



Security and Management of Local Computer Data

Ruicheng Li

Shandong Youth Administrative Cadre' College, Jinan 250103, China

Tel: 86-531-85857405 E-mail: LRC04@163.COM

Abstract

In the computer system, only the data storing in the computer are the real fortune, and the protection of information and data are crucial. In the day that data security becomes more and more important, the stable and self-contained backup system has been the key to ensure the normal running of the system. Data backup is not only the conservation of data, but includes more important content, i.e. the management, or else, the data will be lost even the whole hard disk will be dormant, and hell and gone losses will be induced.

Keywords: Computer system, Data security, Management, Backup

1. Introduction

Data security has been more and more important for the computer system, and there are two reasons which may induce data loss, i.e. the software fault and the hardware fault. Once the important data are destroyed or lost, it will induce huge influences even hell and gone losses. Large-sized data reconstruction needs long time and expensive costs, and the only effective method to reduce the loss minimum is to make the data backup.

The security backup of data has been developed for a long time, and when most domestic enterprises make the network layout and design, they always have not pay enough attention to the data storage and backup management which are proposed rarely even ignored completely sometimes in the design. When the network is established, because of the deficiency of reliable data protection, once the accident occurs, the reparation is too late (Fan, 2006).

Therefore, except for the consciousness, we should pay more attention to the storage and backup of data in practice, and regard the data storage and backup as the first important thing, and adopt advanced data storage backup equipment to ensure the security of the network data in the possible range. The facts have proved that only complete data storage and backup will offer perfectly safe data security and protection for people.

There are two meanings of the data security. The one is the logic security, for example, to prevent the damage from virus and hacking, and the other is the physical security, for example, man-made mistake or irresistible disaster. The former needs the safety protection of the system, and the latter needs the protection of data storage and backup or disaster tolerance.

2. Analysis of reasons (Yu, 2006)

2.1 Virus and other malicious programs

The most familiar malicious program is virus which is the unauthorized code inserting in the legal program. After the computer infects virus, some programs or data can not be used, and usually we can use then antivirus software to kill viruses for the computer, and all problems will be solved. But sometimes the data losses induced by the malicious programs are very serious, and relative to the damage of the data files, the prevention and killing of viruses are always lagged.

2.2 Other maliciously damages by people

In other maliciously damages by people such as the hacking, hacker can use many measures such as the filching and cracking to possess enough operation right, and any data protection of the system will be not safe any longer. Only depending on normal deleting, moving, formatting and other operations can also destroy the data. Some users only create necessary password for their own user names, but for the "Administrator" with the highest limitation, the password is blank, so the any illegal user connected with the network can implement any operations in the system.

2.3 Hardware fault

Hardware fault is one of biggest reasons of data loss. The hardware fault and the unstable pressure always will make the computer automatically restarted. The hardware fault is the most serious problem, and it includes the physical damage, being stolen and so on, and the possibility of the data recovery will be zero.

2.4 Incorrect manipulation

The incorrect manipulations mean some destroying behaviors induced by unfamiliar computer operations, misunderstandings of clue information from the system. For example, quit when the files are not saved, the files or the corrections of the files will be lost, or take out or replace the U disk when editing the files in the U disk, which will induce the editing files destroyed or the files in the new U disk destroyed, or incorrectly deleting, or incorrectly formatting and so on.

3. Hard disk structure and disk storage principle

To know the data structure of the hard disk and the storage principle of files can help use understand and grasp the data recovery technology.

3.1 Data structure of hard disk (Liu, 2007 & Dai, 2003)

The hard disk is generally divided into five parts, i.e. the master boot sector and the DOS boot record, the file allocation table, the directory area and the data area. The master boot sector shares 512 bytes, and it includes the main boot record (MBR) and disk partition table (DPT). The function of MBR is to check whether the DPT is correct and which sector is the boot sector, and transfer the start program of this sector into the memory and exert it when the program ends.

Dos boot record (DBR) is the first sector which the operation system can be directly interviewed, and it includes the boot program and the sector parameter block which is called as BPB (BIOS Parameter Block). The main task of the boot program is to judge whether the former two files in the root directory are the root files of the operation system, read the first file into the EMS memory, and give the control right to the file. BPB parameter records many important parameters such as the start sector, the end sector, the file storage format, the disk medium descriptor, the size of root directory, the amount of FAT, the size of allocation unit (cluster).

FAT (File Allocation Table) is used to indicate the allocation of various clusters and cluster chains occupied by one file, and mark the bad cluster and the usable cluster. There are two FATs in the disk, and the first one is the basic table, and the second FAT is the backup of the first FAT, and their sizes are decided by the size of the sector and the size of the file allocation unit. DIR (or FDT, i.e. File Directory Table) records the start unit and the file attribute of every file (directory). Data area is the real data storage area, and it occupies most space of the disk. Data in the Data area are explained by FDT and FAT, and if FDT and FAT describe the Data area as the “unused”, the corresponding Data area is the “unoccupied” free space which can be written by new data.

3.2 Data storage principle

When the operation system saves the files, it first find the free space in the FDT to write relative information including the file name, the file size and the created time, and find the free space in the Data area to save the files, and write the number of the first cluster of the files in the Data area into FDT, or write the number of the last cluster in the Data area if the files end, and write the end mark in the last cluster of Data area. When reading the file, the operation system reads the file name, filename extension, file size, data modification, and the cluster number of the first cluster saved in the Data area and other information about the file in FDT, and read the data of corresponding cluster number in the Data area according to the cluster number in FDT, and find the corresponding unit of FAT, and if the content is the file end mark, the file ends, or else, save the cluster number of next cluster of data, and in this way, repeat the process until the file end mark occurs.

Through understanding the influences of the data storage structure and various operations to the disk data, we can understand why we can find the data back when the data are destroyed and there are no new data covers, which is the possibility of data recovery.

4. Usual data fault treatment methods

Data recovery can be divided into the pure software recovery and the recovery with the combination of software and hardware. There are many single data recovery software such as Easy Recovery, Disk Genius and so on. Different software programs have different advantages and disadvantages, and we can reasonably select and use them according to the practical situations.

4.1 The system can not find the hard disk

Most these faults occur in the connection cable or the port of IDE, and the fault rate of the disk is rare, but it will induce the system can not be started from the disk, and even can not enter into the disk C when starting from disk A, and the automatic test function of the CMOS can not find the disk too. We can find the fault by the replacement experiments such as re-plugging or re-pulling the disk cable or exchanging the IDE port and cable.

4.2 Recovery of incorrect data deletion

Start Easy Recovery, click the “data recovery”, and enter into the main menu of data recovery. Select “deleting the recovery”, and the deleted files can be recovered. Select the sector where the files are in, and if only recovering one or

two files, the quick scanning in the fault should be selected, and if recovering the whole directory containing subdirectory and files, the complete scanning should be selected. Click the “next”, the system will scan the selected directory. When the scanning finishes, all recovered file information will be displayed on the screen. We can select the files what we want to recover like using “the resource manager”, and click the “next”. Because Easy Recovery needs not to reread the disk when recovering the data, the software only mirrors the FAT and the directory tables in the EMS memory, all recovered files are stored in the EMS memory, so we should select the place storing these files and write the recovered files in the memory on the disk.

4.3 Data recovery after formatting

If the files are deleted because of incorrect manipulation, we need to select “formatting recovery”, and other operations are similar with the “deleting recovery”. For the instance which the partition table is destroyed, Easy Recovery cannot recover the partition table information in disk, but scan the disk according to the cluster, and put the recovered files into different folders by the file type, which provides a sort of new data recovery method for us. When the partition table of disk is destroyed seriously, and we cannot use other recovery software to recover it, we can use this method. But for some big files, because they may be stored in multiple discontinuous clusters, and if the data are not recovered by the partition table, the recovered files may be incomplete. So we should first recover the disk partition table possibly and then recover the data.

5. Conclusions

Any one data recovery solution can not ensure to recover all data. To really protect the data, the most important work nips in the bud. The daily works include installing the anti-virus software and firewall and updating in time to prevent the invasion of viruses, maintaining the computer in time to prevent the system halted, avoiding the file loss induced by incorrect manipulation and other man-made factors, using disk defragment usually to make the data in the Data area continually stored possibly and largely enhance the success rate of data recovery, and especially paying attention to the effective backup of important files which is relatively simple and reliable.

References

- Dai, Shijian & Chen, Yonghong. (2003). *Technology of Restoring DB*. Beijing: Publishing House of Electronics Industry. August of 2003.
- Fan, Hong. (2006). Briefly Description of the Information Security Risk Evaluation Standards. *Netinfo Security*, No. 1.
- Liu, Sanman. (2007). Analysis on Data Restore Technology of Computer. *Shanxi Electronic Technology*, No.1.
- Yu, Jinyun & Luo, Yixin. (2006). Current Status of China's Information Security and Study on Countermeasures. *China Safety Science Journal*, No.1.