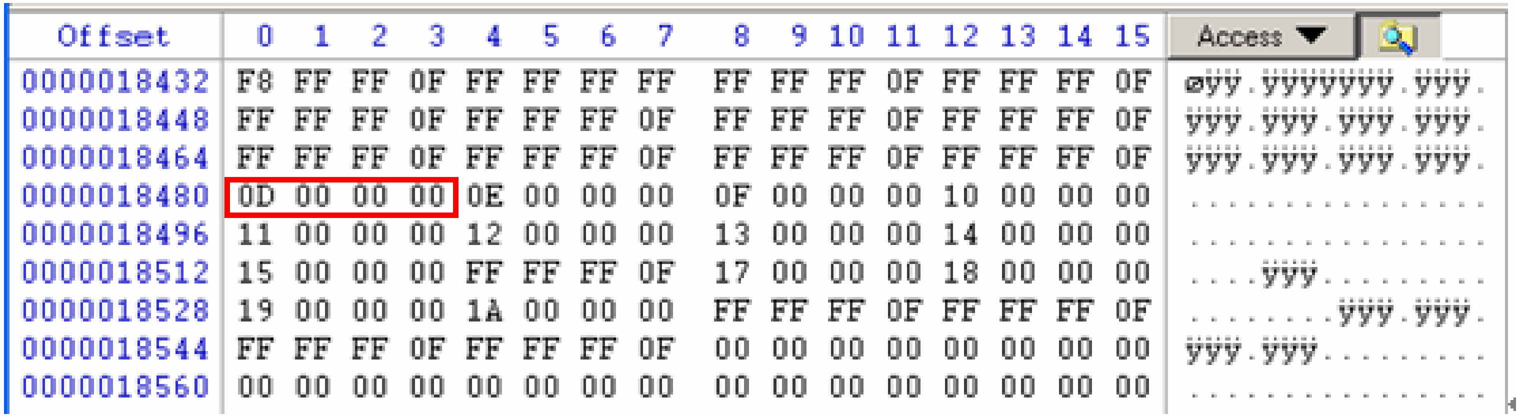
FDT after deletion:



```
Offset      0  1  2  3  4  5  6  7   8  9 10 11 12 13 14 15   Access ▼
0008233120  42 78 00 74 00 00 00 FF  FF FF FF 0F 00 B9 FF FF  Bx.t...ÿÿÿÿ..¹ÿÿ
0008233136  FF FF FF FF FF FF FF FF  FF FF 00 00 FF FF FF FF  ÿÿÿÿÿÿÿÿÿÿ..ÿÿÿÿ
0008233152  01 74 00 65 00 73 00 74  00 20 00 0F 00 B9 66 00  .t.e.s.t. ...¹f.
0008233168  69 00 6C 00 65 00 20 00  32 00 00 00 2E 00 74 00  i.l.e. .2.....t.
0008233184  54 45 53 54 46 49 7E 32  54 58 54 20 00 54 5C 53  TESTFI~2TXT .T\S
0008233200  B2 34 B2 34 00 00 81 53  B2 34 16 00 F0 4B 00 00  ²4²4..▮S²4..ðK..
0008233216  E5 45 53 54 31 20 20 20  54 58 54 20 18 54 5C 53  åEST1   TXT .T\S
0008233232  B2 34 B2 34 00 00 7B 53  B2 34 0C 00 E0 97 00 00  ²4²4..{S²4..à▮..
```

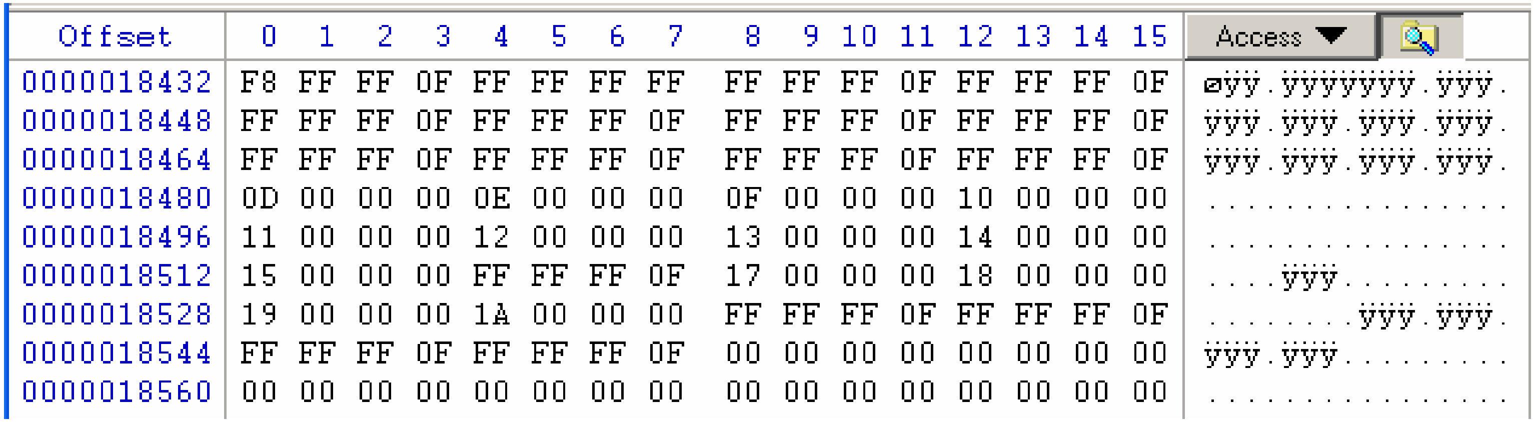
File deletion

FAT before deletion



```
    Offset      0  1  2  3  4  5  6  7   8  9 10 11 12 13 14 15   Access ▼
0000018432     F8 FF FF 0F FF FF FF FF  FF FF FF 0F FF FF FF 0F   øÿÿ.ÿÿÿÿÿÿÿ.ÿÿÿ.
0000018448     FF FF FF 0F FF FF FF 0F  FF FF FF 0F FF FF FF 0F   ÿÿÿ.ÿÿÿ.ÿÿÿ.ÿÿÿ.
0000018464     FF FF FF 0F FF FF FF 0F  FF FF FF 0F FF FF FF 0F   ÿÿÿ.ÿÿÿ.ÿÿÿ.ÿÿÿ.
0000018480     0D 00 00 00 0E 00 00 00  0F 00 00 00 10 00 00 00   ................
0000018496     11 00 00 00 12 00 00 00  13 00 00 00 14 00 00 00   ................
0000018512     15 00 00 00 FF FF FF 0F  17 00 00 00 18 00 00 00   ....ÿÿÿ.........
0000018528     19 00 00 00 1A 00 00 00  FF FF FF 0F FF FF FF 0F   ........ÿÿÿ.ÿÿÿ.
0000018544     FF FF FF 0F FF FF FF 0F  00 00 00 00 00 00 00 00   ÿÿÿ.ÿÿÿ.........
0000018560     00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ................
```

FAT after deletion

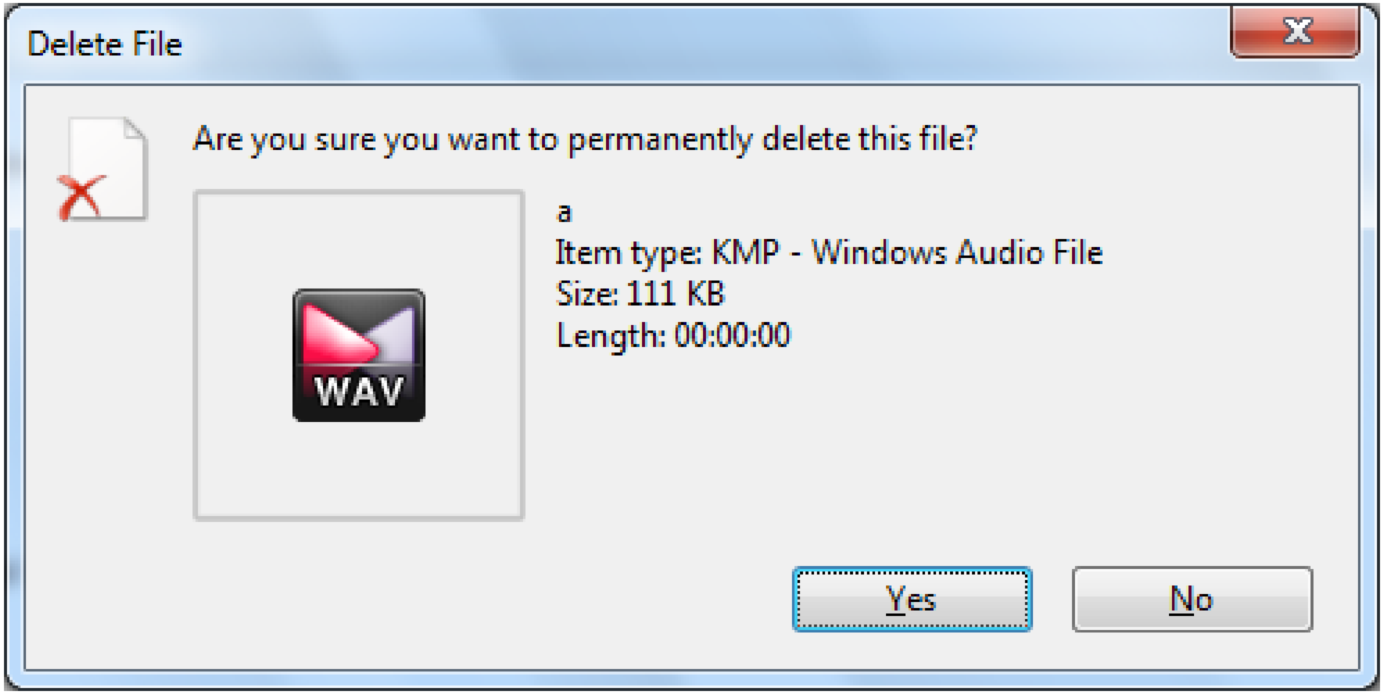


```
    Offset      0  1  2  3  4  5  6  7   8  9 10 11 12 13 14 15   Access ▼
0000018432     F8 FF FF 0F FF FF FF FF  FF FF FF 0F FF FF FF 0F   øÿÿ.ÿÿÿÿÿÿÿ.ÿÿÿ.
0000018448     FF FF FF 0F FF FF FF 0F  FF FF FF 0F FF FF FF 0F   ÿÿÿ.ÿÿÿ.ÿÿÿ.ÿÿÿ.
0000018464     FF FF FF 0F FF FF FF 0F  FF FF FF 0F FF FF FF 0F   ÿÿÿ.ÿÿÿ.ÿÿÿ.ÿÿÿ.
0000018480     0D 00 00 00 0E 00 00 00  0F 00 00 00 10 00 00 00   ................
0000018496     11 00 00 00 12 00 00 00  13 00 00 00 14 00 00 00   ................
0000018512     15 00 00 00 FF FF FF 0F  17 00 00 00 18 00 00 00   ....ÿÿÿ.........
0000018528     19 00 00 00 1A 00 00 00  FF FF FF 0F FF FF FF 0F   ........ÿÿÿ.ÿÿÿ.
0000018544     FF FF FF 0F FF FF FF 0F  00 00 00 00 00 00 00 00   ÿÿÿ.ÿÿÿ.........
0000018560     00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ................
```

File deletion

Complete deletion

how complete delete?



Delete File

Are you sure you want to permanently delete this file?

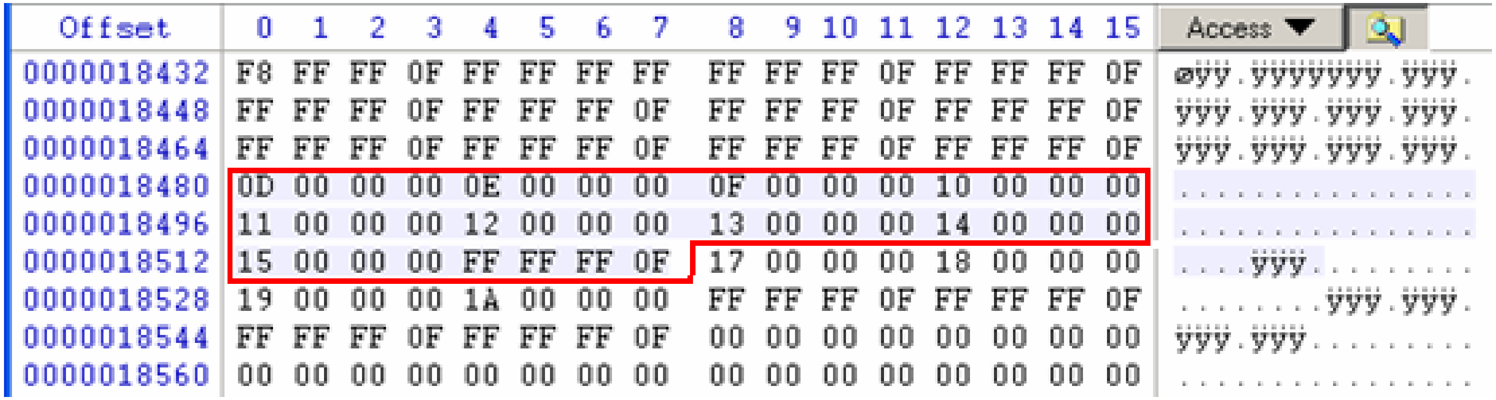
a
Item type: KMP - Windows Audio File
Size: 111 KB
Length: 00:00:00

File deletion

Complete deletion

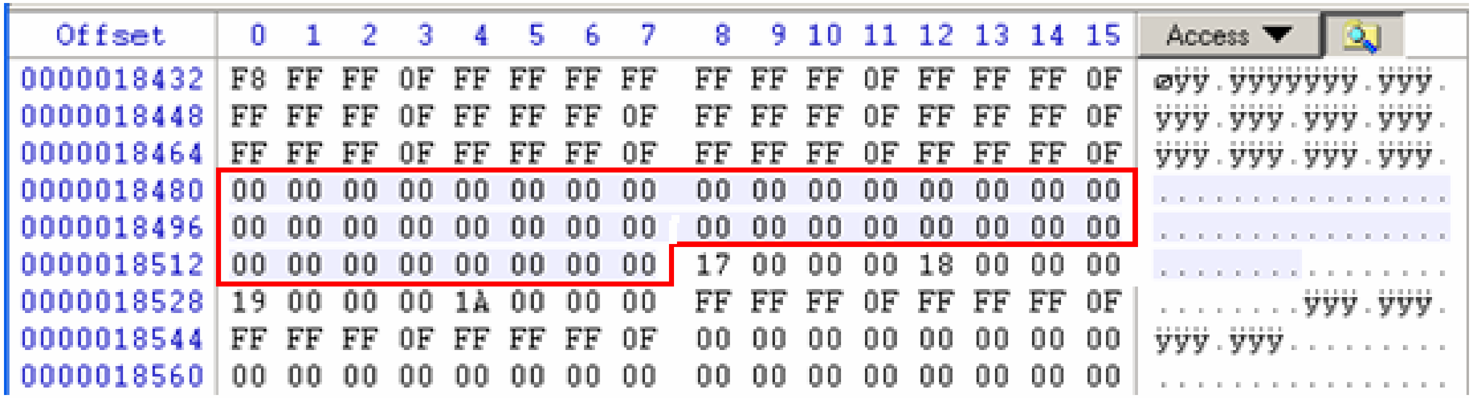
FDT is the same as that of fast deletion.

Before complete deletion, the content of FAT is:



```
Offset       0  1  2  3  4  5  6  7   8  9 10 11 12 13 14 15   Access ▼
0000018432  F8 FF FF 0F FF FF FF FF  FF FF FF 0F FF FF FF 0F   øÿÿ.ÿÿÿÿÿÿÿ.ÿÿÿ.
0000018448  FF FF FF 0F FF FF FF 0F  FF FF FF 0F FF FF FF 0F   ÿÿÿ.ÿÿÿ.ÿÿÿ.ÿÿÿ.
0000018464  FF FF FF 0F FF FF FF 0F  FF FF FF 0F FF FF FF 0F   ÿÿÿ.ÿÿÿ.ÿÿÿ.ÿÿÿ.
0000018480  0D 00 00 00 0E 00 00 00  0F 00 00 00 10 00 00 00   ................
0000018496  11 00 00 00 12 00 00 00  13 00 00 00 14 00 00 00   ................
0000018512  15 00 00 00 FF FF FF 0F  17 00 00 00 18 00 00 00   ....ÿÿÿ.........
0000018528  19 00 00 00 1A 00 00 00  FF FF FF 0F FF FF FF 0F   ........ÿÿÿ.ÿÿÿ.
0000018544  FF FF FF 0F FF FF FF 0F  00 00 00 00 00 00 00 00   ÿÿÿ.ÿÿÿ.........
0000018560  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ................
```

After deletion:

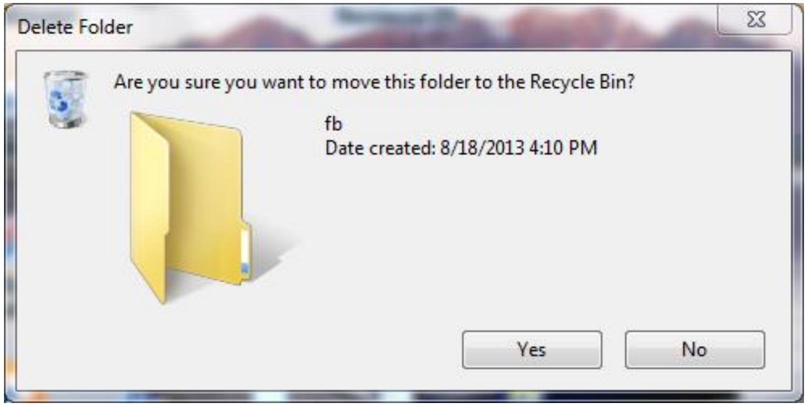


```
Offset       0  1  2  3  4  5  6  7   8  9 10 11 12 13 14 15   Access ▼
0000018432  F8 FF FF 0F FF FF FF FF  FF FF FF 0F FF FF FF 0F   øÿÿ.ÿÿÿÿÿÿÿ.ÿÿÿ.
0000018448  FF FF FF 0F FF FF FF 0F  FF FF FF 0F FF FF FF 0F   ÿÿÿ.ÿÿÿ.ÿÿÿ.ÿÿÿ.
0000018464  FF FF FF 0F FF FF FF 0F  FF FF FF 0F FF FF FF 0F   ÿÿÿ.ÿÿÿ.ÿÿÿ.ÿÿÿ.
0000018480  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ................
0000018496  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ................
0000018512  00 00 00 00 00 00 00 00  17 00 00 00 18 00 00 00   ................
0000018528  19 00 00 00 1A 00 00 00  FF FF FF 0F FF FF FF 0F   ........ÿÿÿ.ÿÿÿ.
0000018544  FF FF FF 0F FF FF FF 0F  00 00 00 00 00 00 00 00   ÿÿÿ.ÿÿÿ.........
0000018560  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ................
```

Subdirectory deletion

Operating system manages sub-directory in the same way as manages files. So, the deletion ways are same, too.

Fast deletion



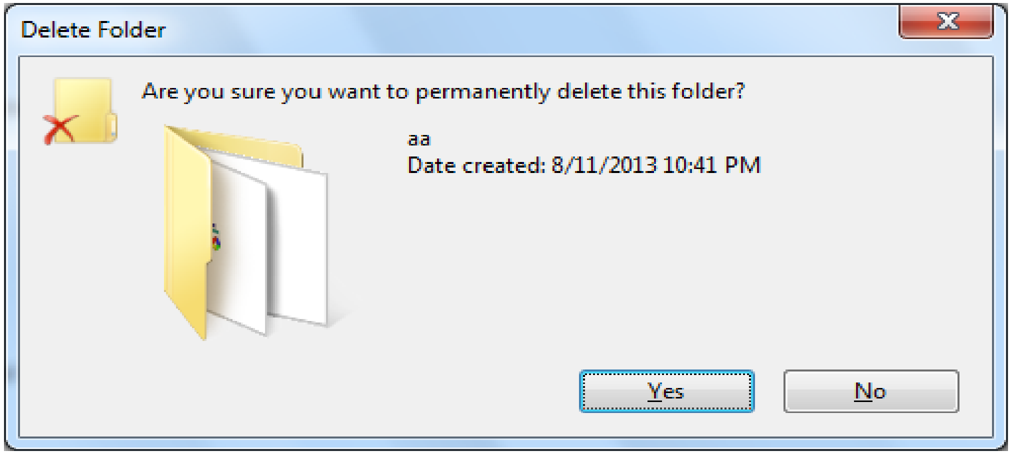
Are you sure you want to move this folder to the Recycle Bin?

fb
Date created: 8/18/2013 4:10 PM

Fast deletion of sub-directory is the same as that of files. It just marked a deletion mark to the beginning byte in FDT that describes sub-directory; all files under this sub-directory and records of its inferior sub-directory are not changed, that is, just to “remove” this sub-directory into recycling bin

Complete deletion

Complete deletion is same as that of in file..

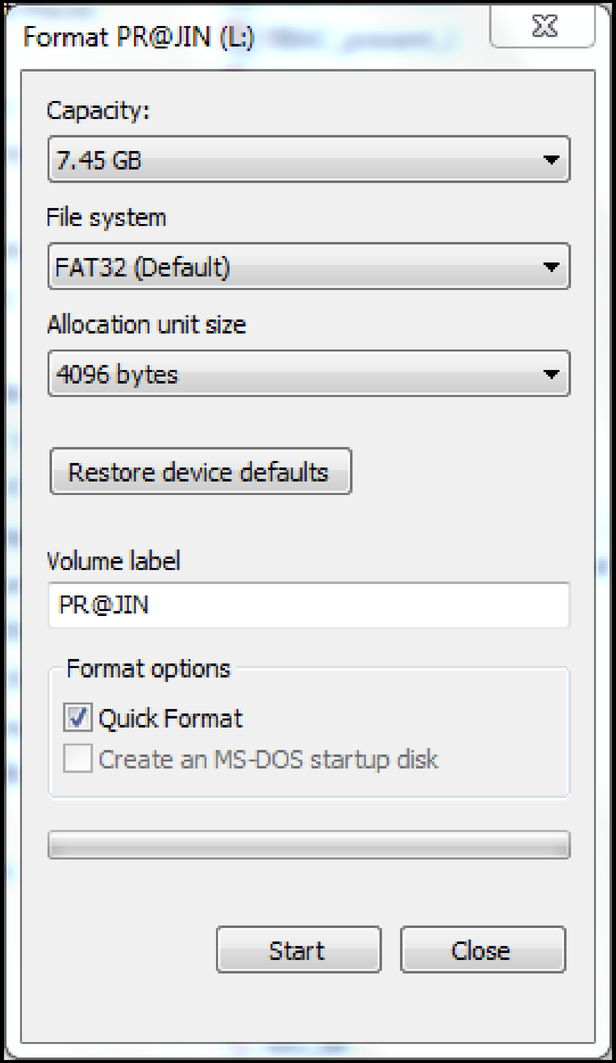


Are you sure you want to permanently delete this folder?

aa
Date created: 8/11/2013 10:41 PM

High level formatting

Fast high level format



Format PR@JIN (L:)

Capacity:
7.45 GB

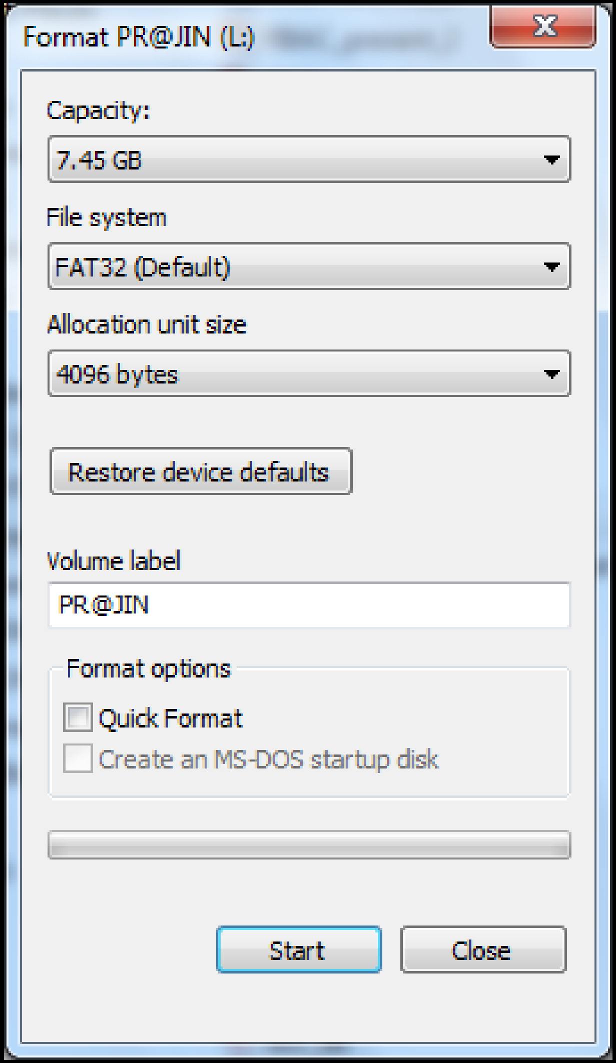
File system
FAT32 (Default)

Allocation unit size
4096 bytes

Volume label
PR@JIN

Format options
☑ Quick Format
□ Create an MS-DOS startup disk

Complete high level format



Format PR@JIN (L:)

Capacity:
7.45 GB

File system
FAT32 (Default)

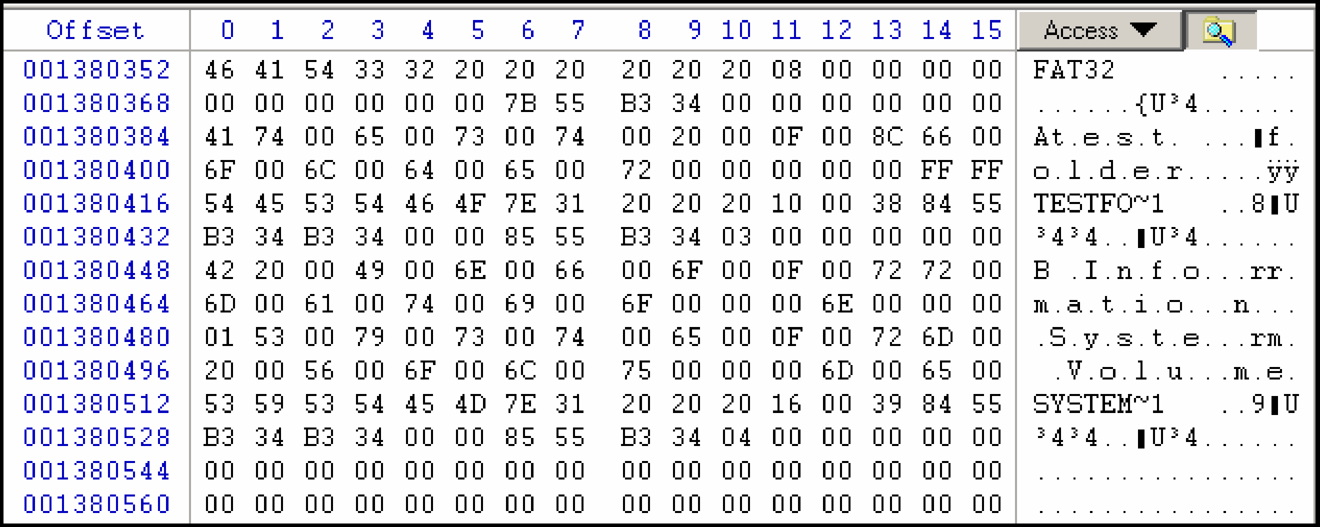
Allocation unit size
4096 bytes

Volume label
PR@JIN

Format options
□ Quick Format
□ Create an MS-DOS startup disk

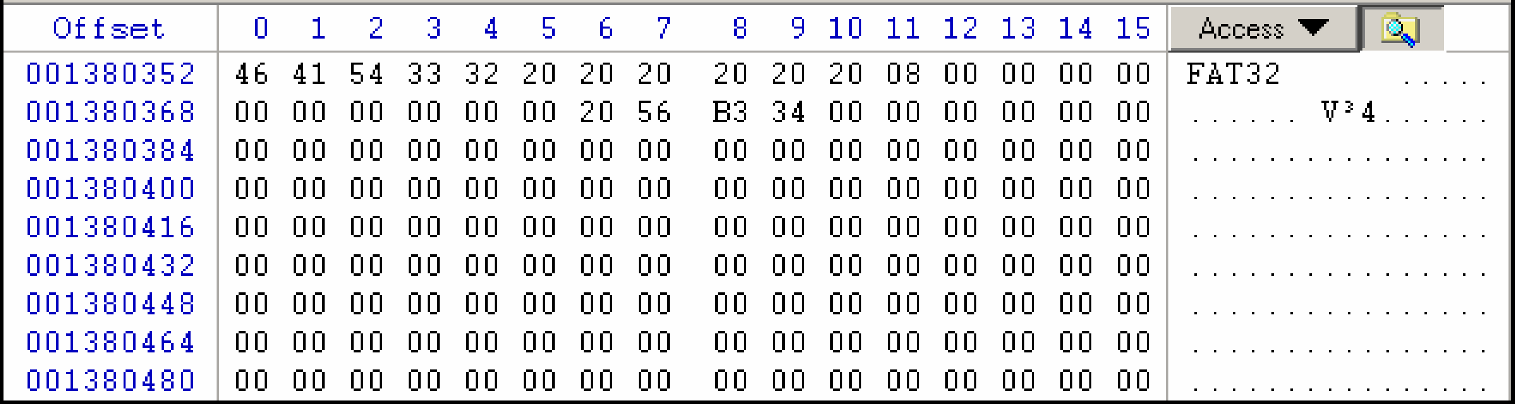
High level formatting

FDT before fast high level format:



```
Offset      0  1  2  3  4  5  6  7   8  9 10 11 12 13 14 15
001380352  46 41 54 33 32 20 20 20  20 20 20 08 00 00 00 00  FAT32      .....
001380368  00 00 00 00 00 00 7B 55  B3 34 00 00 00 00 00 00  ......{U³4......
001380384  41 74 00 65 00 73 00 74  00 20 00 0F 00 8C 66 00  At.e.s.t. ...▮f.
001380400  6F 00 6C 00 64 00 65 00  72 00 00 00 00 00 FF FF  o.l.d.e.r.....ÿÿ
001380416  54 45 53 54 46 4F 7E 31  20 20 20 10 00 38 84 55  TESTFO~1   ..8▮U
001380432  B3 34 B3 34 00 00 85 55  B3 34 03 00 00 00 00 00  ³4³4..▮U³4......
001380448  42 20 00 49 00 6E 00 66  00 6F 00 0F 00 72 72 00  B .I.n.f.o...rr.
001380464  6D 00 61 00 74 00 69 00  6F 00 00 00 6E 00 00 00  m.a.t.i.o...n...
001380480  01 53 00 79 00 73 00 74  00 65 00 0F 00 72 6D 00  .S.y.s.t.e...rm.
001380496  20 00 56 00 6F 00 6C 00  75 00 00 00 6D 00 65 00   .V.o.l.u...m.e.
001380512  53 59 53 54 45 4D 7E 31  20 20 20 16 00 39 84 55  SYSTEM~1   ..9▮U
001380528  B3 34 B3 34 00 00 85 55  B3 34 04 00 00 00 00 00  ³4³4..▮U³4......
001380544  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
001380560  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
```

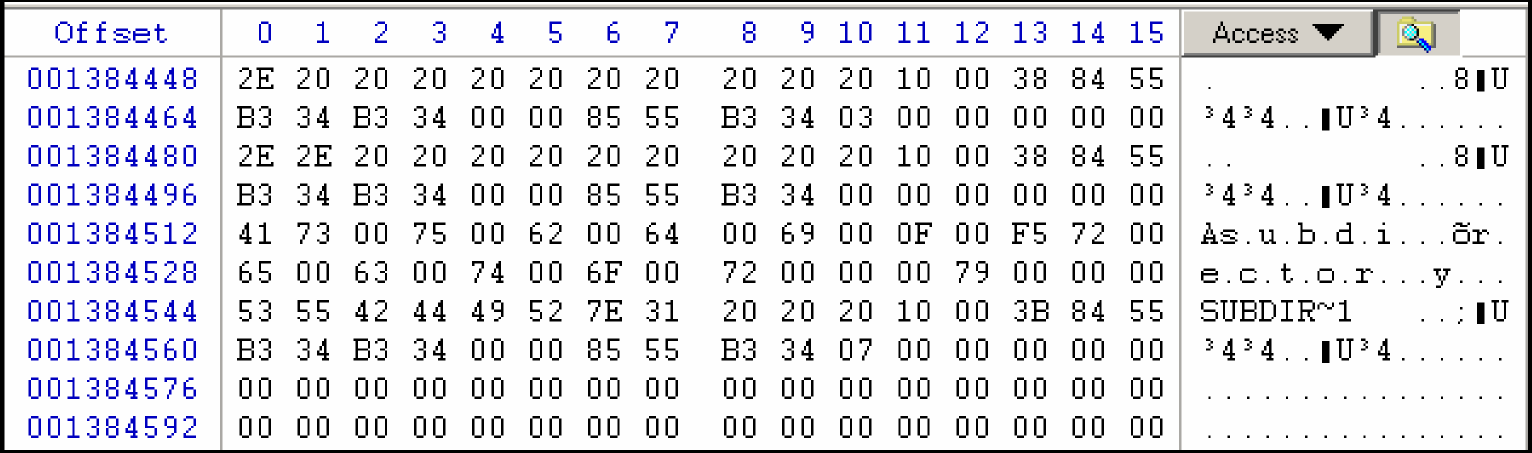
FDT after fast high level format:



```
Offset      0  1  2  3  4  5  6  7   8  9 10 11 12 13 14 15
001380352  46 41 54 33 32 20 20 20  20 20 20 08 00 00 00 00  FAT32      .....
001380368  00 00 00 00 00 00 20 56  B3 34 00 00 00 00 00 00  ...... V³4......
001380384  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
001380400  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
001380416  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
001380432  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
001380448  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
001380464  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
001380480  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
```

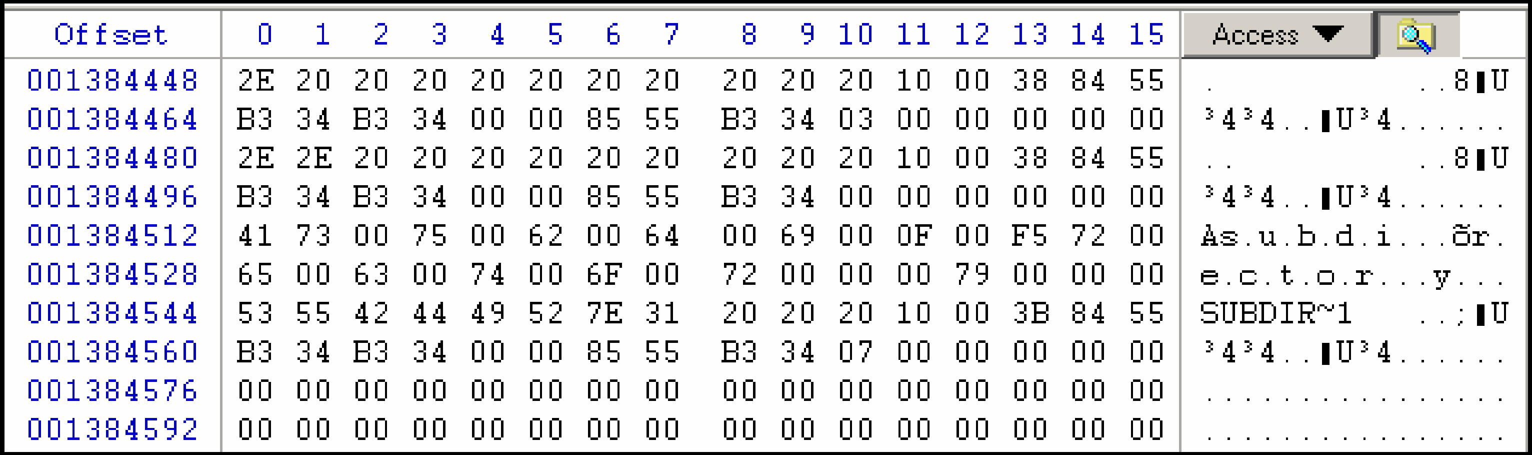
High level formatting

contents of sub-directory Before format:



```
Offset      0  1  2  3  4  5  6  7   8  9 10 11 12 13 14 15   Access ▼
001384448  2E 20 20 20 20 20 20 20  20 20 20 10 00 38 84 55  .          ..8▌U
001384464  B3 34 B3 34 00 00 85 55  B3 34 03 00 00 00 00 00  ³4³4..▌U³4......
001384480  2E 2E 20 20 20 20 20 20  20 20 20 10 00 38 84 55  ..         ..8▌U
001384496  B3 34 B3 34 00 00 85 55  B3 34 00 00 00 00 00 00  ³4³4..▌U³4......
001384512  41 73 00 75 00 62 00 64  00 69 00 0F 00 F5 72 00  As.u.b.d.i...õr.
001384528  65 00 63 00 74 00 6F 00  72 00 00 00 79 00 00 00  e.c.t.o.r...y...
001384544  53 55 42 44 49 52 7E 31  20 20 20 10 00 3B 84 55  SUBDIR~1   ..;▌U
001384560  B3 34 B3 34 00 00 85 55  B3 34 07 00 00 00 00 00  ³4³4..▌U³4......
001384576  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
001384592  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
```

After format:



```
Offset      0  1  2  3  4  5  6  7   8  9 10 11 12 13 14 15   Access ▼
001384448  2E 20 20 20 20 20 20 20  20 20 20 10 00 38 84 55  .          ..8▌U
001384464  B3 34 B3 34 00 00 85 55  B3 34 03 00 00 00 00 00  ³4³4..▌U³4......
001384480  2E 2E 20 20 20 20 20 20  20 20 20 10 00 38 84 55  ..         ..8▌U
001384496  B3 34 B3 34 00 00 85 55  B3 34 00 00 00 00 00 00  ³4³4..▌U³4......
001384512  41 73 00 75 00 62 00 64  00 69 00 0F 00 F5 72 00  As.u.b.d.i...õr.
001384528  65 00 63 00 74 00 6F 00  72 00 00 00 79 00 00 00  e.c.t.o.r...y...
001384544  53 55 42 44 49 52 7E 31  20 20 20 10 00 3B 84 55  SUBDIR~1   ..;▌U
001384560  B3 34 B3 34 00 00 85 55  B3 34 07 00 00 00 00 00  ³4³4..▌U³4......
001384576  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
001384592  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
```

NTFS

NTFS (**New Technology File System**) is a proprietary file system developed by Microsoft Corporation for its Windows NT line of operating systems,

NTFS supersedes the FAT file system as the preferred file system for Microsoft Windows operating systems. NTFS has several technical improvements over FAT and HPFS (High Performance File System), such as improved support for metadata, and the use of advanced data structures to improve performance, reliability, and disk space utilization, plus additional extensions, such as security access control lists (ACL) and file system journaling.

NTFS

- **High-level features of NTFS**

- Multi-data streams
- Name based on Unicode
- General index mechanism
- The dynamic bad cluster reprints maps
- Supports POSIX
- File compression
- File encrypts
- Disk quota
- Hard link and soft link
- Link tracks
- Log records
- Fragmentation

FAT vs. NTFS

FAT32

Maximum disk size: 2 terabytes

Maximum file size: 4 gigabytes

Maximum number of files on disk: 268,435,437

Maximum number of files in a single folder: 65,534

NTFS

Maximum disk size: 256 terabytes

Maximum file size: 256 terabytes

Maximum number of files on disk: 4,294,967,295

Maximum number of files in a single folder: 4,294,967,295

Matters needs attention before recovery

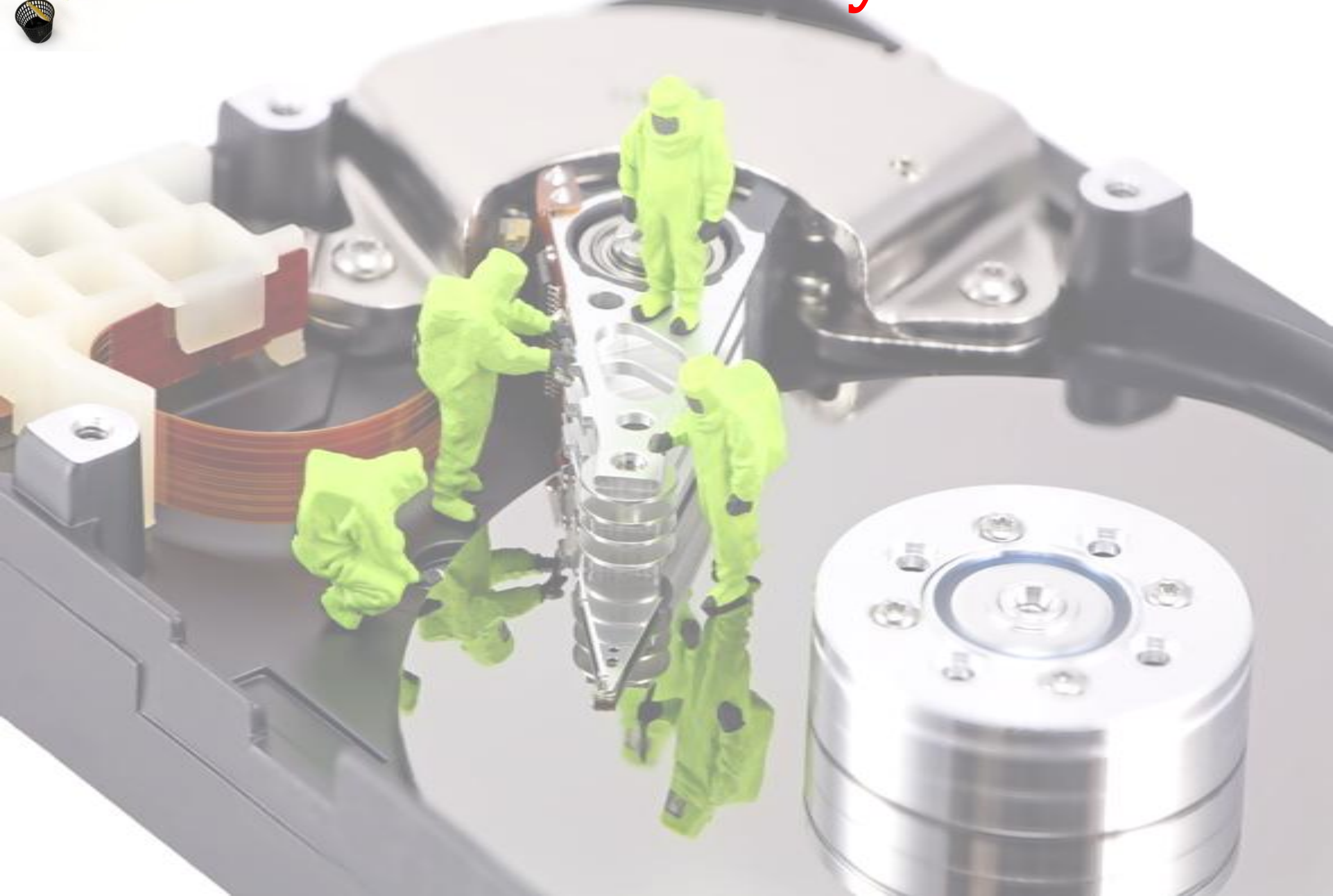
(1)Never operate on partition (such as write and create file) where the data lost.

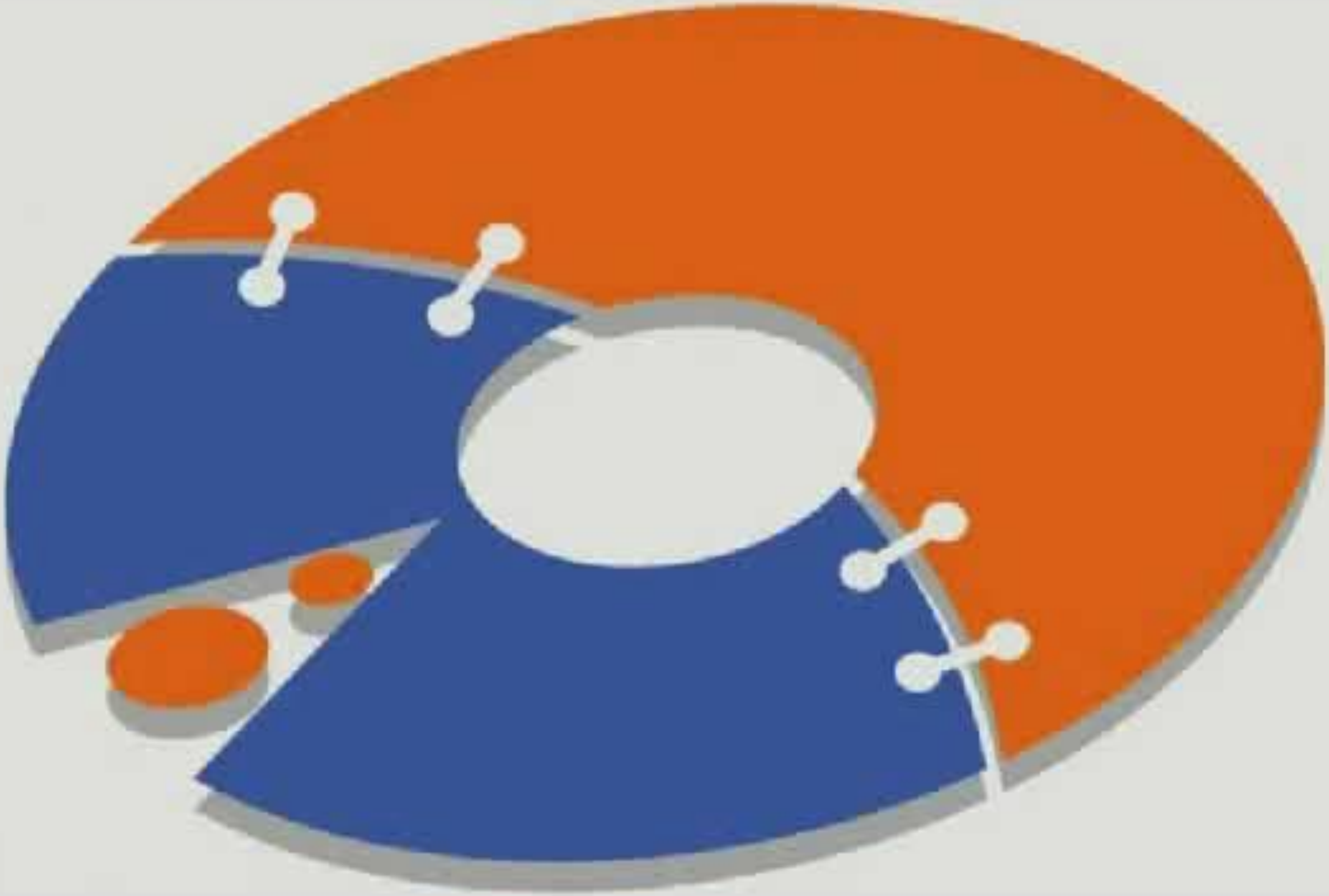
(2)Please close any other application program when Data Recovery Wizard 3.0 is running.

(3)Make sure that there is no physical failure (such as physical bad track) on the disk you are operating. If there is any problem, please stop running Data Recovery Wizard 3.0, and send your disk to maintenance station.

(4)Do not save the recovered files to the original partition. You need make sure that there is enough free space to save the recovered data; also you can save your files to removable devices or network devices.

Hard recovery





RECOVERY

Soft recovery

Advantages and disadvantages

- Data recovery tools can be used to undo mistakes that you made that resulted in lost data.

- Data consistency.

- Digital forensics

- To successfully use a data recovery tool you will need to determine the cause of your data loss.

- A simple reboot cause the over writing of data

- Data security.

- Recovery may generate virus.

Software used for recovery

Bootable
Data recovery cannot always be done on a running system. As a result, a boot disk, Live CD, Live USB, or any other type of Live Distro containing a minimal operating system.

BackTrack:

Boot Repair Disk -

Hiren's BootCD:

SystemRescueCD:
Consistency checkers

CHKDSK:

Disk First Aid:

Disk Utility:

Software used for recovery

File recovery

- CDRoller: Recovers data from optical discs.
- Data LifeSaver (now "EASIS Data Recovery"): Data recovery for FAT and NTFS file systems.
- Data Recovery Wizard: Microsoft Windows file recovery utility.
- Drive Vaccine: Microsoft Windows Auto Restore of files on Reboot
- FileSalvage: A Mac OS X recovery program.
- IsoBuster: Recovers data from optical discs, USB sticks, Flash drives and Hard Drives.
- Recuva: Microsoft Windows 2000 & later, FAT and NTFS.
- TotalRecovery : Microsoft Windows. Bootable backup and recover system.
- TuneUp Utilities: Microsoft Windows XP & later. A suite of utilities that has a file recovery component.
- Power Data Recovery: Data recovery software by MiniTool. 1GB free data recovery for personal use.

Software used for recovery

Forensics

- EnCase: A suite of forensic tools developed by Guidance Software that is used for imaging and forensic analysis for UNIX, Linux, and Windows systems.

- Foremost: An opensource CLI file recovery program, originally developed by the U.S. Air Force Office of Special Investigations and NPS Center for Information Systems Security Studies and Research.

- Forensic Toolkit: by AccessData, used by law enforcement.

- Open Computer Forensics Architecture: An opensource program running on Linux.

- The Coroner's Toolkit: A suite of utilities aimed at assisting in forensic analysis of a UNIX system after a break-in.

- The Sleuth Kit: Also known as TSK, The Sleuth Kit is a suite of forensic analysis tools developed by Brian Carrier for UNIX, Linux and Windows systems. TSK includes the Autopsy forensic browser.

who
where
when
how
why
what

Thank You