窗体顶端

|  |
| --- |
| [**GalaxyPilot —— D.S**](http://www.blogjava.net/galaxyp/)          生命不熄，战斗不止 |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **导航**   * [BlogJava](http://www.blogjava.net/) * [首页](http://www.blogjava.net/galaxyp/) * [新随笔](http://www.blogjava.net/galaxyp/admin/EditPosts.aspx?opt=1) * [联系](http://www.blogjava.net/galaxyp/contact.aspx?id=1) * [RSS 2.0 Feed聚合](http://www.blogjava.net/galaxyp/rss) * [管理](http://www.blogjava.net/galaxyp/admin/EditPosts.aspx)  |  |  |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | | |  |  |  | | --- | --- | --- | | [**<**](javascript:__doPostBack('Calendar1$entryCal','V3712')) | **2010年4月** | [**>**](javascript:__doPostBack('Calendar1$entryCal','V3773')) | | | | | | | | | **日** | **一** | **二** | **三** | **四** | **五** | **六** | | 28 | 29 | 30 | 31 | 1 | 2 | 3 | | 4 | 5 | 6 | 7 | 8 | 9 | 10 | | 11 | 12 | 13 | 14 | 15 | 16 | 17 | | 18 | 19 | 20 | 21 | 22 | [23](http://www.blogjava.net/galaxyp/archive/2010/04/23.html) | 24 | | [25](http://www.blogjava.net/galaxyp/archive/2010/04/25.html) | 26 | 27 | 28 | 29 | 30 | 1 | | 2 | 3 | 4 | 5 | 6 | 7 | 8 |   **常用链接**   * [我的随笔](http://www.blogjava.net/galaxyp/MyPosts.html) * [我的评论](http://www.blogjava.net/galaxyp/MyComments.html) * [我的参与](http://www.blogjava.net/galaxyp/OtherPosts.html) * [最新评论](http://www.blogjava.net/galaxyp/RecentComments.html)   **留言簿**(130)   * [给我留言](http://www.blogjava.net/galaxyp/Contact.aspx?id=1) * [查看公开留言](http://www.blogjava.net/galaxyp/default.aspx?opt=msg) * [查看私人留言](http://www.blogjava.net/galaxyp/admin/MyMessages.aspx)   **随笔档案**(73)   * [2014年1月 (1)](http://www.blogjava.net/galaxyp/archive/2014/01.html) * [2013年10月 (1)](http://www.blogjava.net/galaxyp/archive/2013/10.html) * [2012年12月 (1)](http://www.blogjava.net/galaxyp/archive/2012/12.html) * [2012年7月 (2)](http://www.blogjava.net/galaxyp/archive/2012/07.html) * [2012年6月 (1)](http://www.blogjava.net/galaxyp/archive/2012/06.html) * [2012年5月 (1)](http://www.blogjava.net/galaxyp/archive/2012/05.html) * [2012年2月 (1)](http://www.blogjava.net/galaxyp/archive/2012/02.html) * [2012年1月 (2)](http://www.blogjava.net/galaxyp/archive/2012/01.html) * [2011年6月 (1)](http://www.blogjava.net/galaxyp/archive/2011/06.html) * [2010年4月 (2)](http://www.blogjava.net/galaxyp/archive/2010/04.html) * [2009年11月 (1)](http://www.blogjava.net/galaxyp/archive/2009/11.html) * [2009年3月 (2)](http://www.blogjava.net/galaxyp/archive/2009/03.html) * [2009年2月 (1)](http://www.blogjava.net/galaxyp/archive/2009/02.html) * [2008年12月 (1)](http://www.blogjava.net/galaxyp/archive/2008/12.html) * [2008年11月 (1)](http://www.blogjava.net/galaxyp/archive/2008/11.html) * [2008年9月 (3)](http://www.blogjava.net/galaxyp/archive/2008/09.html) * [2008年4月 (1)](http://www.blogjava.net/galaxyp/archive/2008/04.html) * [2008年1月 (2)](http://www.blogjava.net/galaxyp/archive/2008/01.html) * [2007年11月 (1)](http://www.blogjava.net/galaxyp/archive/2007/11.html) * [2007年10月 (2)](http://www.blogjava.net/galaxyp/archive/2007/10.html) * [2007年6月 (1)](http://www.blogjava.net/galaxyp/archive/2007/06.html) * [2007年3月 (3)](http://www.blogjava.net/galaxyp/archive/2007/03.html) * [2007年2月 (2)](http://www.blogjava.net/galaxyp/archive/2007/02.html) * [2006年12月 (2)](http://www.blogjava.net/galaxyp/archive/2006/12.html) * [2006年10月 (2)](http://www.blogjava.net/galaxyp/archive/2006/10.html) * [2006年9月 (2)](http://www.blogjava.net/galaxyp/archive/2006/09.html) * [2006年8月 (1)](http://www.blogjava.net/galaxyp/archive/2006/08.html) * [2006年7月 (1)](http://www.blogjava.net/galaxyp/archive/2006/07.html) * [2006年6月 (1)](http://www.blogjava.net/galaxyp/archive/2006/06.html) * [2006年5月 (2)](http://www.blogjava.net/galaxyp/archive/2006/05.html) * [2006年4月 (13)](http://www.blogjava.net/galaxyp/archive/2006/04.html) * [2006年3月 (8)](http://www.blogjava.net/galaxyp/archive/2006/03.html) * [2006年2月 (7)](http://www.blogjava.net/galaxyp/archive/2006/02.html)   **文章档案**(1)   * [2006年7月 (1)](http://www.blogjava.net/galaxyp/archives/2006/07.html)   **相册**   * [照片](http://www.blogjava.net/galaxyp/gallery/8590.html)   **搜索**      **积分与排名**   * 积分 - 410518 * 排名 - 92   **最新评论 [http://www.blogjava.net/images/xml.gif](http://www.blogjava.net/galaxyp/CommentsRSS.aspx)**   * [1. re: Geneious Pro 6.0.4 破解[未登录]](http://www.blogjava.net/galaxyp/archive/2015/03/23/392726.html#423757) * 请发给我一份吧，谢谢你了！beckhalo333@sina.com * --chen   **阅读排行榜**   * [1. JAVA内存泄漏——内存泄漏原因和内存泄漏检测工具(zt)(39268)](http://www.blogjava.net/galaxyp/archive/2006/04/28/43724.html) * [2. 硬盘分区表知识——详解硬盘MBR(35479)](http://www.blogjava.net/galaxyp/archive/2010/04/25/319344.html) * [3. 浅谈JAVA程序破解(26757)](http://www.blogjava.net/galaxyp/archive/2006/04/19/41833.html) * [4. JProfiler 4.2 注册分析(21667)](http://www.blogjava.net/galaxyp/archive/2006/10/12/74789.html) * [5. 注册机(20236)](http://www.blogjava.net/galaxyp/archive/2006/04/20/42059.html) * [6. IP地址转换成10进制整数(zt)(20010)](http://www.blogjava.net/galaxyp/archive/2007/03/06/102137.html) * [7. 通用防SQL注入函数java版(19805)](http://www.blogjava.net/galaxyp/archive/2006/03/30/38281.html) * [8. 推荐一套图形报表工具——ChartDirector(19157)](http://www.blogjava.net/galaxyp/archive/2006/08/15/63740.html) * [9. Zelix KlassMaster 破解(18983)](http://www.blogjava.net/galaxyp/archive/2008/01/10/174256.html) * [10. 用java 操作 oracle 日期类型字段(18514)](http://www.blogjava.net/galaxyp/archive/2006/07/01/56073.html)   **评论排行榜**   * [1. Zelix KlassMaster 破解(226)](http://www.blogjava.net/galaxyp/archive/2008/01/10/174256.html) * [2. Geneious Pro 6.0.4 破解(167)](http://www.blogjava.net/galaxyp/archive/2012/12/10/392726.html) * [3. Geneious R7 7.0.2 破解版(48)](http://www.blogjava.net/galaxyp/archive/2013/10/15/405027.html) * [4. 破解 Geneious Pro 3.0.6(46)](http://www.blogjava.net/galaxyp/archive/2007/10/17/153554.html) * [5. CLC Combined Workbench 3.0.3 破解(38)](http://www.blogjava.net/galaxyp/archive/2008/01/28/178166.html) * [6. CADI GC 2.98 破解版(35)](http://www.blogjava.net/galaxyp/archive/2012/01/18/368687.html) * [7. clc 生物工程软件破解(30)](http://www.blogjava.net/galaxyp/archive/2007/03/03/101586.html) * [8. CADI 2.92 电梯调试软件破解(17)](http://www.blogjava.net/galaxyp/archive/2009/11/25/303606.html) * [9. CADI\_GC 2.94 破解版(13)](http://www.blogjava.net/galaxyp/archive/2012/01/13/368475.html) * [10. 通用防SQL注入函数java版(12)](http://www.blogjava.net/galaxyp/archive/2006/03/30/38281.html) | [**硬盘分区表知识——详解硬盘MBR**](http://www.blogjava.net/galaxyp/archive/2010/04/25/319344.html)  硬盘是现在计算机上最常用的存储器之一。我们都知道，计算机之所以神奇，是因为它具有高速分析处理数据的能力。而这些数据都以文件的形式存储在硬盘 里。不过，计算机可不像人那么聪明。在读取相应的文件时，你必须要给出相应的规则。这就是分区概念。      分区从实质上说就是对硬盘的一种格式化。当我们创建分区时，就已经设置好了硬盘的各项物理参数，指定了硬盘主引导记录（即Master Boot Record，一般简称为MBR）和引导记录备份的存放位置。而对于文件系统以及其他操作系统管理硬盘所需要的信息则是通过以后的高级格式化，即 Format命令来实现。面、磁道和扇区硬盘分区后，将会被划分为面（Side）、磁道（Track）和扇区（Sector）。需要注意的是，这些只是个 虚拟的概念，并不是真正在硬盘上划轨道。      先从面说起，硬盘一般是由一片或几片圆形薄膜叠加而成。我们所说，每个圆形薄膜都有两个“面”，这两个面都是用来存储数据的。按照面的多少，依次称为0 面、1面、2面……由于每个面都专有一个读写磁头，也常用0头(head)、1头……称之。按照硬盘容量和规格的不同，硬盘面数(或头数)也不一定相同， 少的只有2面，多的可达数十面。各面上磁道号相同的磁道合起来，称为一个柱面(Cylinder)。        上面我们提到了磁道的概念。那么究竟何为磁道呢？由于磁盘是旋转的，则连续写入的数据是排列在一个圆周上的。我们称这样的圆周为一个磁道。如果读写磁头沿 着圆形薄膜的半径方向移动一段距离，以后写入的数据又排列在另外一个磁道上。根据硬盘规格的不同，磁道数可以从几百到数千不等；一个磁道上可以容纳数KB 的数据，而主机读写时往往并不需要一次读写那么多，于是，磁道又被划分成若干段，每段称为一个扇区。一个扇区一般存放512字节的数据。扇区也需要编号， 同一磁道中的扇区，分别称为1扇区，2扇区……      计算机对硬盘的读写，处于效率的考虑，是以扇区为基本单位的。即使计算机只需要硬盘上存储的某个字节，也必须一次把这个字节所在的扇区中的512字节全部 读入内存，再使用所需的那个字节。不过，在上文中我们也提到，硬盘上面、磁道、扇区的划分表面上是看不到任何痕迹的，虽然磁头可以根据某个磁道的应有半径 来对准这个磁道，但怎样才能在首尾相连的一圈扇区中找出所需要的某一扇区呢？原来，每个扇区并不仅仅由512个字节组成的，在这些由计算机存取的数据的 前、后两端，都另有一些特定的数据，这些数据构成了扇区的界限标志，标志中含有扇区的编号和其他信息。计算机就凭借着这些标志来识别扇区。硬盘的数据结构 在上文中，我们谈了数据在硬盘中的存储的一般原理。为了能更深入地了解硬盘，我们还必须对硬盘的数据结构有个简单的了解。硬盘上的数据按照其不同的特点和 作用大致可分为5部分：MBR区、DBR区、FAT区、DIR区和DATA区。    我们来分别介绍一下：  **1、MBR区**        MBR（Main Boot Record 主引导记录区）位于整个硬盘的0磁道0柱面1扇区。不过，在总共512字节的主引导扇区中，MBR只占用了其中的446个字节，另外的64个字节交给了 DPT（Disk Partition Table硬盘分区表），最后两个字节“55，AA”是分区的结束标志。这个整体构成了硬盘的主引导扇区。      主引导记录中包含了硬盘的一系列参数和一段引导程序。其中的硬盘引导程序的主要作用是检查分区表是否正确并且在系统硬件完成自检以后引导具有激活标志的分 区上的操作系统，并将控制权交给启动程序。MBR是由分区程序（如Fdisk．exe）所产生的，它不依赖任何操作系统，而且硬盘引导程序也是可以改变 的，从而实现多系统共存。      下面，我们以一个实例让大家更直观地来了解主引导记录：  **例：**80 01 01 00 0B FE BF FC 3F 00 00 00 7E 86 BB 00 在这里我们可以看到，最前面的“80”是一个分区的激活标志，表示系统可引导；“01 01 00”表示分区开始的磁头号为01，开始的扇区号为01，开始的柱面号为00；“0B”表示分区的系统类型是FAT32，其他比较常用的有 04（FAT16）、07（NTFS）；“FE BF FC”表示分区结束的磁头号为254，分区结束的扇区号为63、分区结束的柱面号为764；“3F 00 00 00”表示首扇区的相对扇区号为63；“7E 86 BB 00”表示总扇区数为12289622。  **2、DBR区**      DBR（Dos Boot Record）是操作系统引导记录区的意思。它通常位于硬盘的0磁道1柱面1扇区，是操作系统可以直接访问的第一个扇区，它包括一个引导程序和一个被称为 BPB（Bios Parameter Block）的本分区参数记录表。引导程序的主要任务是当MBR将系统控制权交给它时，判断本分区跟目录前两个文件是不是操作系统的引导文件（以DOS为 例，即是Io．sys和Msdos．sys）。如果确定存在，就把它读入内存，并把控制权 交给该文件。BPB参数块记录着本分区的起始扇区、结束扇区、文件存储格式、硬盘介质描述符、根目录大小、FAT个数，分配单元的大小等重要参数。DBR 是由高级格式化程序（即Format．com等程序）所产生的。  **3、FAT区**      在DBR之后的是我们比较熟悉的FAT（File Allocation Table文件分配表）区。在解释文件分配表的概念之前，我们先来谈谈簇（Cluster）的概念。文件占用磁盘空间时，基本单位不是字节而是簇。一般情 况下，软盘每簇是1个扇区，硬盘每簇的扇区数与硬盘的总容量大小有关，可能是4、8、16、32、64…… 同一个文件的数据并不一定完整地存放在磁盘的一个连续的区域内，而往往会分成若干段，像一条链子一样存放。这种存储方式称为文件的链式存储。由于硬盘上保 存着段与段之间的连接信息（即FAT），操作系统在读取文件时，总是能够准确地找到各段的位置并正确读出。 为了实现文件的链式存储，硬盘上必须准确地记录哪些簇已经被文件占用，还必须为每个已经占用的簇指明存储后继内容的下一个簇的簇号。对一个文件的最后一 簇，则要指明本簇无后继簇。这些都是由FAT表来保存的，表中有很多表项，每项记录一个簇的信息。由于FAT对于文件管理的重要性，所以FAT有一个备 份，即在原FAT的后面再建一个同样的FAT。初形成的FAT中所有项都标明为“未占用”，但如果磁盘有局部损坏，那么格式化程序会检测出损坏的簇，在相 应的项中标为“坏簇”，以后存文件时就不会再使用这个簇了。FAT的项数与硬盘上的总簇数相当，每一项占用的字节数也要与总簇数相适应，因为其中需要存放 簇号。FAT的格式有多种，最为常见的是FAT16和FAT32。    **4、DIR区**   DIR（Directory）是根目录区，紧接着第二FAT表（即备份的FAT表）之后，记录着根目录下 每个文件(目录)的起始单元，文件的属性等。定位文件位置时，操作系统根据DIR中的起始单元，结合FAT表就可以知道文件在硬盘中的具体位置和大小了。    **5、数据(DATA)区**      数据区是真正意义上的数据存储的地方，位于DIR区之后，占据硬盘上的大部分数据空间。    **一、硬盘的物理结构：**  　    硬盘存储数据是根据电、磁转换原理实现的。硬盘由一个或几个表面镀有磁性物质的金属或玻璃等物质盘片以及盘片两面所安装的磁头和相应的控制电路组成(图 1)，其中盘片和磁头密封在无尘的金属壳中。  http://p.blog.csdn.net/images/p_blog_csdn_net/sallay/EntryImages/20081231/a1.gif       硬盘工作时，盘片以设计转速高速旋转，设置在盘片表面的磁头则在电路控制下径向移动到指定位置然后将数据存储或读取出来。当系统向硬盘写入数据时，磁头中 “写数据”电流产生磁场使盘片表面磁性物质状态发生改变，并在写电流磁场消失后仍能保持，这样数据就存储下来了；当系统从硬盘中读数据时，磁头经过盘片指 定区域，盘片表面磁场使磁头产生感应电流或线圈阻抗产生变化，经相关电路处理后还原成数据。因此只要能将盘片表面处理得更平滑、磁头设计得更精密以及尽量 提高盘片旋转速度，就能造出容量更大、读写数据速度更快的硬盘。这是因为盘片表面处理越平、转速越快就能越使磁头离盘片表面越近，提高读、写灵敏度和速 度；磁头设计越小越精密就能使磁头在盘片上占用空间越小，使磁头在一张盘片上建立更多的磁道以存储更多的数据。    **二、硬盘的逻辑结构：**      硬盘由很多盘片(platter)组成，每个盘片的每个面都有一个读写磁头。如果有N个盘片。就有2N个面，对应2N个磁头(Heads)，从0、1、2 开始编号。每个盘片被划分成若干个同心圆磁道(逻辑上的，是不可见的。)每个盘片的划分规则通常是一样的。这样每个盘片的半径均为固定值R的同心圆再逻辑 上形成了一个以电机主轴为轴的柱面(Cylinders)，从外至里编号为0、1、2……每个盘片上的每个磁道又被划分为几十个扇区(Sector)，通 常的容量是512byte，并按照一定规则编号为1、2、3……形成Cylinders×Heads×Sector个扇区。这三个参数即是硬盘的物理参 数。我们下面的很多实践需要深刻理解这三个参数的意义。     硬盘存储数据是根据电、磁转换原理实现的。硬盘由一个或几个表面镀有磁性物质的金属或玻璃等物质盘片以及盘片两面所安装的磁头和相应的控制电路组成(图 1)，其中盘片和磁头密封在无尘的金属壳中。    **三、磁盘引导原理：**  3.1 MBR(master boot record)扇区：  　　计算机在按下power键以后，开始执行主板bios程序。进行完一系列检测和配置以后。开始按bios中设定的系统引导顺序引导系统。假定现 在是硬盘。Bios执行完自己的程序后如何把执行权交给硬盘呢。交给硬盘后又执行存储在哪里的程序呢。其实，称为mbr的一段代码起着举足轻重的作用。 MBR(master boot record),即主引导记录，有时也称主引导扇区。位于整个硬盘的0柱面0磁头1扇区(可以看作是硬盘的第一个扇区)，bios在执行自己固有的程序以 后就会jump到mbr中的第一条指令。将系统的控制权交由mbr来执行。在总共512byte的主引导记录中，MBR的引导程序占了其中的前446个字 节(偏移0H~偏移1BDH)，随后的64个字节(偏移1BEH~偏移1FDH)为DPT(Disk PartitionTable，硬盘分区表)，最后的两个字节“55 AA”(偏移1FEH~偏移1FFH)是分区有效结束标志。  　　MBR不随操作系统的不同而不同，意即不同的操作系统可能会存在相同的MBR，即使不同，MBR也不会夹带操作系统的性质。具有公共引导的特 性。  　　我们来分析一段mbr。下面是用winhex查看的一块希捷120GB硬盘的mbr。  **MBR扇区代码**  http://p.blog.csdn.net/images/p_blog_csdn_net/sallay/EntryImages/20081231/a2.gif        你的硬盘的MBR引导代码可能并非这样。不过即使不同，所执行的功能大体是一样的。这里找wowocock关于磁盘mbr的反编译，已加了详细的注释，感 兴趣可以细细研究一下。  我们看DPT部分。操作系统为了便于用户对磁盘的管理。加入了磁盘分区的概念。即将一块磁盘逻辑划分为 几块。磁盘分区数目的多少只受限于C～Z的英文字母的数目，在上图DPT共64个字节中如何表示多个分区的属性呢?microsoft通过链接的方法解决 了这个问题。在DPT共64个字节中，以16个字节为分区表项单位描述一个分区的属性。也就是说，第一个分区表项描述一个分区的属性，一般为基本分区。第 二个分区表项描述除基本分区外的其余空间，一般而言，就是我们所说的扩展分区。这部分的大体说明见表1。  http://p.blog.csdn.net/images/p_blog_csdn_net/sallay/EntryImages/20081231/a3.gif  **DPT代码分析**    注：上表中的超过1字节的数据都以实际数据显示，就是按高位到地位的方式显示。存储时是按低位到高位存储的。两者表现不同，请仔细看清楚。以后出现的表， 图均同。  　　也可以在winhex中看到这些参数的意义：        http://p.blog.csdn.net/images/p_blog_csdn_net/sallay/EntryImages/20081231/a4.gif  **说明：** 每个分区表项占用16个字节，假定偏移地址从0开始。如图3的分区表项3。分区表项4同分区表项3。  　　1、0H偏移为活动分区是否标志，只能选00H和80H。80H为活动，00H为非活动。其余值对microsoft而言为非法值。  　　2、重新说明一下(这个非常重要)：大于1个字节的数被以低字节在前的存储格式格式(little endian format)或称反字节顺序保存下来。低字节在前的格式是一种保存数的方法，这样，最低位的字节最先出现在十六进制数符号中。例如，相对扇区数字段的值 0x3F000000的低字节在前表示为0x0000003F。这个低字节在前的格式数的十进制数为63。  　　3、系统在分区时，各分区都不允许跨柱面，即均以柱面为单位，这就是通常所说的分区粒度。有时候我们分区是输入分区的大小为7000M，分出来 却是6997M，就是这个原因。 偏移2H和偏移6H的扇区和柱面参数中,扇区占6位(bit)，柱面占10位(bit)，以偏移6H为例，其低6位用作扇区数的二进制表示。其高两位做柱 面数10位中的高两位，偏移7H组成的8位做柱面数10位中的低8位。由此可知，实际上用这种方式表示的分区容量是有限的，柱面和磁头从0开始编号,扇区 从1开始编号,所以最多只能表示1024个柱面×63个扇区×256个磁头×512byte=8455716864byte。即通常的8.4GB(实际上 应该是7.8GB左右)限制。实际上磁头数通常只用到255个(由汇编语言的寻址寄存器决定),即使把这3个字节按线性寻址，依然力不从心。 在后来的操作系统中，超过8.4GB的分区其实已经不通过C/H/S的方式寻址了。而是通过偏移CH～偏移FH共4个字节32位线性扇区地址来表示分区所 占用的扇区总数。可知通过4个字节可以表示2^32个扇区，即2TB=2048GB，目前对于大多数计算机而言，这已经是个天文数字了。在未超过 8.4GB的分区上，C/H/S的表示方法和线性扇区的表示方法所表示的分区大小是一致的。也就是说，两种表示方法是协调的。即使不协调，也以线性寻址为 准。(可能在某些系统中会提示出错)。超过8.4GB的分区结束C/H/S一般填充为FEH FFH FFH。即C/H/S所能表示的最大值。有时候也会用柱面对1024的模来填充。不过这几个字节是什么其实都无关紧要了。  　　虽然现在的系统均采用线性寻址的方式来处理分区的大小。但不可跨柱面的原则依然没变。本分区的扇区总数加上与前一分区之间的保留扇区数目依然必 须是柱面容量的整数倍。(保留扇区中的第一个扇区就是存放分区表的MBR或虚拟MBR的扇区，分区的扇区总数在线性表示方式上是不计入保留扇区的。如果是 第一个分区，保留扇区是本分区前的所有扇区。  　　附：分区表类型标志如图4  http://p.blog.csdn.net/images/p_blog_csdn_net/sallay/EntryImages/20081231/a5.gif    3.2 扩展分区    扩展分区中的每个逻辑驱动器都存在一个类似于MBR的扩展引导记录( Extended Boot Record, EBR)，也有人称之为虚拟mbr或扩展mbr，意思是一样的。扩展引导记录包括一个扩展分区表和该扇区的标签。扩展引导记录将记录只包含扩展分区中每个 逻辑驱动器的第一个柱面的第一面的信息。一个逻辑驱动器中的引导扇区一般位于相对扇区32或63。但是，如果磁盘上没有扩展分区，那么就不会有扩展引导记 录和逻辑驱动器。第一个逻辑驱动器的扩展分区表中的第一项指向它自身的引导扇区。第二项指向下一个逻辑驱动器的EBR。如果不存在进一步的逻辑驱动器，第 二项就不会使用，而且被记录成一系列零。如果有附加的逻辑驱动器，那么第二个逻辑驱动器的扩展分区表的第一项会指向它本身的引导扇区。第二个逻辑驱动器的 扩展分区表的第二项指向下一个逻辑驱动器的EBR。扩展分区表的第三项和第四项永远都不会被使用。      通过一幅4分区的磁盘结构图可以看到磁盘的大致组织形式。如图5  http://p.blog.csdn.net/images/p_blog_csdn_net/sallay/EntryImages/20081231/a6.gif      关于扩展分区，如图6所示，扩展分区中逻辑驱动器的扩展引导记录是一个连接表。该图显示了一个扩展分区上的三个逻辑驱动器，说明了前面的逻辑驱动器和最后 一个逻辑驱动器之间在扩展分区表中的差异。  http://p.blog.csdn.net/images/p_blog_csdn_net/sallay/EntryImages/20081231/a7.gif     除了扩展分区上最后一个逻辑驱动器外，表2中所描述的扩展分区表的格式在每个逻辑驱动器中都是重复的：第一个项标识了逻辑驱动器本身的引导扇区，第二个项 标识了下一个逻辑驱动器的EBR。最后一个逻辑驱动器的扩展分区表只会列出它本身的分区项。最后一个扩展分区表的第二个项到第四个项被使用。  http://p.blog.csdn.net/images/p_blog_csdn_net/sallay/EntryImages/20081231/a8.gif        扩展分区表项中的相对扇区数字段所显示的是从扩展分区开始到逻辑驱动器中第一个扇区的位移的字节数。总扇区数字段中的数是指组成该逻辑驱动器的扇区数 目。总扇区数字段的值等于从扩展分区表项所定义的引导扇区到逻辑驱动器末尾的扇区数。      有时候在磁盘的末尾会有剩余空间，剩余空间是什么呢？我们前面说到，分区是以1柱面的容量为分区粒度的，那么如果磁盘总空间不是整数个柱面的话，不够一个 柱面的剩下的空间就是剩余空间了，这部分空间并不参与分区，所以一般无法利用。照道理说，磁盘的物理模式决定了磁盘的总容量就应该是整数个柱面的容量，为 什么会有不够一个柱面的空间呢。在我的理解看来，本来现在的磁盘为了更大的利用空间，一般在物理上并不是按照外围的扇区大于里圈的扇区这种管理方式，只是 为了与操作系统兼容而抽象出来CHS。可能其实际空间容量不一定正好为整数个柱面的容量。  posted on 2010-04-25 22:55 [舵手](http://www.blogjava.net/galaxyp/) 阅读(35479) [评论(0)](http://www.blogjava.net/galaxyp/archive/2010/04/25/319344.html#Post)  [编辑](http://www.blogjava.net/galaxyp/admin/EditPosts.aspx?postid=319344)  [收藏](http://www.blogjava.net/galaxyp/AddToFavorite.aspx?id=319344)  http://www.blogjava.net/galaxyp/aggbug/319344.html?webview=1  [新用户注册](http://www.blogjava.net/RequireRegister.aspx)  [刷新评论列表](javascript:__doPostBack('AjaxHolder$PostComment$refreshList',''))     |  |  |  | | --- | --- | --- | |  | | | |  | | | |  |  |  | |  | [找优秀程序员，就在博客园](http://job.cnblogs.com/) | | | 标题 |  |  | | 姓名 |  |  | | 主页 |  |  | | |  |  |  | | --- | --- | --- | |  | | | | 验证码 | \* |  | | | | | 内容(请不要发表任何与政治相关的内容) | | | |  | | | | Remember Me? | | | |  | [登录](http://www.blogjava.net/login.aspx?ReturnURL=http://www.blogjava.net/galaxyp/archive/2010/04/25/319344.html&SourceURL=/galaxyp/archive/2010/04/25/319344.html) | | | [使用Ctrl+Enter键可以直接提交] | | | |  | | | |  | | | |  | | | |  | | | | 网站导航:  [博客园](http://www.cnblogs.com/)   [IT新闻](http://news.cnblogs.com/)   [知识库](http://kb.cnblogs.com/)   [C++博客](http://www.cppblog.com/)   [程序员招聘](http://job.cnblogs.com/)   [管理](http://www.blogjava.net/galaxyp/archive/2010/04/25/319344.html?opt=admin) | | | |  | | | |  | | | |  | | | |  | | | |
| Powered by:  [BlogJava](http://www.blogjava.net/)  Copyright © 舵手 |

## 1. CHS（Cylinder-Head-Sector）：

was an early method for giving addresses to each physical block of data on a hard disk drive.

#### 1.1 Cylinder(柱面)：

A cylinder comprises（包含，由…组成）【k?m'pra?z】 **the same track number** on **each platter**,

spanning（横跨） all such tracks across（横穿） each platter surface that is able to store data (without regard to whether or not the track is "bad").

Thus, it is a **three-dimensional** structure.

Any track comprising part of a specific cylinder can be written to and read from while the actuator assembly remains stationary,

and one way in which hard drive manufacturers have increased drive access speed has been by increasing the number of platters which can be read at the same time.

#### 1.2 Head（磁头）：

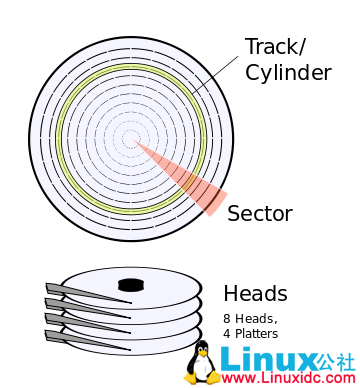
A device called a head reads and writes data in a hard drive by manipulating the magnetic（有磁性的） [m?g'net?k] medium that composes the surface of an associated disk platter.

一个磁头读取的最基本单位是一个Head，每个Head大小512bytes

#### 1.3 Sector（扇区）：

A sector is **the smallest storage unit** that is addressable(可寻址的) by a hard drive, and all information stored by the hard drive is recorded in sectors.

象切蛋糕



#### 1.4 Track

#### 1.5 Block

### 2. 磁盘在Linux中的表示

2.1 Linux所有设备都被抽象为一个文件，保存在**/dev/**目录下

2.2 磁盘按接口分为：（IDE、SATA、SAS、SCSI、USB）

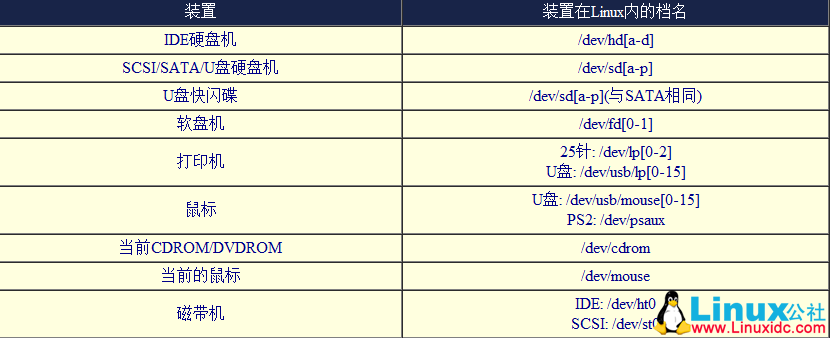
2.2.1 IDE磁盘名称一般为：hd【a-z】，【a-z】代表第几块磁盘;

2.2.2 SATA磁盘、SAS硬盘、SCSI硬盘、USB磁盘名称一般为：sd【a-z】,【a-z】代表第几块磁盘;

例如：第一块sata磁盘表示为：/dev/sda

第二块sata磁盘表示为/dev/sdb

底下列出几个常见的装置与其在Linux当中的档名



### 3. 分区概念

3.1 将一个磁盘逻辑的分为几个区，每个区当做独立磁盘，以方便使用和管理

不同分区的名称一般为：设备名称+分区号

例如：第一块硬盘的第一个分区叫sda1，第一块硬盘的第二个分区sda2

第二块硬盘的第一个分区叫sdb1，第二块硬盘的第二个分区叫sdb2

\*分区并不是硬盘的物理功能，而是软件功能

\*主流的分区机制分为MBR和GPT两种

MBR是PC架构计算机中使用的最为广泛的分区机制

### 4. MBR

4.1 MBR(Master Boot Record)是传统的分区机制，应用于绝大多数使用BIOS引导的PC设备（苹果使用EFI的方式）；很多Server服务器即支持BIOS也支持EFI的引导方式

4.2 MBR的特点

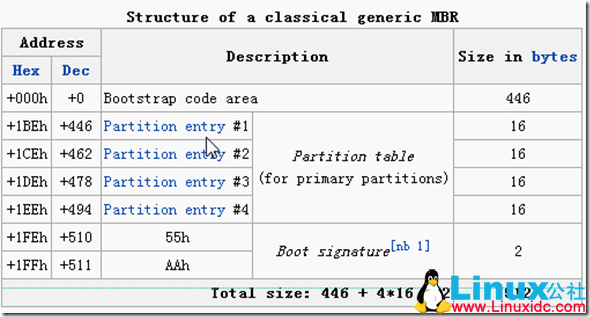
4.2.1优点：MBR支持32bit和64bit系统；

4.2.2缺点：1） MBR支持的分区数量有限制；2）MBR只支持不超过2TB的硬盘，超过2TB的硬盘只能使用2TB的空间(但是有第三方解决方法)，应为**MBR的寻址空间只有32bit长；**

4.3 MBR结构：占用硬盘最开头的512字节

前446字节为：引导代码（Bootstrap Code Area）（引导不同的操作系统；不同操作系统，引导代码是不一样的）

接下来的为4个16字节：分别对应4个主分区表信息(Primary Partition Table)

最后2个字节：为启动标示（Boot Signature），永远都是55和AA；55和ＡＡ是个永久性的标示，代表这个硬盘是可启动的。

### 5. MBR分区

ＭＢＲ分区分为：主分区、扩展分区、逻辑分区

5.1 主分区：一块硬盘最多只能创建4个主分区（因为在MBR分区表结构中中最多可以创建4个主分区表信息，也就是4个16字节的空间，如上图）

5.2 扩展分区：一个扩展分区会占用一个主分区的位置

5.3 逻辑分区：

1）是基于扩展分区创建出来的，先有扩展分区，然后在扩展分区的基础上再创建逻辑分区；也就是说我们要使用逻辑分区，必须先要创建扩展分区；

2）扩展分区的空间是不能被直接使用的，我们必须在扩展分区的基础上去建立逻辑分区，才能够被使用；

3）Linux最多支持63个IDE分区和15个SCSI分区

**PEL:Primary Partition;Extended Partition;Logical Partition**

### 6. GPT

GPT(GUID Partition Table):是一个较新的分区机制，解决了MBR的很多缺点

1）支持超过2TB的磁盘：GPT有64bit寻址空间；而MBR对硬盘空间地址寻址最多只支持32bit，2的32次方，硬盘空间是以地址方式来被识别的，所以MBR只支持容量为2TB以内的磁盘

2）向后兼容MBR

3）但是底层硬件必须支持UEFI（Intel提出的取代BIOS的新一代的引导系统）才能使用，也就是底层硬件必须使用UEFI

4）必须使用64位操作系统

5）Mac、LInux系统都能支持GPT分区格式

6）Windows 7 64bit、Windows Server2008 64bit支持GPT

|  |  |  |  |
| --- | --- | --- | --- |
| [看雪安全论坛](http://www.pediy.com/) | [http://www.pediy.com/temp/ajm05.jpg](http://www.ijiami.cn/activity/rencai) |  |  |
| [http://bbs.pediy.com/images/pediy/misc/head_forum_pediy_tab1.gif](http://bbs.pediy.com/) | [http://bbs.pediy.com/images/pediy/misc/head_forum_modiy_tab2.gif](http://www.kanxue.com/bbs/) |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| |  |  |  | | --- | --- | --- | | [返回](http://bbs.pediy.com/showthread.php?t=176156) |  | [看雪安全论坛](http://bbs.pediy.com/index.php) > [**Windows**](http://bbs.pediy.com/forumdisplay.php?f=3) > [『软件调试逆向』](http://bbs.pediy.com/forumdisplay.php?f=4) | | [刷新本页](http://bbs.pediy.com/showthread.php?t=176156) **系统底层 【原创】FAT32简介（mbr/ebr/dpt/bpb/fat/fdt)** | | | | 窗体顶端   |  |  |  | | --- | --- | --- | | 用户名 |  | 记住 | | 密　码 |  | [忘记密码?](http://bbs.pediy.com/login.php?do=lostpw) |   窗体底端 |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **[KSSD](http://www.pediy.com/kssd/" \t "_blank)** | [**注册账号**](http://bbs.pediy.com/register.php) | [**搜索论坛**](http://www.kanxue.com/) | [**日历事件**](http://bbs.pediy.com/calendar.php) | [**论坛帮助**](http://bbs.pediy.com/faq.php) |

|  |
| --- |
| **『软件调试逆向』** http://bbs.pediy.com/images/Forum_readme.gif[综合性论坛]本版讨论的主题包括：调试逆向、系统底层、商业保护、虚拟机保护、.NET平台等安全相关的话题。 |

|  |  |
| --- | --- |
| Expired Thread | 该主题： **"【原创】FAT32简介（mbr/ebr/dpt/bpb/fat/fdt)"** 因在一定的时间里没有任何回复而自动关闭。 如果您还对该主题感兴趣或者想参与对此主题的讨论，请您重新发表一篇相关的新主题。 |

|  |
| --- |
| [发表新主题](http://bbs.pediy.com/newthread.php?do=newthread&f=4) [关闭主题](http://bbs.pediy.com/newreply.php?do=newreply&noquote=1&p=1203215) |

|  |  |  |
| --- | --- | --- |
| 精华帖 | [**主题工具**](http://bbs.pediy.com/showthread.php?t=176156&nojs=1#goto_threadtools)**http://bbs.pediy.com/images/pediy/misc/menu_open.gif** | [**显示模式**](http://bbs.pediy.com/showthread.php?t=176156&nojs=1#goto_displaymodes)**http://bbs.pediy.com/images/pediy/misc/menu_open.gif** |

|  |  |  |
| --- | --- | --- |
| 本站声明：看雪论坛文章版权属于作者，受法律保护。没有作者书面许可不得转载。若作者同意转载，必须以超链接形式标明文章原始出处和作者信息及本声明！ | | |
| [foxive](http://bbs.pediy.com/member.php?u=243387)  级别:3 | 在线时长:28小时 | 升级还需:4小时级别:3 | 在线时长:28小时 | 升级还需:4小时级别:3 | 在线时长:28小时 | 升级还需:4小时  普通会员  普通会员  资　料:  注册日期: Feb 2009  帖子: [29](http://bbs.pediy.com/search.php?do=finduser&u=243387) foxive 品行端正  精华: [1](http://bbs.pediy.com/search.php?do=finduser&goodnees=1&u=243387)  现金: 179 Kx  致谢数: 0  获感谢文章数：0 获会员感谢数：0 | | |  |  | | --- | --- | | **[1](http://bbs.pediy.com/showpost.php?p=1203215&postcount=1" \t "new)** 旧 2013-07-26 20:20:52 默认 **【原创】FAT32简介（mbr/ebr/dpt/bpb/fat/fdt)** | foxive 当前离线 |   标 题: 【原创】FAT32简介（mbr/ebr/dpt/bpb/fat/fdt) 作 者: foxive 时 间: 2013-07-26,20:20:52 链 接: http://bbs.pediy.com/showthread.php?t=176156  没上过大学，纯野路子。不当之处请指证。 当然，如果有人在这方面比我还菜的话，有以下话想说。 如果你看完了什么都没记住，这很正常。如果想简单地看明白，并记住点什么的话，还是自己动手分析计算。 我用到两个工具：       二进制编辑器程序010EDIT，论坛有，可供下载。  BOCHS，可去官网下载，免费的。如果软件不会用，请看帮助文件。  **FAT32简介**  名称:  1.png 查看次数: 2 文件大小:  144.6 KB **图1**  这是硬盘0磁头0道1扇区的内容，这部分内容一般是由分区程序生成，与操作系统无关。共三部分：硬盘主引导记录MBR（MAIN BOOT RECORD），分区表DPT（DISK PARTITION TABLE），分区结束标志（55AA）。其中MBR共446B，DPT64B，结束标志2B。MBR是一段引导程序，主要功能是检查DPT的有效性，找到活动分区，并将活动分区的第一扇区内容读入内存，并跳转到这段程序继续执行。  那么我们来看MBR具体是怎么执行的： <bochs:4> u/200 00007c00: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif mov si, 0x7c00            ; be007c 00007c03: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif cli                       ; fa ——初始化堆栈段前关中断 00007c04: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif xor ax, ax                ; 33c0 00007c06: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif mov ss, ax                ; 8ed0 00007c08: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif mov sp, si                ; 8be6 00007c0a: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif sti                       ; fb 以下内容是将整个引导扇区内容复制到0：0600H开始的一段内存空间中，并跳转到061EH处继续执行MBR程序。 00007c0b: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif mov ds, ax                ; 8ed8 00007c0d: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif mov es, ax                ; 8ec0 00007c0f: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif push ax                   ; 50 00007c10: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif mov ax, 0x061e            ; b81e06 00007c13: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif push ax                   ; 50 00007c14: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif mov di, 0x0600            ; bf0006 00007c17: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif mov cx, 0x0100            ; b90001 00007c1a: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif cld                       ; fc 00007c1b: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif rep movsw word ptr es:[di], word ptr ds:[si] ;  f3a5 00007c1d: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif retf                      ; cb  00007c1e: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif mov bx, 0x0763            ; bb6307 00007c21: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif mov si, 0x07be            ; bebe07 00007c24: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif mov ax, 0x0031            ; b83100 00007c27: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif cmp byte ptr ds:[si], 0x80 ; 803c80  DS：[SI]相当于0x7be-0x600=0x1be。而从上图中看0x1be正是DPT开始的字节。 下面我们来看DPT的结构。DPT分为四个表项，各占16字节，每一表项描述一个分区，所以最多可以有四个分区。但现在的用法一般是：第一项描述主分区，第二项描述扩展分区，第三第四项为0。每一表项的不同字节意义如下：  第0字节 是否为活动分区，是则为80H，否则为00H  第1字节 该分区起始磁头号  第2字节 该分区起始扇区号（低6位）和起始柱磁头号（高2位）  第3字节 该分区起始柱面号的低8位  第4字节 系统标志，00H表该分区未使用，06H表高版本DOS系统，05H扩展DOS分区，65H表Netwear分区  第5字节 该分区结束磁头号  第6字节 该分区结束扇区号（低6位）和结束柱面号（高2位）  第7字节 该分区结束柱面号的低8位  第8~11字节 相对扇区号，该分区起始的相对逻辑扇区号，高位在后低位在前  第12~15字节 该分区所用扇区数，高位在后，低位在前  以上蓝字内容是复制的。我们只要知道0字节处，80H代表活动分区。那我们接着看MBR程序下面要做什么 00007c2a: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif jnz .+9                   ; 7509 因为17BE处的内容为80H，所以第一次执行此程序段时这个跳转不会发生。但也说明活动分区并不一定要是第一个分区。跳转的位置为：00007C35 00007c2c: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif inc bx                    ; 43 原来BX内容为0X0763，而0X0764-0X600=0X0164（图1中），所以下条指令改写的是图1中0X0164中的内容 00007c2d: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif mov byte ptr ds:[bx], al  ; 8807   AL=31H 00007c2f: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif inc bx                    ; 43 00007c30: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif mov byte ptr ds:[bx], 0x2f ; c6072f此时图1中字0X0164中的内容变为：2F31H 00007c33: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif inc ah                    ; fec4   00007c35: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif add si, 0x0010            ; 83c610 检查第二个表项 00007c38: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif inc al                    ; fec0 00007c3a: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif cmp al, 0x35              ; 3c35 00007c3c: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif jb .-23                   ; 72e9 跳转到00007C27处，当AL=35H，四个表项全部检查完毕，向下执行 00007c3e: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif mov byte ptr ds:[bx], 0x3f ; c6073f 此时BX=0765。但如果有两个活动分区，或者四个活动分区则BX值增量。 00007c41: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif inc bx                    ; 43 00007c42: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif mov word ptr ds:[bx], 0x0020 ; c7072000 00007c46: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif or ah, ah                 ; 0ae4 AH记录活动分区的个数：这里为1 00007c48: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif jnz .+6                   ; 7506 跳转至00007C50 00007c4a: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif mov bx, 0x06f8            ; bbf806 00007c4d: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif jmp .+137                 ; e98900 如果没有活动分区，则跳转至00007CD9，调用一个过程显示一段：No partition bootable（在图1中地址0F8H处）的信息。 00007c50: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif mov al, byte ptr ds:0x764 ; a06407 00007c53: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif cmp ah, 0x02              ; 80fc02 00007c56: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif jb .+53                   ; 7235 跳转至00007c8d，如果有两个以上活动分区则不跳转 00007c58: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif mov bx, 0x0744            ; bb4407 00007c5b: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif call .+128                ; e88000 跳至7CDE显示一段信息：Enter patrtition # to boot from, （后面的内容就是前面检查活动分区时修改的从0X164开始的一段数据）1/2/3/4？。并调用INT16H取得键盘输入，选择从哪里BOOT。 00007c5e: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif jmp .+5                   ; eb05 00007c60: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif mov al, 0x07              ; b007 00007c62: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif call .+133                ; e88500 00007c65: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif xor ah, ah                ; 32e4 00007c67: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif int 0x16                  ; cd16 00007c69: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif mov byte ptr ds:0x782, al ; a28207 00007c6c: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif mov cl, 0x04              ; b104 00007c6e: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif sub al, 0x31              ; 2c31 00007c70: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif jb .-18                   ; 72ee 00007c72: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif cmp al, cl                ; 3ac1 00007c74: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif jnb .-22                  ; 73ea 00007c76: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif shl al, cl                ; d2e0 00007c78: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif xor ah, ah                ; 32e4 00007c7a: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif add ax, 0x07be            ; 05be07 00007c7d: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif mov si, ax                ; 8bf0 00007c7f: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif cmp byte ptr ds:[si], 0x80 ; 803c80 00007c82: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif jnz .-36                  ; 75dc 00007c84: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif mov bx, 0x0782            ; bb8207 00007c87: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif call .+84                 ; e85400 00007c8a: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif mov al, byte ptr ds:0x782 ; a08207 00007c8d: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif sub al, 0x31              ; 2c31 00007c8f: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif mov cl, 0x04              ; b104 00007c91: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif shl al, cl                ; d2e0 00007c93: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif xor ah, ah                ; 32e4 00007c95: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif add ax, 0x07be            ; 05be07 00007c98: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif mov word ptr ds:0x6f6, ax ; a3f606 00007c9b: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif mov cx, 0x0005            ; b90500 00007c9e: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif push cx                   ; 51 00007c9f: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif mov si, word ptr ds:0x6f6 ; 8b36f606 00007ca3: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif mov dx, word ptr ds:[si]  ; 8b14 Ds[si]内容为图1中地址01BE处内容。也就是DPT的首字。 00007ca5: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif mov cx, word ptr ds:[si+2] ; 8b4c02 00007ca8: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif mov bx, 0x7c00            ; bb007c 00007cab: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif mov ax, 0x0201            ; b80102 00007cae: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif int 0x13                  ; cd13 此时，DX=0180，CX=0001，BX=7C00，所以是将硬盘1磁头，0柱面，1扇区的内容读入7C00起始的内存中。我认为这段程序是存在BUG的。当活动分区的起始柱面号大于FFH时就会出错，什么时候柱面号会大于FFH，细看DPT后就会明了。 00007cb0: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif pop cx                    ; 59 00007cb1: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif jnb .+18                  ; 7312 读盘成功跳转至00007cc5。否则执行磁盘复位，重复读盘或显示出错信息 00007cb3: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif push ax                   ; 50 00007cb4: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif xor ax, ax                ; 33c0 00007cb6: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif int 0x13                  ; cd13 00007cb8: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif pop ax                    ; 58 00007cb9: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif cmp ah, 0x80              ; 80fc80 00007cbc: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif jz .+2                    ; 7402 00007cbe: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif loop .-34                 ; e2de 00007cc0: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif mov bx, 0x0724            ; bb2407 00007cc3: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif jmp .+20                  ; eb14 00007cc5: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif mov bx, 0x7c00            ; bb007c 00007cc8: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif cmp word ptr ds:[bx+510], 0xaa55 ; 81bffe0155aa   检查1磁头，0道，1扇区的分区表结束标志的有效性。 00007cce: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif jnz .+6                   ; 7506 00007cd0: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif mov si, word ptr ds:0x6f6 ; 8b36f606 00007cd4: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif push bx                   ; 53 00007cd5: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif ret                       ; c3 00007cd6: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif mov bx, 0x070f            ; bb0f07 00007cd9: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif call .+2                  ; e80200 00007cdc: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif jmp .-2                   ; ebfe 00007cde: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif mov al, byte ptr ds:[bx]  ; 8a07 00007ce0: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif or al, al                 ; 0ac0 00007ce2: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif jz .+17                   ; 7411 00007ce4: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif call .+3                  ; e80300 00007ce7: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif inc bx                    ; 43 00007ce8: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif jmp .-12                  ; ebf4 00007cea: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif push ax                   ; 50 00007ceb: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif push bx                   ; 53 00007cec: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif mov ah, 0x0e              ; b40e 00007cee: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif mov bx, 0x0007            ; bb0700 00007cf1: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif int 0x10                  ; cd10 00007cf3: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif pop bx                    ; 5b 00007cf4: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif pop ax                    ; 58 00007cf5: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif ret                       ; c3 00007cf6: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif add byte ptr ds:[bx+si], al ; 0000  <bochs:5> 现在，我们先放过MBR的内容，现在开始看分区表DPT。其实，没有注释部分的MBR内容，已经比较明了了。 我们将图1中主分区与扩展分区的描述项的内容写在下面： 80   01  01 00   0C   FE FF FF   3F 00 00 00   02 AB 10 03 00  00   C1 FF  0F   FE FF FF   41 AB 10 03   40 9A 0B 1A 先看主分区：80表示活动分区。01表示分区开始于1面或者1磁头。01 00，分区开始的扇区号和柱面号。这些在MBR程序中已做过介绍。 那么接下来0C，是系统标志，0C代表的含义是，FAT32，使用LBA模式和扩展的INT 13H。另外，FAT32还用0B表示，但0B的意义与0C是有区别的，分区格式小于等于8.4GB（实际可能是7.8）；但无论是0B还是0C基本没什么意义，大容量磁盘都不再会使用CHS模式来访问磁盘，而使用LBA（LBA28/LBA48等），而更大容量的磁盘甚至不再使用MBR分区格式，而是使用GPT分区格式，每个分区可以大于2TB，但我没有64位机，完全不懂。这这也是我们在研究MBR程序时说的INT13H使用上存在BUG的原因。因为每个磁道只能有111111B-1个扇区（扇区数从1开始），每个柱面的磁头号有FE个。DPT格式中柱面号最多可以表示到1111111111B（1024）个，但现在的磁盘都会超过个数，我们经常会看到EF FF FF，但这里的柱面号可能已经超过了1024，但仍然这样表示。所以，通过此项来计算分区起始或分区大小是不准确的。 NTFC的话则为07。 FE FF FF 是分区结束的磁头，扇区和柱面。通过这一项可以算出分区的大小，但前面我们刚刚说过这个是不准确的。 3F 00 00 00这个是硬盘的稳含扇区，也就是此分区的到引导区之间的扇区数目。意思是这样的，双字0000003F个扇区占多少个字节：3F\*200H=7E00H，于是我们找到硬盘数据7E00H地址，看一下这个扇区。  名称:  2.png 查看次数: 1 文件大小:  206.7 KB **图2**  我们再看一下C盘的数据，比较发现，C盘的数据地址00H起至200H的内容与这一扇区的内容是完全一样的。其实这就是主分区的扩展引导记录EBR（EXTAND BOOT RECORD），而活动磁盘上的EBR我们又称为：第二引导扇区或系统引导扇区DBR（DOS BOOT RECORD）。也是MBR程序要读取到内存7C00H地址处的内容。这也是C盘的开始扇区。所以上文称MBR为硬盘主引导记录，而不是C盘主引导记录。 02 AB 10 03表示分区的大小（扇区数）。分区的字节数是：0310AB02\*200H=621560400H，那么，621560400H+7E00H处是什么内容呢？  [点击图片以查看大图  图片名称: 3.png 查看次数: 1 文件大小: 56.5 KB 文件 ID : 82946](http://bbs.pediy.com/attachment.php?attachmentid=82946&d=1379434530) **图3**  这是哪里呢？首先这不是D盘的第一扇区。但这个扇区却有一个DPT。根据我们计算的过程，主分区应该是在这一扇区的上一扇区结束。那么这里是扩展分区的开始扇区。我们看一下扩展分区与主引导扇区间的扇区数为：41 AB 10 03。字节数为：0310AB41\*200H=621568200H，正好与图3中的地址吻合。那么扩展分区的大小：40 9A 0B 1A。1A0B9A40\*200H=3417348000H，再加上621568200H，减1正好是硬盘结束的地址：3A388B01FFH。  再看主分区，将621568200H-1，是主分区结束的字节地址。但是C盘却是在620917FFFH处结束。C盘共620918000H个字节，这个数字与WINDOWS看到的C盘容量（26316210176）是相同的。比主分区少了0C48400H个字节，这些字节在C盘之后。那么主分区不是C盘，C盘包含在主分区里。  现在看图3，这里的DPT也有两个分区表项。这里的DPT是主引导扇区分区表中扩展分区的再分区表。暂称作第二分区  第二分区的主分区（第二主分区）：00 01 C1 FF 0B FE FF FF 3F 00 00 00 00 4F D5 92 09 。非活动分区，开始磁头号为1，扇区号与柱面号为：C1 FF。结束磁头，扇区，柱面号为：FE FF FF。主分区距分区表的字节数是7E00，而这也与D盘的00H处的数据是相同的。D盘开始于第一扩展分区7E00字节处。在硬盘中的地址为621570000H。第二主分区的大小为：0992D54F\*200H=1325AA9E00H。D盘大小为：1324780000H比第二主分区小  1329E00H字节，距第二扩展分区1331A00H字节。  我们看到不仅C盘比第一分区的主分区小，D盘比第二分区的主分区小。那么C盘前面的60几个扇区，D盘前面和后面的扇区做什么用了呢？其实这些都是系统隐藏扇区，系统是无法访问的，除分区表的空间外，其他可以存储一些我们要保密的数据，在这里的数据通常情况下是安全的。但也许我们并不想要这些隐藏扇区，毕竟这些扇区也不是绝对安全的，至少破坏MBR的病毒就能找到这些扇区。要简单地解决这个问题现在只有一个办法：不使用MBR格式的分区，而使用GPT分区格式。因为MBR分区格式，必须是以柱面为单位的。不能对柱面进行分割。  好了，我们再看DPT分区表。DPT分区表的数据结构好像是一个单链表，第一分区：主分区地址，扩展分区地址指向下一个DPT分区表，NULL，NULL。第二分区：第二主分区地址，第二扩展分区地址指向第三分区DPT表，NULL，NULL。于是我们得出结论：最后一个分区：最后一个主分区地址，NULL，NULL，NULL。DPT中只要使用两个表项就可以做到很多个分区。以前的许多资料也是这样介绍DPT数据结构的。但我们通过DPT表寻找分区时并不是一帆风顺的，比如我的硬盘，230G，分为CDEF四个区，而第三分区DPT表扩展分区的隐含扇区却不是相对于第三分区分区表所在扇区的，而是相对于第二分区分区表所在扇区。原因我还不知道，是不是因为第四字节？哪位大神知道告诉我。  那么我们继续，我们看图二。DBR中也包括三部分内容：DBR程序，本分区参数记录表BPB（BIOS PARAMETER BLOCK）和结束标记55AA。这部分内容由高级格式化程序生成（与操作系统相关）。DBR程序的主要功能是判断本分区根目录前的两个文件是否是系统引导文件，并把第一个文件读入内存，并将控制权交给该文件。DBR程序从扇区0字节开始，前三个字节利用一个短转移+NOP指令（NOP指令一般是由编译器生成的，具体请参照汇编编译器关于JMP指令的编译）跳过从03H——59H共57H字节的BPB。  下面是图二中的内容的反汇编  <bochs:4> u/280 00007c00: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif jmp .+88                  ; eb58 跳转至7C5A 00007c02: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif nop                       ; 90   00007c5a: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif xor cx, cx                ; 33c9 00007c5c: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif mov ss, cx                ; 8ed1 00007c5e: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif mov sp, 0x7bf4            ; bcf47b 00007c61: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif mov es, cx                ; 8ec1 00007c63: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif mov ds, cx                ; 8ed9 00007c65: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif mov bp, 0x7c00            ; bd007c 00007c68: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif mov byte ptr ss:[bp+2], cl ; 884e02 00007c6b: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif mov dl, byte ptr ss:[bp+64] ; 8a5640 图2中偏移40H处的一个字节，是INT13H中断呼叫预设值，软盘为00H，硬盘为：80H 00007c6e: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif mov ah, 0x08              ; b408 00007c70: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif int 0x13                  ; cd13 00007c72: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif jnb .+5                   ; 7305 跳至00007C79。调用INT13H的8H号功能获取磁盘参数。INT13H的这一功能我不了解，听说，当磁盘大于8G时应当使用扩展的INT13H的48H号功能。如果使用8号功能则CF=1。但对于我的250G的硬盘，C盘24.5G，执行8号功能后，CF=0，而CX=FEFF，DX=FE01。所以这里肯定有没搞明白的地方。 00007c74: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif mov cx, 0xffff            ; b9ffff 00007c77: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif mov dh, cl                ; 8af1 00007c79: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif movzx eax, dh             ; 660fb6c6 00007c7d: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif inc ax                    ; 40 00007c7e: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif movzx edx, cl             ; 660fb6d1 00007c82: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif and dl, 0x3f              ; 80e23f 00007c85: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif mul ax, dx                ; f7e2 00007c87: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif xchg ch, cl               ; 86cd 00007c89: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif shr ch, 0x06              ; c0ed06 00007c8c: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif inc cx                    ; 41 00007c8d: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif movzx ecx, cx             ; 660fb7c9 00007c91: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif mul eax, ecx              ; 66f7e1 将CHS换算成LBA线性地址 00007c94: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif mov dword ptr ss:[bp-8], eax ; 668946f8 00007c98: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif cmp word ptr ss:[bp+22], 0x0000 ; 837e1600 00007c9c: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif jnz .+56                  ; 7538 图二中相对扇区起始偏移16 H地址处的一个字表示FAT16文件分配表的长度，FAT32位则为零 00007c9e: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif cmp word ptr ss:[bp+42], 0x0000 ; 837e2a00 00007ca2: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif jnbe .+50                 ; 7732 图2相对扇区起始偏移2AH处的两个字节表示文件系统的主次版本。这里为0不跳转 00007ca4: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif mov eax, dword ptr ss:[bp+28] ; 668b461c 图2相对扇区起始偏移1C处的一个双字，表示分区前隐藏扇区数目，也就是分区表到EBR的扇区偏移。 00007ca8: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif add eax, 0x0000000c       ; 6683c00c 至于这里为什么是0CH，可能是MS公司规定的。 00007cac: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif mov bx, 0x8000            ; bb0080 00007caf: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif mov cx, 0x0001            ; b90100 00007cb2: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif call .+43                 ; e82b00 转移至00007ce0。7CE0处是一个过程，将会把相对分区表偏移EAX个扇区开始的共ECX个扇区内容装入内存ES：BX处。 00007cb5: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif jmp .+840                 ; e94803 跳转至：0X：8000，也就是将系统控制权交给硬盘相对MBR扇区偏移3FH+CH扇区存放的程序。为了更深入理解BPB我们还要对这个程序进行分析。我们暂称这个程序为操作系统引导程序。 00007cb8: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif mov al, byte ptr ds:0x7dfa ; a0fa7d 由此可以看出图二中相对扇区起始偏移01F9至01FB存放的数据是出错信息相对扇区起始偏移地址的低八位。以下显示一段信息：Disk erro 换行Press any key to restart 00007cbb: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif mov ah, 0x7d              ; b47d 00007cbd: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif mov si, ax                ; 8bf0 00007cbf: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif lodsb al, byte ptr ds:[si] ; ac 00007cc0: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif test al, al               ; 84c0 00007cc2: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif jz .+23                   ; 7417 DBR中的出错信息共三行，用FFH间隔，用00H结束，当显示完Press any key to restart后则执行7CDB处的CBW命令。等待输入重新运行MBR。 00007cc4: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif cmp al, 0xff              ; 3cff 00007cc6: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif jz .+9                    ; 7409 00007cc8: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif mov ah, 0x0e              ; b40e 00007cca: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif mov bx, 0x0007            ; bb0700 00007ccd: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif int 0x10                  ; cd10 00007ccf: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif jmp .-18                  ; ebee 跳至7CBF 00007cd1: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif mov al, byte ptr ds:0x7dfb ; a0fb7d 00007cd4: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif jmp .-27                  ; ebe5 00007cd6: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif mov al, byte ptr ds:0x7df9 ; a0f97d 00007cd9: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif jmp .-32                  ; ebe0 跳至7CBB 00007cdb: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif cbw                       ; 98 00007cdc: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif int 0x16                  ; cd16 00007cde: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif int 0x19                  ; cd19  过程开始 00007ce0: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif pushad                    ; 6660 00007ce2: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif cmp eax, dword ptr ss:[bp-8] ; 663b46f8 将EAX的值与前面利用INT13H获得的磁盘参数计算出的LBA线性扇区数比较，看是否超过此范围，。 00007ce6: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif jb .+74                   ; 0f824a00 未超范围则跳转至7d34，否则调用扩展的INT13H。 00007cea: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif push 0x00000000           ; 666a00 00007ced: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif push eax                  ; 6650 00007cef: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif push es                   ; 06 00007cf0: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif push bx                   ; 53 00007cf1: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif push 0x00010010           ; 666810000100 00007cf7: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif cmp byte ptr ss:[bp+2], 0x00 ; 807e0200 00007cfb: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif jnz .+32                  ; 0f852000 00007cff: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif mov ah, 0x41              ; b441 00007d01: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif mov bx, 0x55aa            ; bbaa55 00007d04: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif mov dl, byte ptr ss:[bp+64] ; 8a5640 00007d07: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif int 0x13                  ; cd13 检查INT13H扩展功能是否存在 00007d09: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif jb .+28                   ; 0f821c00 00007d0d: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif cmp bx, 0xaa55            ; 81fb55aa 00007d11: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif jnz .+20                  ; 0f851400 00007d15: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif test cl, 0x01             ; f6c101 00007d18: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif jz .+13                   ; 0f840d00 00007d1c: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif inc byte ptr ss:[bp+2]    ; fe4602 00007d1f: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif mov ah, 0x42              ; b442 00007d21: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif mov dl, byte ptr ss:[bp+64] ; 8a5640 00007d24: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif mov si, sp                ; 8bf4 00007d26: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif int 0x13                  ; cd13 扩展读 00007d28: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif mov al, 0xf9              ; b0f9 00007d2a: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif pop eax                   ; 6658 00007d2c: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif pop eax                   ; 6658 00007d2e: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif pop eax                   ; 6658 00007d30: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif pop eax                   ; 6658 00007d32: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif jmp .+42                  ; eb2a 00007d34: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif xor edx, edx              ; 6633d2 00007d37: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif movzx ecx, word ptr ss:[bp+24] ; 660fb74e18 图2扇区起始偏移18H处的两个字节表示：每磁道的扇区数。值为003F。 00007d3c: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif div eax, ecx              ; 66f7f1 00007d3f: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif inc dl                    ; fec2 00007d41: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif mov cl, dl                ; 8aca 00007d43: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif mov edx, eax              ; 668bd0 00007d46: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif shr edx, 0x10             ; 66c1ea10 00007d4a: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif div ax, word ptr ss:[bp+26] ; f7761a 图2中相对扇区起始偏移1A处的两个字节表示磁盘的磁头数，值为FFH 00007d4d: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif xchg dh, dl               ; 86d6 00007d4f: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif mov dl, byte ptr ss:[bp+64] ; 8a5640 40H处存放驱动器号 00007d52: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif mov ch, al                ; 8ae8 00007d54: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif shl ah, 0x06              ; c0e406 00007d57: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif or cl, ah                 ; 0acc 以上将LBA转换为CHS 00007d59: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif mov ax, 0x0201            ; b80102 00007d5c: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif int 0x13                  ; cd13 00007d5e: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif popad                     ; 6661 00007d60: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif jb .-172                  ; 0f8254ff 如果CF=1则跳至00007cb8 00007d64: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif add bx, 0x0200            ; 81c30002 00007d68: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif inc eax                   ; 6640 00007d6a: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif dec cx                    ; 49 00007d6b: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif jnz .-143                 ; 0f8571ff 00007d6f: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif ret                       ; c3  过程正常返回  00007d70: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif dec si                    ; 4e 00007d71: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif push sp                   ; 54 00007d72: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif dec sp                    ; 4c 00007d73: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif inc sp                    ; 44 00007d74: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif push dx                   ; 52 00007d75: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif and byte ptr ds:[bx+si], ah ; 2020 00007d77: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif and byte ptr ds:[bx+si], ah ; 2020 00007d79: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif and byte ptr ds:[bx+si], ah ; 2020 00007d7b: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif add byte ptr ds:[bx+si], al ; 0000 00007d7d: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif add byte ptr ds:[bx+si], al ; 0000 00007d7f: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif add byte ptr ds:[bx+si], al ; 0000 00007d81: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif add byte ptr ds:[bx+si], al ; 0000 00007d83: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif add byte ptr ds:[bx+si], al ; 0000 00007d85: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif add byte ptr ds:[bx+si], al ; 0000 00007d87: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif add byte ptr ds:[bx+si], al ; 0000 00007d89: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif add byte ptr ds:[bx+si], al ; 0000 00007d8b: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif add byte ptr ds:[bx+si], al ; 0000 00007d8d: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif add byte ptr ds:[bx+si], al ; 0000 00007d8f: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif add byte ptr ds:[bx+si], al ; 0000 00007d91: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif add byte ptr ds:[bx+si], al ; 0000 00007d93: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif add byte ptr ds:[bx+si], al ; 0000 00007d95: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif add byte ptr ds:[bx+si], al ; 0000 00007d97: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif add byte ptr ds:[bx+si], al ; 0000 00007d99: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif add byte ptr ds:[bx+si], al ; 0000 00007d9b: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif add byte ptr ds:[bx+si], al ; 0000 00007d9d: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif add byte ptr ds:[bx+si], al ; 0000 00007d9f: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif add byte ptr ds:[bx+si], al ; 0000 00007da1: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif add byte ptr ds:[bx+si], al ; 0000 00007da3: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif add byte ptr ds:[bx+si], al ; 0000 00007da5: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif add byte ptr ds:[bx+si], al ; 0000 00007da7: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif add byte ptr ds:[bx+si], al ; 0000 00007da9: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif add byte ptr ds:[bx+si], al ; 0000 00007dab: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif add byte ptr ds:[di], cl  ; 000d 00007dad: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif or cl, byte ptr ss:[bp+84] ; 0a4e54 00007db0: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif dec sp                    ; 4c 00007db1: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif inc sp                    ; 44 00007db2: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif push dx                   ; 52 00007db3: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif and byte ptr ds:[bx+di+115], ch ; 206973 00007db6: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif and byte ptr ds:[di+105], ch ; 206d69 00007db9: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif jnb .+115                 ; 7373 00007dbb: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif imul bp, word ptr ss:[bp+103], 0x0dff ; 696e67 ff0d 00007dc0: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif or al, byte ptr ds:[si+105] ; 0a4469 00007dc3: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif jnb .+107                 ; 736b 00007dc5: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif and byte ptr ds:[di+114], ah ; 206572 00007dc8: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif jb .+111                  ; 726f 00007dca: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif jb .-1                    ; 72ff 00007dcc: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif or ax, 0x500a             ; 0d0a50 00007dcf: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif jb .+101                  ; 7265 00007dd1: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif jnb .+115                 ; 7373 00007dd3: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif and byte ptr ds:[bx+di+110], ah ; 20616e 00007dd6: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif jns .+32                  ; 7920 00007dd8: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif imul sp, word ptr ds:[di+121], 0x0020 ; 6b6579 20 00007ddc: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif jz .+111                  ; 746f 00007dde: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif and byte ptr ss:[bp+si+101], dh ; 207265 00007de1: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif jnb .+116                 ; 7374 00007de3: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif popa                      ; 61 00007de4: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif jb .+116                  ; 7274 00007de6: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif or ax, 0x000a             ; 0d0a00 00007de9: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif add byte ptr ds:[bx+si], al ; 0000 00007deb: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif add byte ptr ds:[bx+si], al ; 0000 00007ded: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif add byte ptr ds:[bx+si], al ; 0000 00007def: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif add byte ptr ds:[bx+si], al ; 0000 00007df1: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif add byte ptr ds:[bx+si], al ; 0000 00007df3: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif add byte ptr ds:[bx+si], al ; 0000 00007df5: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif add byte ptr ds:[bx+si], al ; 0000 00007df7: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif add byte ptr ds:[bx+si], al ; 0000 00007df9: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif lodsb al, byte ptr ds:[si] ; ac 00007dfa: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif mov di, 0x00cc            ; bfcc00 00007dfd: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif add byte ptr ds:[di-86], dl ; 0055aa  下面是具体BPB各参数的意义： FAT32系统： 0BH    2字节  每扇区的字节数一般为0200H。 0DH    1字节  每簇扇区数，取决于分区文件系统格式和分区大小。我的C盘上是20H 0EH    2字节  为操作系统保留的扇区数。也即逻辑盘引导区至文件分配表（FAT表）的偏移，以扇区为单位。图2中为26H 10H    1字节  FAT表的个数，一般为02H。 11H    2字节  FAT16中根目录中允许登记的目录项的个数。FAT32中为0。 13H    2字节  容量小于32MB时表示扇区数目，否则不使用，仅为兼容小磁盘，FAT32中为0 15H    1字节  磁盘介质类型，硬盘用F8表示。 16H    2字节  FAT16中文件分配表长度，FAT32中未使用，值为0 18H    2字节  每磁道扇区数。003F 1AH    2字节  磁盘磁头数。图二中0FFH表示255个磁头。 1CH    4字节  分区前隐藏的扇区数。即该分区分区表到引导扇区的扇区数目：0000003F 20H    4字节  逻辑盘的扇区总数。图二中为0310AAF0，即62155E000H字节。这个比C盘的实际容量：620918000H字节要大，而又比分区表DPT中所标识的字节数：621560400H要小。我们从硬盘上看，偏移0310AAF0+3F-1扇区之前都是有数据的。而从0310AAF0+3F至第一主分区结束则无数据存储，全部为0。 24H    4字节  每个FAT表所占扇区数目。 28H    2字节  FAT表镜像标志。0表示保存有两份FAT表互为备份，而1则只有一份。 2AH    2字节  文件系统主次版本（fat32系统保留未使用） 2CH    4字节  磁盘根目录起始簇号 30H    2字节  文件系统参数扇区号，通常为引导扇区的下一扇区。即01H 32H    2字节  备份分区引导扇区的扇区号 34H    12字节  保留未使用。 40H    1字节  磁盘号，为INT13H呼叫所做的预高值，80为硬盘，00为软盘 41H    1字节  用于中断13H呼叫 42H    1字节  磁盘读写参数扩展标志，值为29H 43H    4字节  格式化时随机产生的磁盘卷的序列号 47H    11字节  格式化时人工输入的磁盘卷标号 52H    8字节  文件系统标识号（FAT32）  而NTFC文件系统则不同，BPB的长度也不一样。 操作系统引导程序：  名称:  4.png 查看次数: 1 文件大小:  135.1 KB **图4**  00008000: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif movzx eax, byte ptr ss:[bp+16] ; 660fb64610 00008005: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif mov ecx, dword ptr ss:[bp+36] ; 668b4e24 00008009: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif mul eax, ecx              ; 66f7e1 0000800c: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif add eax, dword ptr ss:[bp+28] ; 6603461c 00008010: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif movzx edx, word ptr ss:[bp+14] ; 660fb7560e 00008015: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif add eax, edx              ; 6603c2 00008018: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif mov dword ptr ss:[bp-4], eax ; 668946fc 以上计算文件分配表结束后的第一个扇区相对硬盘0面0道1扇区的偏移。并存入内存7BFCH。 0000801c: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif mov dword ptr ss:[bp-12], 0xffffffff ; 66c746f 4ffffffff 00008024: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif mov eax, dword ptr ss:[bp+44] ; 668b462c 00008028: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif cmp eax, 0x00000002       ; 6683f802 0000802c: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif jb .-858                  ; 0f82a6fc 如果根目录起始簇数小于2则跳至7CD6显示一段出错信息：“NTLDR is missing”  另起行：“Press any key to restart”。为什么要与2进行比较，这与文件分配表FAT有关。FAT表中前两个表项（表项00，01）一般不用，而用来存储磁盘的介质类型。FAT32系统硬盘一般为F8 FF FF 0F  FF FF FF 0F。所以有效簇号是从2开始的。下面简介下FAT表  名称:  6.png 查看次数: 1 文件大小:  130.5 KB **图6**  图6是FAT表第一扇区的内容。FAT表的每一个表项是4字节。第0，1表项的值是F8 FF FF 0F  FF FF FF FF。和我们上面说的不一样？看完后面再来理解：FAT表项值只要大于等0FFFFFF8就意味着文件在此簇号结束，而0FFFFFF7（F7 FF FF 0F）则意味着坏簇。而下一行程序的数字0FFFFFF8也就可以理解了。所有小于这个数字并且大于1的数字都表示文件的下一簇号——文件往往一个簇放不下，那么就将文件用到的第一个簇号存在PDT中，找到这一簇号对应的FAT表项，则以下是一个链表，这个链表只有一个数据项：一个指针，指向下一个链表的地址。一个文件在PAT表中的各表项就是这样一个链表。当链表指向大于0FFFFFF8时，链表结束。 00008030: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif cmp eax, 0x0ffffff8       ; 663df8ffff0f 00008036: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif jnb .-868                 ; 0f839cfc   FC9C+803A=7CD6 0000803a: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif push eax                  ; 6650 0000803c: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif sub eax, 0x00000002       ; 6683e802 00008040: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif movzx ebx, byte ptr ss:[bp+13] ; 660fb65e0d 00008045: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif mov si, bx                ; 8bf3 00008047: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif mul eax, ebx              ; 66f7e3 0000804a: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif add eax, dword ptr ss:[bp-4] ; 660346fc 0000804e: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif mov bx, 0x8200            ; bb0082 00008051: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif mov di, bx                ; 8bfb 00008053: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif mov cx, 0x0001            ; b90100 00008056: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif call .-889                ; e887fc 调用7CE0过程。将相对0面0道1扇区偏移626FH扇区的一个扇区内容，读入内存8200H。 00008059: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif cmp byte ptr ds:[di], ch  ; 382d 0000805b: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif jz .+30                   ; 741e 1E+805D=807B 0000805d: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif mov cl, 0x0b              ; b10b 0000805f: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif push si                   ; 56 00008060: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif mov si, 0x7d70            ; be707d 00008063: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif rep cmpsb byte ptr es:[di], byte ptr ds:[si] ;  f3a6 在这里应当是REPE CMPSB 应该是反汇编的问题。这个操作其实是在文件目录表FDT(File Directory Table)中查找名称为NTLDR的文件，这个文件在C盘根目录。请看下面关于FDT的介绍。  [点击图片以查看大图  图片名称: 5.png 查看次数: 0 文件大小: 174.9 KB 文件 ID : 82949](http://bbs.pediy.com/attachment.php?attachmentid=82949&d=1379434822) **图5**  FDT中长文件名与否决定了表项长度，32B或64B。如果是64B则前32B为长文件名链接说明，后32字节为文件属性说明：文件长度，起始地址，日期时间等。不支持长文件名的情况下，只有32B的文件属性说明。具体来说： 0-7字节    文件名 8-A字节    文件扩展名 0B字节    文件属性。对于FAT32来讲，0至5位分别是只读位、隐藏位、系统位、卷标位、子目录位、归档位。最高两位保留未用 0C-0D字节  短文件名字节校验和 0E-0F字节  文件创建时间 10-11字节  文件创建日期 12-13字节  文件最近访问日期 14-15字节  文件存放的起始簇号高16位 16-17字节  文件最近修改时间 18-19字节  文件最近修改日期 1A-1B字节  文件存放的起始簇号低16位 1C-1F字节  文件长度（字节） 其中文件名部分，字节不足则用空格的ASCII码20填充。而0字节还有特别的含义。00表示空目录。E5表示被删除的文件，2E表示特殊文件“.”或“..”。其他值才表示文件名的第一个字符ASCII码。 00008065: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif pop si                    ; 5e 00008066: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif jz .+27                   ; 741b 8068+1B=8083。从图五可以看出当DI=8280H+0BH时跳转。 00008068: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif add di, cx                ; 03f9 0000806a: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif add di, 0x0015            ; 83c715 从805D到这里，相当于DI=DI+20H。 0000806d: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif cmp di, bx                ; 3bfb 0000806f: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif jb .-24                   ; 72e8 E8+71=59 00008071: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif dec si                    ; 4e 00008072: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif jnz .-38                  ; 75da 00008074: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif pop eax                   ; 6658 00008076: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif call .+101                ; e86500 00008079: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif jb .-65                   ; 72bf  0000807b: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif add sp, 0x0004            ; 83c404 0000807e: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif jmp .-939                 ; e955fc FC55+8081=7CD6 00008081: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif add byte ptr ds:[bx+si], ah ; 0020  以下查找NTLDR的起始位置并将NTLDR文件完整地读入内存，并将系统控制仅交给NTLDR程序。 00008083: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif add sp, 0x0004            ; 83c404 00008086: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif mov si, word ptr ds:[di+9] ; 8b7509 SI=0 00008089: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif mov di, word ptr ds:[di+15] ; 8b7d0f DI=F9A5 0000808c: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif mov ax, si                ; 8bc6 0000808e: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif shl eax, 0x10             ; 66c1e010 00008092: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif mov ax, di                ; 8bc7 00008094: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif cmp eax, 0x00000002       ; 6683f802 00008098: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif jb .-966                  ; 0f823afc 0000809c: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif cmp eax, 0x0ffffff8       ; 663df8ffff0f 000080a2: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif jnb .-976                 ; 0f8330fc 000080a6: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif push eax                  ; 6650 000080a8: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif sub eax, 0x00000002       ; 6683e802 000080ac: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif movzx ecx, byte ptr ss:[bp+13] ; 660fb64e0d 000080b1: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif mul eax, ecx              ; 66f7e1 000080b4: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif add eax, dword ptr ss:[bp-4] ; 660346fc 000080b8: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif mov bx, 0x0000            ; bb0000 000080bb: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif push es                   ; 06 000080bc: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif mov es, word ptr ds:0x8081 ; 8e068180 ES=2000，BX=0，EAX=1F96CFH 000080c0: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif call .-995                ; e81dfc FC1D+80C3=7CE0 000080c3: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif pop es                    ; 07 ES=0 000080c4: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif pop eax                   ; 6658 EAX=F9A5 000080c6: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif shr bx, 0x04              ; c1eb04 000080c9: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif add word ptr ds:0x8081, bx ; 011e8180 将刚分配的字节数右移四位加到8081H处做为下一次分配内存的段地址。 000080cd: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif call .+14                 ; e80e00 80D0+0E=80DE 000080d0: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif jnb .+2                   ; 0f830200 000080d4: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif jb .-48                   ; 72d0 D0+80D6=8086，如果不是文件的最后一簇则重复读下一簇。NTLR共用10H个簇 000080d6: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif mov dl, byte ptr ss:[bp+64] ; 8a5640 000080d9: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif jmp far 2000:0000         ; ea00000020  000080de: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif shl eax, 0x02             ; 66c1e002 000080e2: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif call .+17                 ; e81100 80E5+11=80F6 000080e5: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif mov eax, dword ptr es:[bx+di] ; 26668b01 ES=0，DI=7E00，所以此时EAX的值等于NTLR文件起始簇号所对应FAT表项的值。 000080e9: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif and eax, 0x0fffffff       ; 6625ffffff0f 000080ef: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif cmp eax, 0x0ffffff8       ; 663df8ffff0f 而FAT表项的值，如果大于0FFFFFF8则表示此簇为文件的最后一簇，否则为文件存放的下一簇号。 000080f5: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif ret                       ; c3 下面的过程计算NTLR文件起始簇号所对应FAT表项的扇区（EAX）和相对扇区起始的偏移（EDX），将表项所在扇区相对0道0面1扇区的相对偏移，并将其读入内存7E00H处。而最终BX值等于FAT表中NTLR文件起始簇号所对应表项相对扇区开始的偏移。 000080f6: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif mov di, 0x7e00            ; bf007e 000080f9: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif movzx ecx, word ptr ss:[bp+11] ; 660fb74e0b 000080fe: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif xor edx, edx              ; 6633d2 00008101: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif div eax, ecx              ; 66f7f1 00008104: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif cmp eax, dword ptr ss:[bp-12] ; 663b46f4 00008108: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif jz .+58                   ; 743a 0000810a: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif mov dword ptr ss:[bp-12], eax ; 668946f4 0000810e: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif add eax, dword ptr ss:[bp+28] ; 6603461c 00008112: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif movzx ecx, word ptr ss:[bp+14] ; 660fb74e0e 00008117: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif add eax, ecx              ; 6603c1 0000811a: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif movzx ebx, word ptr ss:[bp+40] ; 660fb75e28 0000811f: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif and bx, 0x000f            ; 83e30f 00008122: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif jz .+22                   ; 7416 16+8124=813A 00008124: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif cmp bl, byte ptr ss:[bp+16] ; 3a5e10 00008127: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif jnb .-1109                ; 0f83abfb FBAB+812B=7CD6H 0000812b: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif push dx                   ; 52 0000812c: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif mov ecx, eax              ; 668bc8 0000812f: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif mov eax, dword ptr ss:[bp+36] ; 668b4624 00008133: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif mul eax, ebx              ; 66f7e3 00008136: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif add eax, ecx              ; 6603c1 00008139: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif pop dx                    ; 5a  0000813a: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif push dx                   ; 52 0000813b: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif mov bx, di                ; 8bdf 0000813d: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif mov cx, 0x0001            ; b90100 00008140: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif call .-1123               ; e89dfb FB9D+8143=7CE0H 00008143: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif pop dx                    ; 5a 00008144: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif mov bx, dx                ; 8bda 00008146: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif ret                       ; c3 00008147: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif add byte ptr ds:[bx+si], al ; 0000 00008149: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif add byte ptr ds:[bx+si], al ; 0000 000081f9: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif add byte ptr ds:[bx+si], al ; 0000 000081fb: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif add byte ptr ds:[bx+si], al ; 0000 000081fd: (                   &nbsphttp://bbs.pediy.com/images/smilies/wink.gif add byte ptr ds:[di-86], dl ; 0055aa   接下来跳至2000：00H处执行的程序就有点大了，20H个扇区，而实际上这个程序的有效字节大约在30000H多。这就可以做很多事情，比如：进入保护模式等，离主题越来越远了。 好了，我们回到正题。上面程序中是如何计算表项地址的？ FAT表项所在扇区相对FAT表起始扇区偏移扇区数（对应扇区）=对应簇号\*4/200，因为每个FAT表项占4个字节。 FAT表项相对对应扇区偏移字节=对应簇号\*4%200。 操作系统就是通过这种方法利用FDT和FAT查找并将文件读入内存。  紧接FDT的就是罗辑盘的DATA区。具体存放各种文件（以簇为单位）。当EBR，FAT，甚至FDT损坏后，其实，我们仍然可以通过搜索DATA区的办法来恢复文件。   注：本帖由看雪论坛志愿者PEstone 重新将DOC整理排版，若和原文有出入，以原作者附件为准  上传的附件   |  |  | | --- | --- | | 文件类型: rar | [硬盘.rar](http://bbs.pediy.com/attachment.php?attachmentid=81152&d=1374841198) (1,003.4 KB, 391 次下载) | |
|  |
| 此帖于 2013-09-29*00:45:07*被 PEstone 最后编辑  http://bbs.pediy.com/images/pediy/statusicon/line.gif [[公告]如果你觉得有人语言挑衅，请点每帖右上角的“举报”按钮！](http://bbs.pediy.com/showthread.php?t=71978)  [回复时引用此帖](http://bbs.pediy.com/newreply.php?do=newreply&p=1203215) [返回顶端](http://bbs.pediy.com/showthread.php?t=176156#top) |

|  |  |  |  |
| --- | --- | --- | --- |
| [a糊涂虫](http://bbs.pediy.com/member.php?u=554440)  级别:21 | 在线时长:571小时 | 升级还需:1小时级别:21 | 在线时长:571小时 | 升级还需:1小时级别:21 | 在线时长:571小时 | 升级还需:1小时  [a糊涂虫 的头像](http://bbs.pediy.com/member.php?u=554440)  初级会员  初级会员  资　料:  注册日期: Nov 2012  帖子: [232](http://bbs.pediy.com/search.php?do=finduser&u=554440) a糊涂虫 品行端正  精华: 0  现金: 85 Kx  致谢数: 10  获感谢文章数：0 获会员感谢数：0 | |  |  | | --- | --- | | **[2](http://bbs.pediy.com/showpost.php?p=1203219&postcount=2" \t "new)** 旧 2013-07-26, 20:28:29 默认 | a糊涂虫 当前离线 |   楼主估计是下了不少功夫 |
|  |
| http://bbs.pediy.com/images/pediy/statusicon/line.gif [[招生]15PB软件安全培训开始接受第007期报名（05.05开课）！](http://bbs.pediy.com/showthread.php?t=168402)  [回复时引用此帖](http://bbs.pediy.com/newreply.php?do=newreply&p=1203219) [返回顶端](http://bbs.pediy.com/showthread.php?t=176156#top) |
| [白玉箫](http://bbs.pediy.com/member.php?u=428523)  级别:34 | 在线时长:1339小时 | 升级还需:26小时级别:34 | 在线时长:1339小时 | 升级还需:26小时级别:34 | 在线时长:1339小时 | 升级还需:26小时级别:34 | 在线时长:1339小时 | 升级还需:26小时  初级会员  初级会员  资　料:  注册日期: May 2011  帖子: [163](http://bbs.pediy.com/search.php?do=finduser&u=428523) 白玉箫 品行端正  精华: 0  现金: 437 Kx  致谢数: 3  获感谢文章数：1 获会员感谢数：1 | |  |  | | --- | --- | | **[3](http://bbs.pediy.com/showpost.php?p=1203226&postcount=3" \t "new)** 旧 2013-07-26, 20:49:08 默认 | 白玉箫 当前离线 |   FAT32还算简单的 你看过刘伟写的那本数据恢复的书 并写过恢复类软件的话 对磁盘的理解会更深 |
|  |
| http://bbs.pediy.com/images/pediy/statusicon/line.gif [[招生]15PB软件安全培训开始接受第007期报名（05.05开课）！](http://bbs.pediy.com/showthread.php?t=168402)  [回复时引用此帖](http://bbs.pediy.com/newreply.php?do=newreply&p=1203226) [返回顶端](http://bbs.pediy.com/showthread.php?t=176156#top) |

|  |  |  |  |
| --- | --- | --- | --- |
| [zhczf](http://bbs.pediy.com/member.php?u=75640)  级别:6 | 在线时长:63小时 | 升级还需:14小时级别:6 | 在线时长:63小时 | 升级还需:14小时级别:6 | 在线时长:63小时 | 升级还需:14小时  初级会员  初级会员  资　料:  注册日期: Feb 2007  帖子: [239](http://bbs.pediy.com/search.php?do=finduser&u=75640) zhczf 品行端正  精华: 0  现金: 198 Kx  致谢数: 245  获感谢文章数：0 获会员感谢数：0 | |  |  | | --- | --- | | **[4](http://bbs.pediy.com/showpost.php?p=1203229&postcount=4" \t "new)** 旧 2013-07-26, 21:02:58 默认 | zhczf 当前离线 |   支持楼主。楼主没有上过大学，但很厉害 |
|  |
| http://bbs.pediy.com/images/pediy/statusicon/line.gif [[培训]"麦洛克菲"内核底层开发培训，看雪会员报名减免200元！](http://bbs.pediy.com/showthread.php?t=142155)  [回复时引用此帖](http://bbs.pediy.com/newreply.php?do=newreply&p=1203229) [返回顶端](http://bbs.pediy.com/showthread.php?t=176156#top) |
| [黑涩火焰](http://bbs.pediy.com/member.php?u=425108)  级别:7 | 在线时长:86小时 | 升级还需:10小时级别:7 | 在线时长:86小时 | 升级还需:10小时级别:7 | 在线时长:86小时 | 升级还需:10小时级别:7 | 在线时长:86小时 | 升级还需:10小时  [黑涩火焰 的头像](http://bbs.pediy.com/member.php?u=425108)  初级会员  初级会员  资　料:  注册日期: Apr 2011  帖子: [18](http://bbs.pediy.com/search.php?do=finduser&u=425108) 黑涩火焰 品行端正  精华: 0  现金: 20 Kx  致谢数: 0  获感谢文章数：0 获会员感谢数：0 | |  |  | | --- | --- | | **[5](http://bbs.pediy.com/showpost.php?p=1203256&postcount=5" \t "new)** 旧 2013-07-26, 22:08:09 默认 | 黑涩火焰 当前离线 |   标记下…！^\_^ |
|  |
| http://bbs.pediy.com/images/pediy/statusicon/line.gif [[培训]"麦洛克菲"内核底层开发培训，看雪会员报名减免200元！](http://bbs.pediy.com/showthread.php?t=142155)  [回复时引用此帖](http://bbs.pediy.com/newreply.php?do=newreply&p=1203256) [返回顶端](http://bbs.pediy.com/showthread.php?t=176156#top) |

|  |  |  |  |
| --- | --- | --- | --- |
| [Prolovecui](http://bbs.pediy.com/member.php?u=591686)  级别:21 | 在线时长:569小时 | 升级还需:3小时级别:21 | 在线时长:569小时 | 升级还需:3小时级别:21 | 在线时长:569小时 | 升级还需:3小时  [Prolovecui 的头像](http://bbs.pediy.com/member.php?u=591686)  初级会员  初级会员  资　料:  注册日期: Jul 2013  帖子: [69](http://bbs.pediy.com/search.php?do=finduser&u=591686) Prolovecui 品行端正  精华: 0  现金: 379 Kx  致谢数: 4  获感谢文章数：0 获会员感谢数：0 | |  |  | | --- | --- | | **[6](http://bbs.pediy.com/showpost.php?p=1203266&postcount=6" \t "new)** 旧 2013-07-26, 22:41:03 默认 | Prolovecui 当前离线 |   很好，支持一下。 |
|  |
| http://bbs.pediy.com/images/pediy/statusicon/line.gif [[培训]"麦洛克菲"内核底层开发培训，看雪会员报名减免200元！](http://bbs.pediy.com/showthread.php?t=142155)  [回复时引用此帖](http://bbs.pediy.com/newreply.php?do=newreply&p=1203266) [返回顶端](http://bbs.pediy.com/showthread.php?t=176156#top) |
| [cnppk](http://bbs.pediy.com/member.php?u=440935)  级别:30 | 在线时长:1055小时 | 升级还需:30小时级别:30 | 在线时长:1055小时 | 升级还需:30小时级别:30 | 在线时长:1055小时 | 升级还需:30小时级别:30 | 在线时长:1055小时 | 升级还需:30小时级别:30 | 在线时长:1055小时 | 升级还需:30小时级别:30 | 在线时长:1055小时 | 升级还需:30小时  [cnppk 的头像](http://bbs.pediy.com/member.php?u=440935)  初级会员  初级会员  资　料:  注册日期: Jul 2011  帖子: [109](http://bbs.pediy.com/search.php?do=finduser&u=440935) cnppk 品行端正  精华: 0  现金: 524 Kx  致谢数: 0  获感谢文章数：0 获会员感谢数：0 | |  |  | | --- | --- | | **[7](http://bbs.pediy.com/showpost.php?p=1206172&postcount=7" \t "new)** 旧 2013-08-04, 17:25:44 默认 | cnppk 当前离线 |   标记一下 |
|  |
| http://bbs.pediy.com/images/pediy/statusicon/line.gif [[招生]15PB软件安全培训开始接受第007期报名（05.05开课）！](http://bbs.pediy.com/showthread.php?t=168402)  [回复时引用此帖](http://bbs.pediy.com/newreply.php?do=newreply&p=1206172) [返回顶端](http://bbs.pediy.com/showthread.php?t=176156#top) |

|  |  |  |  |
| --- | --- | --- | --- |
| [Stimulants](http://bbs.pediy.com/member.php?u=586715)  级别:6 | 在线时长:62小时 | 升级还需:15小时级别:6 | 在线时长:62小时 | 升级还需:15小时级别:6 | 在线时长:62小时 | 升级还需:15小时  [Stimulants 的头像](http://bbs.pediy.com/member.php?u=586715)  初级会员  初级会员  资　料:  注册日期: Jun 2013  帖子: [17](http://bbs.pediy.com/search.php?do=finduser&u=586715) Stimulants 品行端正  精华: 0  现金: 23 Kx  致谢数: 0  获感谢文章数：0 获会员感谢数：0 | |  |  | | --- | --- | | **[8](http://bbs.pediy.com/showpost.php?p=1206291&postcount=8" \t "new)** 旧 2013-08-05, 08:35:12 默认 | Stimulants 当前离线 |   看到楼上那些大牛，表示膜拜啊！ |
|  |
| http://bbs.pediy.com/images/pediy/statusicon/line.gif [[公告]如果你觉得有人语言挑衅，请点每帖右上角的“举报”按钮！](http://bbs.pediy.com/showthread.php?t=71978)  [回复时引用此帖](http://bbs.pediy.com/newreply.php?do=newreply&p=1206291) [返回顶端](http://bbs.pediy.com/showthread.php?t=176156#top) |
| [zhaohumm](http://bbs.pediy.com/member.php?u=436274)  级别:12 | 在线时长:193小时 | 升级还需:28小时级别:12 | 在线时长:193小时 | 升级还需:28小时级别:12 | 在线时长:193小时 | 升级还需:28小时  [zhaohumm 的头像](http://bbs.pediy.com/member.php?u=436274)  初级会员  初级会员  资　料:  注册日期: Jun 2011  帖子: [25](http://bbs.pediy.com/search.php?do=finduser&u=436274) zhaohumm 品行端正  精华: 0  现金: 24 Kx  致谢数: 1  获感谢文章数：0 获会员感谢数：0 | |  |  | | --- | --- | | **[9](http://bbs.pediy.com/showpost.php?p=1207633&postcount=9" \t "new)** 旧 2013-08-08, 15:03:55 默认 | zhaohumm 当前离线 |   励志哥呀 |
|  |
| http://bbs.pediy.com/images/pediy/statusicon/line.gif [[培训]"麦洛克菲"内核底层开发培训，看雪会员报名减免200元！](http://bbs.pediy.com/showthread.php?t=142155)  [回复时引用此帖](http://bbs.pediy.com/newreply.php?do=newreply&p=1207633) [返回顶端](http://bbs.pediy.com/showthread.php?t=176156#top) |

|  |  |  |  |
| --- | --- | --- | --- |
| [Acicada](http://bbs.pediy.com/member.php?u=328608)  级别:1 | 在线时长:10小时 | 升级还需:2小时  初级会员  初级会员  资　料:  注册日期: Mar 2010  帖子: [3](http://bbs.pediy.com/search.php?do=finduser&u=328608) Acicada 品行端正  精华: 0  现金: 33 Kx  致谢数: 0  获感谢文章数：0 获会员感谢数：0 | |  |  | | --- | --- | | **[10](http://bbs.pediy.com/showpost.php?p=1248694&postcount=10" \t "new)** 旧 2013-12-20, 16:28:29 默认 | Acicada 当前离线 |   分析的不错，顶一个。 |
|  |
| http://bbs.pediy.com/images/pediy/statusicon/line.gif [[培训]"麦洛克菲"内核底层开发培训，看雪会员报名减免200元！](http://bbs.pediy.com/showthread.php?t=142155)  [回复时引用此帖](http://bbs.pediy.com/newreply.php?do=newreply&p=1248694) [返回顶端](http://bbs.pediy.com/showthread.php?t=176156#top) |
| [永远的神话](http://bbs.pediy.com/member.php?u=613745)  级别:4 | 在线时长:33小时 | 升级还需:12小时  [永远的神话 的头像](http://bbs.pediy.com/member.php?u=613745)  初级会员  初级会员  资　料:  注册日期: Dec 2013  帖子: [86](http://bbs.pediy.com/search.php?do=finduser&u=613745) 永远的神话 品行端正  精华: 0  现金: 8 Kx  致谢数: 5  获感谢文章数：1 获会员感谢数：1 | |  |  | | --- | --- | | **[11](http://bbs.pediy.com/showpost.php?p=1248720&postcount=11" \t "new)** 旧 2013-12-20, 17:55:23 默认 | 永远的神话 当前离线 |   好多笑脸啊 |
|  |
| http://bbs.pediy.com/images/pediy/statusicon/line.gif [[公告]如果你觉得有人语言挑衅，请点每帖右上角的“举报”按钮！](http://bbs.pediy.com/showthread.php?t=71978)  [回复时引用此帖](http://bbs.pediy.com/newreply.php?do=newreply&p=1248720) [返回顶端](http://bbs.pediy.com/showthread.php?t=176156#top) |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| [hbcld](http://bbs.pediy.com/member.php?u=382062)  级别:6 | 在线时长:69小时 | 升级还需:8小时级别:6 | 在线时长:69小时 | 升级还需:8小时级别:6 | 在线时长:69小时 | 升级还需:8小时  [hbcld 的头像](http://bbs.pediy.com/member.php?u=382062)  初级会员  初级会员  资　料:  注册日期: Nov 2010  帖子: [184](http://bbs.pediy.com/search.php?do=finduser&u=382062) hbcld 品行端正  精华: 0  现金: 20 Kx  致谢数: 63  获感谢文章数：0 获会员感谢数：0 | | |  |  | | --- | --- | | **[12](http://bbs.pediy.com/showpost.php?p=1249135&postcount=12" \t "new)** 旧 2013-12-22, 21:57:37 默认 | hbcld 当前离线 |   如果是NTFS简介就好了 | |
|  | |
| http://bbs.pediy.com/images/pediy/statusicon/line.gif [[培训]"麦洛克菲"内核底层开发培训，看雪会员报名减免200元！](http://bbs.pediy.com/showthread.php?t=142155)  [回复时引用此帖](http://bbs.pediy.com/newreply.php?do=newreply&p=1249135) [返回顶端](http://bbs.pediy.com/showthread.php?t=176156#top) | |
| [发表新主题](http://bbs.pediy.com/newthread.php?do=newthread&f=4) [关闭主题](http://bbs.pediy.com/newreply.php?do=newreply&noquote=1&p=1249135) | |

|  |
| --- |
| 添加到书签 |
| * [提交主题到 Digg](http://digg.com/submit?phrase=2&url=http%3A%2F%2Fbbs.pediy.com%2Fshowthread.php%3Ft%3D176156&title=%E3%80%90%E5%8E%9F%E5%88%9B%E3%80%91FAT32%E7%AE%80%E4%BB%8B%EF%BC%88mbr%2Febr%2Fdpt%2Fbpb%2Ffat%2Ffdt%29) [Digg](http://digg.com/submit?phrase=2&url=http%3A%2F%2Fbbs.pediy.com%2Fshowthread.php%3Ft%3D176156&title=%E3%80%90%E5%8E%9F%E5%88%9B%E3%80%91FAT32%E7%AE%80%E4%BB%8B%EF%BC%88mbr%2Febr%2Fdpt%2Fbpb%2Ffat%2Ffdt%29) * [提交主题到 del.icio.us](http://del.icio.us/post?url=http%3A%2F%2Fbbs.pediy.com%2Fshowthread.php%3Ft%3D176156&title=%E3%80%90%E5%8E%9F%E5%88%9B%E3%80%91FAT32%E7%AE%80%E4%BB%8B%EF%BC%88mbr%2Febr%2Fdpt%2Fbpb%2Ffat%2Ffdt%29) [del.icio.us](http://del.icio.us/post?url=http%3A%2F%2Fbbs.pediy.com%2Fshowthread.php%3Ft%3D176156&title=%E3%80%90%E5%8E%9F%E5%88%9B%E3%80%91FAT32%E7%AE%80%E4%BB%8B%EF%BC%88mbr%2Febr%2Fdpt%2Fbpb%2Ffat%2Ffdt%29) * [提交主题到 StumbleUpon](http://www.stumbleupon.com/submit?url=http%3A%2F%2Fbbs.pediy.com%2Fshowthread.php%3Ft%3D176156&title=%E3%80%90%E5%8E%9F%E5%88%9B%E3%80%91FAT32%E7%AE%80%E4%BB%8B%EF%BC%88mbr%2Febr%2Fdpt%2Fbpb%2Ffat%2Ffdt%29) [StumbleUpon](http://www.stumbleupon.com/submit?url=http%3A%2F%2Fbbs.pediy.com%2Fshowthread.php%3Ft%3D176156&title=%E3%80%90%E5%8E%9F%E5%88%9B%E3%80%91FAT32%E7%AE%80%E4%BB%8B%EF%BC%88mbr%2Febr%2Fdpt%2Fbpb%2Ffat%2Ffdt%29) * [提交主题到 Google](http://www.google.com/bookmarks/mark?op=edit&output=popup&bkmk=http%3A%2F%2Fbbs.pediy.com%2Fshowthread.php%3Ft%3D176156&title=%E3%80%90%E5%8E%9F%E5%88%9B%E3%80%91FAT32%E7%AE%80%E4%BB%8B%EF%BC%88mbr%2Febr%2Fdpt%2Fbpb%2Ffat%2Ffdt%29) [Google](http://www.google.com/bookmarks/mark?op=edit&output=popup&bkmk=http%3A%2F%2Fbbs.pediy.com%2Fshowthread.php%3Ft%3D176156&title=%E3%80%90%E5%8E%9F%E5%88%9B%E3%80%91FAT32%E7%AE%80%E4%BB%8B%EF%BC%88mbr%2Febr%2Fdpt%2Fbpb%2Ffat%2Ffdt%29) * [提交主题到 百度搜藏](http://cang.baidu.com/do/add?it=%E3%80%90%E5%8E%9F%E5%88%9B%E3%80%91FAT32%E7%AE%80%E4%BB%8B%EF%BC%88mbr%2Febr%2Fdpt%2Fbpb%2Ffat%2Ffdt%29&iu=http%3A%2F%2Fbbs.pediy.com%2Fshowthread.php%3Ft%3D176156&dc=&fr=ien#nw=1) [百度搜藏](http://cang.baidu.com/do/add?it=%E3%80%90%E5%8E%9F%E5%88%9B%E3%80%91FAT32%E7%AE%80%E4%BB%8B%EF%BC%88mbr%2Febr%2Fdpt%2Fbpb%2Ffat%2Ffdt%29&iu=http%3A%2F%2Fbbs.pediy.com%2Fshowthread.php%3Ft%3D176156&dc=&fr=ien#nw=1) * [提交主题到 QQ 书签](http://shuqian.qq.com/post?from=3&title=%E3%80%90%E5%8E%9F%E5%88%9B%E3%80%91FAT32%E7%AE%80%E4%BB%8B%EF%BC%88mbr%2Febr%2Fdpt%2Fbpb%2Ffat%2Ffdt%29&uri=http%3A%2F%2Fbbs.pediy.com%2Fshowthread.php%3Ft%3D176156&jumpback=2&noui=1) [QQ 书签](http://shuqian.qq.com/post?from=3&title=%E3%80%90%E5%8E%9F%E5%88%9B%E3%80%91FAT32%E7%AE%80%E4%BB%8B%EF%BC%88mbr%2Febr%2Fdpt%2Fbpb%2Ffat%2Ffdt%29&uri=http%3A%2F%2Fbbs.pediy.com%2Fshowthread.php%3Ft%3D176156&jumpback=2&noui=1) * [提交主题到 雅虎收藏](http://myweb.cn.yahoo.com/popadd.html?url=http%3A%2F%2Fbbs.pediy.com%2Fshowthread.php%3Ft%3D176156&title=%E3%80%90%E5%8E%9F%E5%88%9B%E3%80%91FAT32%E7%AE%80%E4%BB%8B%EF%BC%88mbr%2Febr%2Fdpt%2Fbpb%2Ffat%2Ffdt%29) [雅虎收藏](http://myweb.cn.yahoo.com/popadd.html?url=http%3A%2F%2Fbbs.pediy.com%2Fshowthread.php%3Ft%3D176156&title=%E3%80%90%E5%8E%9F%E5%88%9B%E3%80%91FAT32%E7%AE%80%E4%BB%8B%EF%BC%88mbr%2Febr%2Fdpt%2Fbpb%2Ffat%2Ffdt%29) |

|  |  |
| --- | --- |
| Expired Thread | 该主题： **"【原创】FAT32简介（mbr/ebr/dpt/bpb/fat/fdt)"** 因在一定的时间里没有任何回复而自动关闭。 如果您还对该主题感兴趣或者想参与对此主题的讨论，请您重新发表一篇相关的新主题。 |

**«** [上一主题](http://bbs.pediy.com/showthread.php?t=176156&goto=nextoldest) | [下一主题](http://bbs.pediy.com/showthread.php?t=176156&goto=nextnewest) **»**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| | [http://bbs.pediy.com/images/pediy/buttons/collapse_thead.gif](http://bbs.pediy.com/showthread.php?t=176156#top)发帖规则 | | | --- | --- | | 您**不可以**发表主题  您**不可以**回复帖子  您**不可以**上传附件  您**不可以**编辑自己的帖子 | 论坛论坛**启用** [vB 代码](http://bbs.pediy.com/misc.php?do=bbcode)  论坛**启用** [表情图标](http://bbs.pediy.com/misc.php?do=showsmilies)  论坛**启用** [[IMG] 代码](http://bbs.pediy.com/misc.php?do=bbcode#imgcode)  [论坛规则](http://bbs.pediy.com/misc.php?do=bbcode#imgcode) | | |  | | --- | | 窗体顶端    窗体底端 | |

| **[http://bbs.pediy.com/images/pediy/buttons/collapse_tcat.gif](http://bbs.pediy.com/showthread.php?t=176156#top)相似的主题** | | | | |
| --- | --- | --- | --- | --- |
| 主题 | 主题作者 | 论坛 | 回复 | 最后发表 |
| [【原创】神奇的MBR](http://bbs.pediy.com/showthread.php?t=120613) | 独奏者 | 『软件调试逆向』 | 92 | 2013-09-23 12:43:00 |
| [关于硬盘MBR 和DPT](http://bbs.pediy.com/showthread.php?t=165392) | Ryanspears | 『求助问答』 | 21 | 2013-09-22 01:24:03 |
| [【原创】解析NTFS(一) MBR部分](http://bbs.pediy.com/showthread.php?t=112459) | microdebug | 『编程技术』 | 26 | 2012-03-29 14:21:36 |
| [【求助】如何计算FDT所在扇区？](http://bbs.pediy.com/showthread.php?t=82973) | subwin | 『经典问答』 | 3 | 2011-03-26 10:12:54 |

窗体顶端

所有时间均为**北京时间**, 现在的时间是 12:05:32.

|  |  |  |
| --- | --- | --- |
|  |  | [**联系我们**](http://bbs.pediy.com/sendmessage.php)**-**[**看雪学院**](http://www.pediy.com/)**-**[**文字模式**](http://bbs.pediy.com/archive/index.php)**-**[**返回顶端**](http://bbs.pediy.com/showthread.php?t=176156#top) |

  ©2000-2015 看雪学院([**PEdiy.com**](http://www.pediy.com/)) |[关于我们](http://www.pediy.com/team.htm) | [京ICP备10040895号-8](http://www.miitbeian.gov.cn/) | [知道创宇](http://www.knownsec.com/)提供带宽资源 | 微信公众帐号：[**i**kanxue](http://bbs.pediy.com/showpost.php?p=1193897&postcount=1)   手机客户端： [http://www.pediy.com/common/image/android.gif](http://bbs.pediy.com/showthread.php?t=162413)

窗体底端

窗体底端