DOS 磁盘文件系统的恢复方法

陈长法　　(中国地质大学)

摘要:本文介绍一种方法,使磁盘文件系统在遭到严重破坏时,如何巧妙地利用 *PCTOOLS* 中的 *Undelete* 功能,快速、准确、全面地恢复磁盘上的整个文件系统。

当磁盘文件被误删或遭到某种破坏时均可利用 PCTOOLS, NORTON 或 DOS5.0 中所提供的 Undelete 功能恢复文件,但当磁盘上最重要的数据区:主 BOOT-主引导扇区(仅硬盘有),BOOT-引导扇区,FAT-文件分配表,ROOT-根目录区这四个部分的数据在未采取保护性备份的情况下,遭到病毒的攻击或其它破坏时,以上软件的文件恢复功能就无能为力了。

上述四个部分的数据被破坏有如下几种情况:

1.主 BOOT 区数据被破坏,此时整个硬盘系统瘫痪。当用户试图进入硬盘,就会出现提示"invalid drive specification"(非法驱动器指定)。若该扇区数据以前未作备份,就必须用 FDISK 命令对硬盘重新分区;

2.BOOT 区数据被破坏,系统就不能从硬盘自举,某些汉化软件不能正常工作,此时只好重新格式化磁盘了;

3.FAT 表和 ROOT 区数据被破坏,就会使系统无法读写文件,这两个区域通常是某些破坏磁盘文件的恶性病毒攻击对象。

一、磁盘结构

磁盘被格式化后,其结构如图 1 所示,图中最上一部分仅硬盘有。

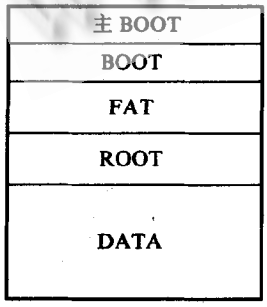


图 1　磁盘结构

1.主 BOOT 区-即主引导扇区,占用物理 0 头 0 柱 1 扇区,该区存放着引导硬盘活动分区的主引导程序和硬盘逻辑分区情况表,该表具体记录了 DOS 引导盘的逻辑盘号/建立在 DOS 扩展分区上的逻辑盘号,大小容量和起始物理地址,是硬盘上最重要的系统数据扇区,其数据由硬盘低级格式化命令和磁盘分区命令 FDISK 产生建立。因此,软盘没有此扇区。

2.BOOT 区-即引导扇区,也包括一个主引导记录(但没有主引导程序),分区引导记录,该记录存放着下一个逻辑盘的链接表。对于 DOS 活动盘,还存放着系统自举时的 DOS 引导程序。该扇区数据由 FORMAT 命令产生建立,占用每个盘的逻辑 0 扇区。

3.FAT 表-即文件分配表,可变长度,视磁盘空间大小占用不同的扇区数。该表记录了磁盘空间的分配情况和每个文件的具体分配地址。

4.ROOT 区-即根目录区,可变长度,用于存放根目录下的文件名或一级子目录名。

5.DATA 区-存放具体文件内容或子目录名的数据区。

二、文件的读写过程

磁盘空间是以簇(Clust)为单位进行分配的,一个或多个扇区(Sector)作为一簇,对于软盘,高密(1.2M);1Clust=1Sector,低密(360 K);1Clust=2Sector,一般硬盘为:1Clust= 4 Sector,视具体系统而定,磁盘上的每一簇号均在 FAT 表中有相应的登记项,以标明该簇的使用情况。该登记项在小于 16M 的硬盘和高密软盘上占用 1.5 个字节,在大于 16M 的硬盘和低密软盘上占用 2 个字节。FAT 表的前二项(即第 0,1 项,占第 0-3 个

字节)是该表的表头。第0个字节存放磁盘介质说明符,说明磁盘的性质和规格(见表1),第1-3个字节由系统规定为FF FF FF。从第2项(第4,5字节)开始登记第二簇的使用情况,第3项(第6,7字节)登记第三簇的使用情况,依此类推,磁盘上每一簇在FAT表中均对应着唯一的一个登记项。因FAT表的前二项被系统占用,故磁盘上DATA区的起始簇号总是从2开始的,若某一簇已被使用时,就在FAT表中相应的登记项填上标志,各标志的含义见表2,当文件需要多于一簇的空间时,便在FAT表中形成一个簇链表,具体向磁盘上写文件时,先在文件目录表填写文件目录项。然后到FAT表中查找未被使用的磁盘空间(簇号)写入文件。

表1 FAT表头标志含义

说明符	含 义
FD	5(1/4)″低密盘(360K)
F9	5(1/4)″高密盘(1.2M)或3(1/2)″低密盘(720K)
F0	3(1/2)″高密盘(1.44M)
F8	硬盘

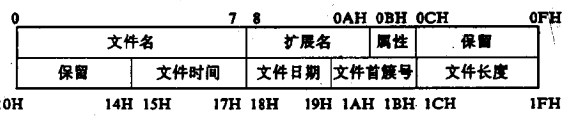
表2 FAT表中登记项各标志含义

标志符	含 义
0000H	可供分配的簇
FFF0-FFF6H	保留簇
FFF7H	坏簇,不分配
FFF8-FFFFH	文件结束标志簇
××××	即除上述之外的任何字符,指文件下一簇编号

ROOT区只作为根目录下的文件目录表填写根目录下的文件名和一级子目录名,子目录的文件目录表均被任意分配到DATA区,其文件目录项结构都是一致的,但子目录的文件目录表开始的前二个文件名为"＊"　"＊＊",分别表示父目录和子目录,子目录名仍然按文件名一样填写文件目录项,但有二项填法不同。

每个文件目录项占32个字节,其结构如表3所示。

表3 文件目录结构表



其中:(1)属性—规定文件存储读写方式,对于目录名,规定为"10";

(2)文件首簇号—即分配给文件的起始簇号,对于子目录名,则为存放它的文件目录表的起始簇号;

(3)文件长度—即文件所占磁盘空间的字节数,对于子目录名,该项全为0文件被删除时,只是将该文件目录项第0个字节改为ES,并将它占用的簇号在FAT表中对应的登记项全改为0,以标志该空间释放,恢复文件实质上是将文件目录项中ES改为正确文件的第一个字符所对应的代码,并在FAT表中恢复被清0前的字符,显然使用手工方法将是一个非常烦琐和小心的事,但这一步可借助PCTOOLS或EDOS5.0中的Undelete功能完成。

对磁盘进行格式化时,仅仅只是将FAT表中除系统保留的前四个字节外,其余全部清0,但对检查出的坏扇区,则在FAT相应位置填上坏簇标志FFF7H.同时也将ROOT区全部清0,对DAT区的数据不作任何改动,即使是专毁坏磁盘数据的恶性病毒,一般也只破坏FAT表,ROOT区和DATA区前面的一些数据,因为要改写整个磁盘必须用较长的时间。

因此,只要DATA区的数据未被破坏,就有恢复的可能。

三、具体恢复方法

(一)BOOT区或FAT表,ROOT区数据被破坏

1.子目录下文件的恢复(为方便恢复,任何子目录下的文件都作为一级目录文件恢复)

(1)格式化磁盘:FORMATC:↓,之后不要往盘上拷贝任何文件;

(2)查找子目录文件目录表的起始簇号,具体方法:

A.从软盘上运行低版本PCTOOLS,如4,3版;

B.按F3选择磁盘字节查找功能"FIND";

C.输入查找字串"＊＊"或该子目录中唯一具有的一个文件名。

D.查找暂停后,按"E"键查看是否已找到了待恢复的文件目录表,若是,则记下它的簇(CLUST)号,若不是,则继续查找;

(3)将存放文件目录表的簇号转换为16进制数;

(4)按F3选择磁盘字节编辑功能"VIEW／EDIT",进入ROOT区填写文件目录项;

A.在0—0AH字节用16进制字符任意填写一个子目录名(但不与其它文件名重复),剩余项改为"20";

B.将属性项(0BH字节)改为"10";

C.在文件首簇号项(1AH—1BH字节)按低位在前,高位在后的次序填写文件目录表的存放簇号,如簇号为2125(=66AH),则该项填写为"6A06";

D.文件长度项(1CH—1FH字节)仍为0,其余各项也可保持为0;

E.将以上修改存盘,退出该功能。

(5)在PCTOOLS状态下重选C盘,即显示刚填写的子目录及该子目录下的全部文件名;

(6)打印全部文件名,供恢复文件时间;

(7)删除子录下的所有文件名;

(8)进入PCTOOLS的文件恢复功能Undelete,按照提示逐个恢复刚删去的文件。

至此,即巧妙地借助PCTOOLS的Undelete功能达到了快速恢复文件的目的。

2.原根目录下单个文件的恢复

由于根目录下的文件,其文件目录项是存放在ROOT区的,一旦磁盘格式化后,这些数据均遭破坏,故恢复较前述麻烦,具体方法如下:

(1)同上1,(1),FORMATC:

(2)查找文件存放的起台簇号,最好选择被恢复文件中唯一具有的一个字符串用PCTOOLS中的"FIND"功能确定该文件的起始簇号(Clust);

(3)找到它的起始簇号后,同时计算文件所占磁盘字节总数;

(4)将起始簇号和文件长度转换为16进制数;

(5)进入到磁盘ROOT区,填写文件目录项;

A.将该项最前一字节(0字节)改为E5(文件被删除标志,以使用Undelete恢复时识别),随后填写文件名的16进制代码,剩余部分改为"20";

B.属性项(OBH字节)改为"20";

C.IAH—IBH字节填写文件的首簇号;

D.1CH—1FH字节填写文件长度。ICH和IDH字节分别填写文件长度后四位数中的低二位和高二位,1EH和1FH则填写文件长度前四位数中的低二位和高二位,如若文件长度为107204(=1A2C4H),则1CH—1FH字节写为"C4A 20100";

E.其余各项均可保持为0;

F.将以上修改存盘退出.

(6)进入PCTOOLS的Undelete功能,刚填写的文件各显示在可被恢复文件之列。根据提示恢复该文件。

这样就完成了单个文件的恢复。

(二)主*BOOT*区数据被破坏

这时由于磁盘逻辑分区参数被破坏,必须用FDISK命令对硬盘重新进行分区,新的分区参数必须和原分区参数一致。因FAT表和ROOT区所占扇区数与磁盘的大小容量有关,磁盘容量越大,FAT和ROOT所占扇区数越多。若新分区与原分区参数不一致,就会使新FAT和BOOT所占扇区数可能与原来的不一致。若如此,就会导致DATA区的起始扇区号与原来的也不一致,而磁盘分配中的开始簇号2总是从DATA区的起始扇区开始计算机,因此就会出现在新分区中,第三簇对应比如说是第153扇区,而在原分区中可能对应的是第149扇区,其结果是对于恢复子目录中的各文件时,按原磁盘分配填写的文件目录项中的"文件首簇号"在新磁盘分区中是完全错误的。同时也可能出现在同一簇号的四个扇区或二个扇区中存放着二个都需要的不同文件的信息,但按文件管理方法,这是不行的,此时无论如何也不能使文件恢复成功。

因此,主BOOT区数据破坏扣恢复文件时,用FDISK对磁盘分区过程中,如何选择与原分区较一致的参数是后面恢复文件的关键问题。

完成FISK后,其后方法与"(一)"中所述一致。

对于某些不是按连续空间存放的文件,在使用Undelete功能时,必须按提示用手工的方法恢复,由于这个过程容易出错,为了不影响其它文件的正常恢复,这样的文件最好在最后恢复。

参考文献:

沈永耀,陶铮正编,《磁盘文件管理与加密原理》,中国科学院希望高级电脑技术公司,*1990.9*