用 WinHex 分析 FAT32 的磁盘存储结构

蒋　波,付尚朴,孙　琛

(中国工程物理研究院 职工工学院,四川 绵阳 621900)

摘要:在硬盘修复、数据恢复和教学实验中,需要研究文件系统的磁盘存储结构,WinHex 是能满足这一需求的较好软件,作者显示了用 WinHex 来分析 FAT32 文件系统的方法。

关键词:WinHex;FAT32;FDT;簇

中图分类号:TP363.3　　文献标识码:A　　文章编号:1671 - 5365(2006)06 - 0077 - 02

在微机组装与维护等课程的磁盘存储系统教学中,通常教材要对磁盘分区、文件分配表 FAT 与文件目录表 FDT 等进行理论描述,但只有通过对文件在磁盘上的具体存储结构进行实验分析才能加深对这些概念的理解,WinHex 就是能满足这种需求的一种磁盘编辑软件,在我们的教学实践中取得了很好的教学效果,同时它也是硬盘修复和数据恢复的一个重要工具,这个软件可以从网上免费下载,下面用它来分析 Windows 系统常用的 FAT32 文件系统的文件存储结构。

我们知道,一个物理硬盘包括主引导记录 MBR 和多个分区,分区也被称为逻辑盘,如一个物理硬盘可划分成 C,D,E…多个逻辑盘,下面的讨论限制在一个 FAT32 逻辑盘上,作为示例,在这个逻辑盘的根目录下创建一个名为 TEST.DOC 的文件,大小为 61440 字节(60k)。

1　DOS 引导记录(DBR)

FAT32 文件系统在逻辑盘上的结构如图 1 所示。

DBR(保留扇区)	FAT1	FAT2	DATA(含 FDT)

图 1　FAT32 各区域的关系图

其中,保留扇区的数目、FAT 的大小和根目录 FDT 的位置在 FAT32 下不再是固定的,但它们可以从 DBR 中的 BPB 参数块获得,图 2 给出了 WinHex 所显示的逻辑盘引导扇区 DBR 的部分内容。

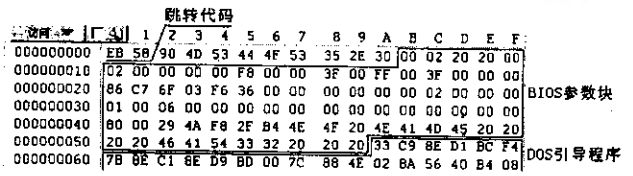

图 2　FAT32 逻辑盘引导扇区部分内容

偏移 0 处的跳转指令将程序执行流程跳转到偏移 5A 处的 DOS 引导程序入口,这里不详细分析引导代码。BPB 参数块从第 12(0BH)字节开始,占用 80(0BH ~ 5AH)字节,前面提到的一些重要参数在 BPB 中的偏移及值如表 1 所示。

表 1　BPB 参数的部分字段及意义

偏移	长度	值	说　明
0D	1	0x20	每簇扇区数
0E	2	0x20	保留扇区数
1C	4	0x3F	隐含扇区:从硬盘 LBA = 0 至 DBR 的扇区数
24	4	0x36F6	每 FAT 扇区数
2C	4	0x02	根目录 FDT 在 DATA 区的起始簇位置

由表 1,该逻辑盘每簇有 32(0x20)个扇区,簇大小为 32 × 512 = 16k,保留扇区数是 32,这也是图 1 中 FAT1 的起始扇区编号,DATA 区的起始扇区为 0x20 + 2 * 0x36F6 = 28172,根目录 FDT 在 DATA 区的起始簇为 2。

2　根目录 FDT

用 Format 命令进行高级格式化时,为(逻辑)磁盘建立了一个根目录文件目录表 FDT,在根目录下用户可以再创建不同的子目录或文件,根目录以及各个子目录都有自己的 FDT,FDT 定义了文件名、文件大小以及文件存放的起始簇号。我们用 WinHex 来分析 TEST.DOC 在根目录 FDT 中的目录登记项。

首先要在 WinHex 中定位出根目录 FDT,单击 WinHex 显示内容中的"访问"下拉列表的"根目录"项可直接到达根目录 FDT 的起始偏移,参考图 1 也可计算出起始偏移,计算公式为:

根目录 FDT 起始偏移字节 = (保留扇区数 + 2 × 每 FAT 扇区数 + (FDT 起始簇号 - 2) × 每簇扇区数) × 每扇区 512 字节

其中"起始簇号 - 2"是因为 FAT 中第 0 簇和第 1 簇为保留簇,起始簇号从 2 开始。根目录下的所有文件及其子目录,在根目录 FDT 中都有一个 32 字节的目录登记项,目录登记项部分字节的内容如表 2 所示。

根据文件名可在根目录 FDT 中找到 TEST.DOC 文件的目录登记项,图 3 显示出它的全部内容。

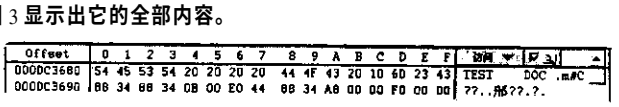

图 3　TEST.doc 在 FDT 中的目录登记项

收稿日期:2006 - 04 - 19

作者简介:蒋波(1963—),男,四川绵阳人,讲师,学士,主要从事计算机组成原理与接口研究。

表 2 FDT 中文件目录项的部分内容及含义

字节偏移	字节数	内容及含义
0 ~ 7	8	用于表示文件名字
8 ~ 0AH	3	用于表示文件的扩展名
0BH	1	按二进制位定义的文件属性,如只读位、系统位、隐藏位、子目录位等,0FH 表示该项为长文件名记录项。
14H ~ 15H	2	文件起始簇号的高 16 位
1AH ~ 1BH	2	文件起始簇号的低 16 位
1CH ~ 1FH	4	32 位文件字节长度

从相对偏移 14H ~ 15H、1AH ~ 1BH 可读出 TEST.DOC 的起始簇号为 0B00A8H,相对偏移 1CH ~ 1FH 指出文件大小为 F000H 字节(61440 字节)。

3 文件分配簇链

文件分配表 FAT 是用来记录每个文件的存储位置的表格,操作系统以簇为单位给文件分配磁盘空间,每个簇在 FAT 表中占有一个登记项,簇编号也是登记项编号,对 FAT32,每个登记项占用 4 个字节(32 位),0 号登记项和 1 号登记项是表头,簇的登记项从 2 开始,表项值 00000000H 表示未使用的簇,00000002H ~ FFFFFFEFH 表示一个已分配的簇号,FFFFFF0FH 表示文件结束簇,FFFFFFF7H 表示坏簇等,但注意要高字节在后地读出已分配的簇号。一个文件至少占用一个簇,当文件占用多个簇时这些簇的簇号不一定是连续的。

在用 WinHex 观察簇号链时,同样首先要定位出 FAT 的起始偏移,单击 WinHex 显示内容的"访问"下拉列表中的"FAT1"项可直接进入 FAT1 表,用保留扇区数 × 512 也可计算出 FAT1 的起始偏移字节为 4000H,前面已确定出 TEST.DOC 的起始簇号为 0B00A8H,每个登记簇项占用 4 个字节,由此可确定出 TEST.DOC 第 1 个簇登记项的起始字节偏移为 4000H + 4 × B00A8H = 2C42A0H,图 4 显示出 TEST.DOC 的簇链。

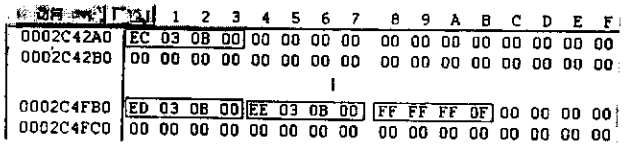

图 4 TEST.DOC 的簇号链

由图可知第 1 个簇登记项的值为 0B03ECH,这也是第 2 个簇的簇号,第 2 个簇登记项的起始字节偏移为 4000H + 4 × B03ECH = 2C4FB0H,它的登记项值是 0B03EDH,依此类推可得出文件 TEST.DOC 被分配的簇号链是 B00A8H、B03ECH、B03EDH、B03EEH 共 4 个簇,图 4 也清楚地显示 B03EEH 簇的登记项值 FFFFFF0FH,它指出文件结束簇。TEST.DOC 的文件大小是 60k,但它占据了四个簇大小(64k)的磁盘空间。

4 文件的删除

许多人可能认为在删除文件时,系统会把被删除文件的内容全部清出,实际情况并不如此。在删除文件时,系统只是在该文件的文件目录项上做一个删除标记,把它们在 FAT 表中所占用的簇标记为空簇,即登记项值为 0,而 DATA 区域中仍旧保存着原文件的内容,只是在操作系统下不借助专门程序或软件是看不到它们的。例如,用 Shift + Del 键把前面的 TEST.DOC 文件不放入回收站而彻底删除,在根目录 FDT 中仍可找到如图 5 所示的目录登记项。

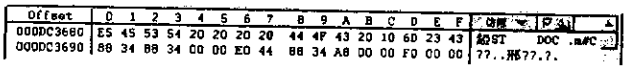

图 5 文件删除后 TEST.DOC 的目录登记项

将图 5 与图 3 相比较,可见除文件名的第 1 个字符改为删除标记 E5 外,目录登记项的其余字节完全相同,从这个登记项仍可读出起始簇号、文件大小等信息,如果文件较小只占用 1 个簇,或文件分配的簇是连续的,用 WinHex 可容易地把彻底删除的文件复原,若文件分配的簇是不连续的,则复原要困难一些。

5 结语

用 WinHex 还可分析子目录管理以及在 Windows9x 以后引入的长文件名实现,在 WinHex 中可以把修改的字节内容写回磁盘扇区,被病毒破坏引导扇区的硬盘可用 WinHex 进行修复,因此,WinHex 不仅是硬盘修复与数据恢复的实用软件,也是一种很好的教学实验软件。

参考文献:

〔1〕戴世剑,涂彦晖. 数据恢复技术〔M〕. 北京:电子工业出版社,2005

〔2〕宋群生,宋亚琼. 硬盘扇区读写技术——修复硬盘与恢复文件〔M〕. 北京 机械工业出版社,2004.

To Analyze On – disk Structure of FAT32 Using WinHex

JIANG Bo, *FU Shang – pu*, *SUN Che*

(CAEP Institute of Technology, Mianyang 621900, China)

Abstract: Disk repair, data recovery and teaching experiments all require the research of the on – disk structure of file systerm. Hence, WinHex is the good software to satisfy such requirement. The method using WinHex to analyze FAT32 file system is discussed in the article.

Key words: WinHes; FAT32; FDT; Cluster