硬盘系统资源分析及应用

李晓华 （云南省军区自动化站）

摘要：本文详细讨论和分析了硬盘系统资源，对硬盘存储空间作了划分。对主(总)引导记录、*DOS* 分区引导记录、文件分配表 *FAT*、根目录扇区作了全面的剖析。了解和掌握硬盘系统资源对初学者和各级计算机管理人员在分析和排除计算机软故障、防止和发现计算机病毒都具有十分重要的实现意义。

一、引言

目前计算机的使用人员中多数都不是计算机专业人员，对计算机的内部结构及工作原理没有更多的掌握和了解，以致于当计算机病毒入侵、硬盘系统资源丢失之后，不知如何下手。笔者认为，这此问题都与硬盘系统资源有关。了解和掌握硬盘系统资源，对计算机操作和管理人员来说是非常重要的。

二、硬盘系统资源

1.物理扇区、逻辑扇区

在分析硬盘系统资源之彰，先看看与硬盘操作非常密切的 2 个容易混淆的概念：

(1)物理扇区号：它是按照磁道(柱面)、磁头、扇区的三维物理位置而过行编址的，通常从 1 开始编号。它适用于整个硬盘，用 BIOS 的 INT 13H 进行磁盘操作。

(2)逻辑扇区号：它不是笼统指硬盘扇区，而是把所有的扇区排序后，用它表示从硬盘边沿算起的某一扇区的位置。它是对分区而言，从 0 开始连续编号。通常用 DOS 的 INT25H / INT26H 进行读 / 写操作。

请注意，按 DOS 分配硬盘逻辑扇区的原则，连续的逻辑扇区在磁盘上可能不对应连续的物理扇区，这取决于低级格式化硬盘时所选用的交替因子。这个交替因子在两个逻辑扇区之间规定物理扇区号。

在实际应用中，通常所使用的是逻辑扇区，而实际上最后对硬盘操作的是物理扇区号。通过下列几个公式能实现把逻辑扇区转换成物理扇区，即 int13H 的入口地址参数：

磁道号＝[逻辑扇区号 / 每道扇区数]MOD 磁头数

扇区号＝([逻辑扇区号 / 每道扇区数] / 磁头数)

扇区号＝(逻辑扇区 MOD 每道扇区数)+1

其中 MOD 是取余数操作

实现程序

```
; 功    能：计算 INT13H 入口参数
; 入    口：AX＝逻辑扇区号
;           SectorsTrack＝磁头数
;           NumberofHead＝每道扇区数
; 出口参数：NS＝扇区号；NH＝磁头号；NC＝磁道号(柱面)
Set-int13-in  prog
              xor dx, dx
              div word prt ds: SectorsTrack
              nc dl
              mov ds: NS, dl
              xor dx, dx
              div word otr ds; NumberofHead
              mov ds: NH, dl
              mov ds: NC, ax
              ret
Set-int13-in endp
```

2.硬盘物理格式化

硬盘的物理初始化通常由厂方在出厂时已经完成，但当机器出现软故障(错误的系统信息、系统信息丢知、硬盘面损坏、试图装入不同的操作系统等)、计算机病毒入侵后，造成计算机工作异常。此时必须对硬盘进行修复。根据在实践工作中所遇到的情况，往往出现机器异

常时，不是由于机器硬件所致，而是由于软故障造成的。此时可通过低级格式化便能修复。笔者总结了实现硬盘低级格式化的几种方法，供读者参考：

(1)利用 BIOS INT 13H 实现硬盘低级格式化。

a、05 号功能实现单条磁道的格式化：下列程序能对硬盘 0 面 0 道 0 扇区进行低级格式化。

```
A>DEBUG
-A  XXXX:100  MOV AX,0500   (05号功能)
              MOV DX,0080   (硬盘)
              MOV CX,0001   (0道1扇区)
              MOV BX,200    (参数表)
              INT 13
              INT 3
-E  200:      0     0     1     2
```

磁道号 磁头号 扇区号 512 字节(字节／每扇区)

b.07 号功能：实现整个硬盘的低级格式化

```
A>DEBUG
-A  XXXX:100 MOV、 AX,0703 (03为交替因子)
             MOV   DX,0080
             MOV   CX,0001
             INT   13
             INT   3
```

(2)利用 ROM-BIOS 中的硬盘格式化程序通常在硬盘控制板上的 ROM-BIOS 程序(系统规定它的起始地址为 C800:0000)中都有一个硬盘初始化程序。其入口地址为 C800:XXXX(每种机器的入口地址是不同的)。为寻找有效的硬盘控制程序，必须查看 C800:XXXX 地址程序段前几个字节是否为：第 1 字节 55H、第 2 字节 AAH、第 3 字节 ROM 程序长度、第 4 字节 EBH 一定是一条 JMP 指令。具体如下：

```
a.C>DEBUG
  -D C800:0003-000F
```

查看 C800:0003-000F 单元中的内容。以确定适配器的 ROM。

b.用反汇编把 C800:0003-000F 之间的目标码反汇编出来。

c.查看 JMP 转到硬盘低级格式化程序的首地址 C800:XXXX。通常 2-3 条 JMP 是 08XX，其中 JMP 开始的指令为 ROM 中硬盘低级格式化的入口地址。

d.执行低级格式化程序：

```
  -G=C800:XXXX(其中 C800:XXXX 对应 JMP 08XX-行)
```

(3)使用磁盘管理程序 LOWFORM 和 DM 实用程序。使用 LOWFORM 程序实现对 8088／8086 系列机的低级格式化，DM 程序实现对 286 以上机器的低级格式化。

(4)利用随机软件提供的诊断程序。在随机提供的诊断软件中有一个硬盘格式化菜单程序，选择条件或无条件格式化便能实现对硬盘低级初始化。

(5)利用机器本身提供系统设置过程中的低级格式化程序。在一部分机器中，系统的设置过程中有低级格式化程序。利用其格式化程序，便能实现低级格式化。

硬盘的低级格式化是一次复杂的过程，一般用户不要做。只有当确认非必要做时，才能对硬盘进行低级格式化工作。所有硬盘初始化工作除建立必须的硬盘格式外，便是在硬盘上建立主引导程序和分区信息表，当然硬盘数据将全部丢失。

在完成初始化和分区后，可由相应的磁盘格式化程序(如 DOS 操作系统用 FORMAT，CM-P／86 操作系统用 NEWDISK 程序)实现磁盘的高级格式化。高级格式化的目的除划分磁盘必须的格式外，主要是在相应分区的前导写上相应的引导程序和有关的信息标志。如 DOS 操作系统除写上 DOS 分区引导程序外，同时还建立文件分配表 1、文件分配表 2、根目录等系统信息。如图 1 所示。DOS 操作系统在格式化的同时，还将两个系统隐文件(IO.SYS MSDOS.SYS)写到根目录的最前导位置。最后把命令处理器文件(COMMAND. COM)拷入到硬盘。至此整个过程完成，硬盘便可正常工作了。

3.硬盘系统信息及分区信息

硬盘的一般存储格式由 2 大部分组成：即系统信息占用扇区和正文数据占用扇区，如图 1 所示。系统信息占用扇区通常由主引导扇(MBR)、DOS 分区引导扇(DOS-P-R)、文件分配表(FAT)、根目录占用扇区(RD)4 个部分组成。

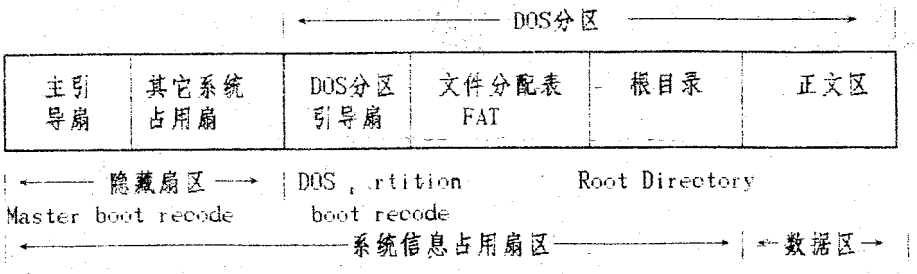


图 1 硬盘系统资源占用扇区情况

在硬盘使用前，一般已在厂家进行了物理初始化和分区。通常一个硬盘有 4 个分区，以便用于不同的操作系统。如 DOS 操作系统 XINX 操作系统、CP-M／86 的操作系统等。每一种操作系统在硬盘上建立自己的分区时都要由一个相应的实用程序来完成。如 DOS 分区要用 FDISK 实用程序、CP-M／86 分区要用 HDMAIHT 实用程序，以实现分区大小、数目、“活动标志”的控制。硬盘的 4 个分区见图 2 所示：

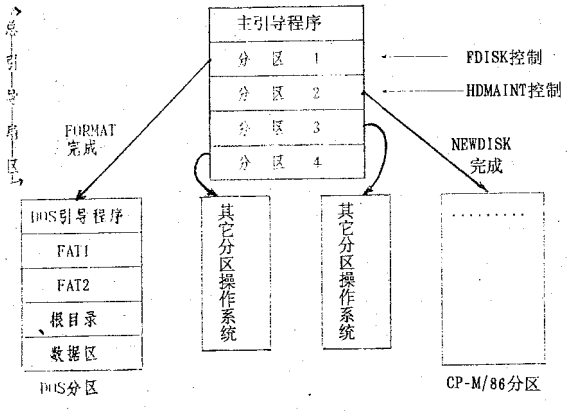


图 2 硬盘分区信息

4.隐藏扇区及其应用

这一部分区域存放主引导程序（通常又称总引导程序）。一般隐藏扇区由一个到十几个扇区组成（根据硬盘容量而定）。主引导程序是入在 0 面 0 道第 1 扇区，其它扇区做为保留和备用。见图 3 隐藏扇区的划分。

要对这部分扇区进行读／写操作，只能用 BIOS 的 INT 13H 中断程序，而不能用绝对读／写中断程序。由于这部分扇区得不到 DOS 的控制，因而用 DOS 操作系统的 FORMAT.EXE 格式化程序已不能对该区域进行格式化。这就是 FORMAT 格式化程序不能清除系统型病毒的关键所在（通常系统型病毒的引导部分和感染部分都存入于隐藏扇区内）。

可以利用其这部分中的空余区域编写硬盘加密程序，防止计算机病毒的入侵，以保护硬盘数据的安全。具体程序请见《计算机系统应用》1993 年第 2 期“一种实用的硬盘加锁程序 李晓华”。

在隐藏扇区中，主引导扇区是一个非常重要的部分，它的主要任务之一就是找到被标记这种“活动”的分区，即引导标志为 80H 字节的分区，然后把控制权交给该分区所对应的分区引导程序。

为恢复硬盘主引导记录，可以在机器正常时把主引导记录备份下来，当机器异常时再恢复。如下所示：

读出主引导记录	重写主引导记录
A＞DEBUG	A＞DEBUG
-A100:XXXX MOV AX,0201	-A100:XXXX MOV AX,0301
MOV CX,0001	MOV CX,0001
MOV DX,0080	MOV DX,0080
MOV BX,200	MOV BX,200
INT 13	INT 13
INT 20	INT 20
-G	-G
-N A:BOOT.COM	
-R:CX	
512	
-W	

5.DOS 分区引导扇

分区引导记录占用相对 DOS 分区的第 1 扇区，当主引导程序判定硬盘有效后，根据分区信息表的“活动”标志，转去相应的分区引导程序，并把控制权转交给它。

在 DOS 分区格式时，在磁盘上产生如图 4 所示的格式：

BPB 参数块由 DOS 外部命令 FORMAT 程序记录在盘的引导偏移为 OBH-1DH 处，总 19 字节，其初值固化在 ROM-BIOS 芯片中。加电时，由 ROM 初始化程序根据控制板上的 DIP 开关来选择对应的表入口，并存于 INT 41H 中断向量中。ROM 自举程序依据此表对硬盘驱动器进行初始化工作。并把它送入控制器中，控制器将根据参数表来控制硬盘驱动器。

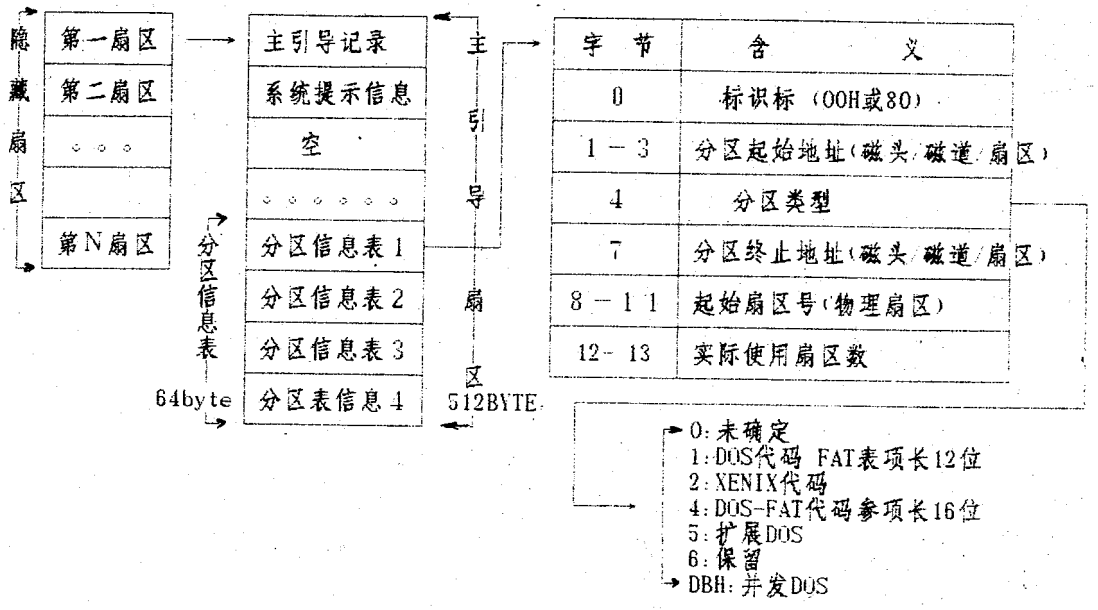


图 3　隐藏扇区及其信息

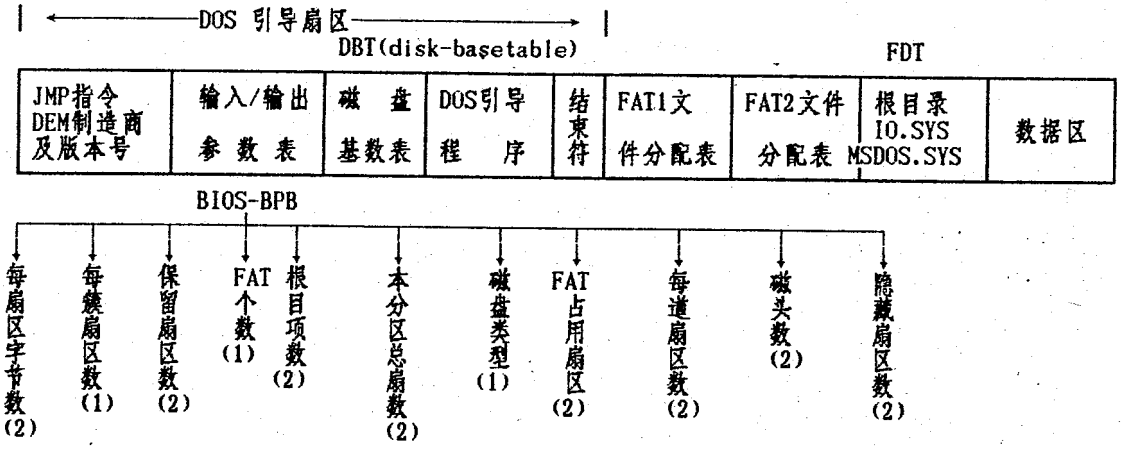


图 4　*DOS* 引导扇区及其信息

从图 4 中可以看出 DOS 引导扇区有四部分组成：即转移到引导程序的指令及制造商和版本号；输入输出参数块、磁盘基数表；DOS 引导记录；结束标志。DOS 引导记录主要任务之一是检查两个系统隐藏文件是否存在、有效位置是否正确。如异常出现错误提示信息。如正确则读入系统文件，并把控制权转向 IO. SYS，由 IO. SYS，由它去执行命令处理程序，最后出现操作提示符。

在 DOS 引导扇中，除 DOS 记录外还有 2 张非常重

要的表即 BIOS BPB 参数表，它记录了硬盘介质特性的物理参数，供 DOS 管理文件使用。另一张为磁盘基数表 DBT(Disk-BaseTable)，是供硬盘驱动程序直接控制硬盘使用的。

对于各种硬盘，其 DOS 分区引导程序是一样的，只是磁盘结构参数表中的有些内容不同。由于 DOS 分区引导程序不存在隐藏扇区，而是放在逻辑扇区号为 0 的位置。然而它不是一定存放在硬盘的第二扇区。主要原因是，一方面硬盘存在有隐藏扇区，另一方面 DOS 分区不一定在硬盘的第一个分区。至于 DOS 引导程序在第几扇区，要通过查看 DOS 分区信息表中的分区起始扇区号而定。

用 DEBUG 的 L 直接读出 DOS 引导扇	用 INT13H 读出引导扇:
C>DEBUG	C>DEBUG
-C XXXX: 0 2 01	-A> XXXX:100 MOV AX,0201
| | |	MOV CX,0012(物理扇区)
逻辑扇区号 C盘 扇区数	MOV DX,0080
	MOV BX,200
	INT 13
	INT 20
	-G
	20M 硬盘 DOS 引导扇从第 18 个扇区

可以利用其 DOS 引导扇区存放一些系统和应用程序，如修改 BIOSBPB 参数块中的参数，实现对磁盘的加密。或者利用 JMP 指令后的位置存放硬盘口令，以实现硬盘数据的保护。

6.文件分配表 FAT 占用扇区

文件分配表记录每一个文件的分配情况，它是以簇为单位进行分配的。为确保文件操作的可靠性，DOS 设置了 2 份内容完全一样的表。每个表包括四个方面的内容：即磁盘类型、扇区使用情况、扇区封锁信息、文件的簇号。

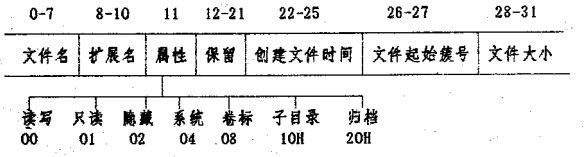
根据 DOS 版本的不同，其 FAT 的长度不一样，通常为 12 位或 16 位（前者为 DOS2.XX，后者为 DOS3.XX）。FAT 占用相对 DOS 分区第二扇区开始的位置，即逻辑扇区号为 01 的位置。其中 FAT 占用扇＝FAT 个数×每个 FAT 占用扇数。

在实际工作中，我们发现有些病毒对 FAT 占用扇进行了攻击。如大麻(Stoned)病毒入侵后，将其主引导扇区的主引导记录和分区信息表搬移至 FAT1 中的某一个扇区，若该扇区有文件链簇号在此，则文件遭到破坏。所以造成磁盘上文件丢失。此时可用 FAT2 的内容去恢复 FAT1 的内容。如 20M 硬盘，见下列程序：

读 FAT2 的内容	写 FAT1 的内容
A>DEBUG	A>DEBUG
-A XXXX:100 MOV AX,02029	-A> XXXX:100 MOV AX,03029
MOV CX,003C	MOV CX,0001
MOV DX,0080	MOV DX,0080
MOV BX,200	MOV BX,200
INT 13	INT 13
INT 20	INT 20
-G	-G
式中:FAT2 的扇区数为 29H(41)	式中:0001 为 FAT1 起始物理扇区
FAT2 的起始扇区为物理	
扇区 3CH(60)	

7.根目录扇区

目录区包括文件目录、子目录等信息。每个目录由 32 个字节组成。各字节定义如下：



一般文件起始簇号指向 FAT 表项的，它用来确定子目录和文件存放在磁盘的地址。子目录的格式与文件名一样，只是文件字节数为 0。为了求得逻辑扇区号可用下列公式完成：

逻辑扇区号＝(簇号-C×每簇扇区数+正文区起始逻辑扇区号

正文逻辑扇区＝隐藏扇区+保留扇+占用扇+目录占用扇

目录占用扇＝(目录项数×20H+1FFH)／每扇字节数

根据簇号得到逻辑扇区号，再把逻辑扇区号用前面

(下转第 44 页)

(上接第 37 页)

的公式转化成为物理扇区号，就可以对文件控制了。

为保护数据安全可对文件(子目录)的起始簇号或文件(子目录)属性字节进行修改，使之达到数据(子目录)加密。

下面介绍几种子目录的加密方法：

(1)通过修改目录的起始簇号实现子目录的加密。加密时把目录起始簇号搬移到安全的地方保存起来，再把起始簇号置 0。解密时把目录的起始簇号恢复即可。

(2)通过修改目录的属性字节和长度字节，即可实现子目录的加密。该加密后的子目录用 PCTOOLS 使之不能发现。其基本思路是：知道当文件名的属性字节为 1H 时，该文件为子目录，且文件长度为 0。加密子目录时将属性改为 12H，使之为隐藏。再把长度字节改为 12H，使之不具备子目录的性质。具体做法如下：

C＞MD SUB-DIR(建立 SUB-DIR 子目录)

C＞PC (进入 PCTOOLS)

1.选 F3 进入 DISK SERVICES；

2.按 EDIT 进入编辑；

3.按 F2 选择区域“R”= First ROOT Directory Sector(根目录区)；

4.按 Pgdn 找到子目录(SUB-DIR)；

5.按 F3 进入编辑关状态。

6.移动光标到子目录(SUB-DIR)的第 12 字节，改 10H 为 12H；

7.移动光标到子目录(SUB-DIR)的第 32 字节，改 00H 为 12H；

8.按 F5 确认；

9.按 U 执行；最后按 ESC 退出。

至此，SUB-DIR 已加密完成。