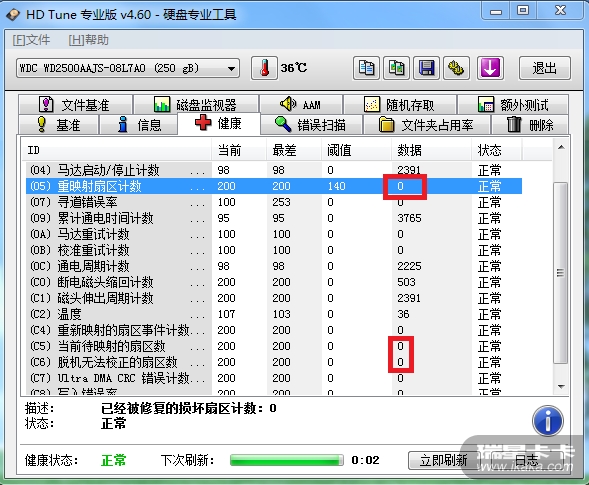
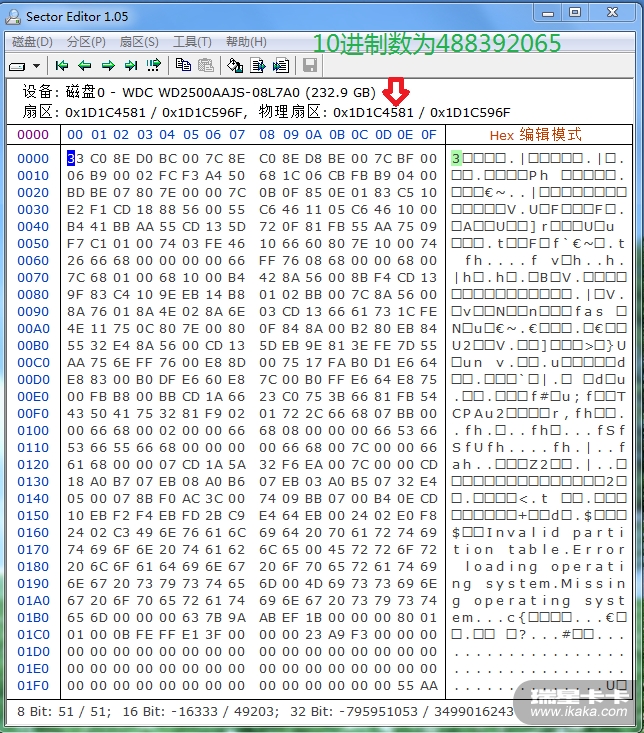
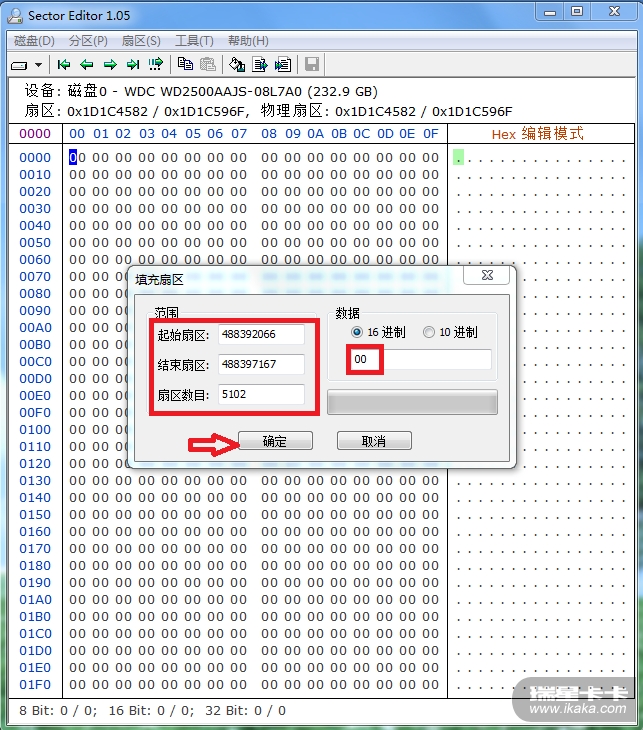
**手工杀毒时"备用扇区" 的处理问题**

这话从何说起呢？还是从TDSS TDL 类病毒的手工清理说起。用TDSSKILLER专杀工具杀毒者可以飘过。  
  
TDSS TDL类病毒，除了改写MBR，还在硬盘“备用扇区”（DISKGENIUS称之为“附加扇区”；位于硬盘末端）中的N个连续扇区写入了病毒代码。TDSSKILLER专杀工具是不管这部分内容的。其实TDSSKILLER这样处理是有道理的，原因如下：  
1、TDSSKILLER更正了MBR 后，备用扇区中的病毒代码就成了废物，不会对系统构成威胁。  
2、不同用户，其备用扇区的实际情况比较复杂。具体表现为：  
（1）不同硬盘的备用扇区数目不同。  
（2）不同用户的电脑，其备用扇区的实际使用情况不同。硬盘状态好者，可能一个备用扇区也没用（所有备用扇区中的内容均为“零”）；硬盘状态虽然不太好但还能凑合着维持运行者，其硬盘的“备用扇区”部分则可能存在一个或N个“重映射扇区”，这些“重映射扇区”中是有内容的，其中的具体内容就是S.M.A.R.T检测到的且已标记过的硬盘坏扇区中的内容。手工处理感染TDSS TDL病毒的硬盘时，可能会遇到这样的窘境：重映射扇区与病毒写入的备用扇区混杂在一起，无法区分哪些扇区该保留，那些扇区可以填“零”。  
  
自己动手，手工清理备用扇区，实际上是一种“洁癖”的强迫症状。一般用户完全可以无视这种操作。  
  
我在几个论坛上看到过几起谈论“清除TDSS TDL 写入备用扇区代码”的帖子，大多没谈具体的操作细节以及手工操作应该注意的问题。这样蛮干比较危险。故发此贴，与手工杀毒爱好者分享一下我自己清理硬盘“备用扇区”垃圾的思路与具体操作。  
  
个人感觉， 硬盘“备用扇区”这玩意儿有点儿像“跳出三界外不在五行中”的“怪物”。无论在WINDOWS环境，还是在PE环境中，你用DISKGENIUS之类的磁盘工具实施硬盘分区操作时，是不能处理硬盘“备用扇区”的。硬盘备用扇区位于硬盘尾部，不同的硬盘，备用扇区数目不同。这些备用扇区用作硬盘的“备胎”，当S.M.A.R.T检测到坏扇区时，它会标记这些坏扇区（以后不再访问之），并将其重新映射到“备用扇区”，以维持硬盘正常运行。  
了解了这些，清理备用扇区的思路基本就理清了。这里说的具体处理方法是“填零”法。此法仅仅适用于**硬盘“备用扇区”尚未使用**的情形。  
  
下面一一列出操作步骤（建议在PE环境下操作）：  
  
  
1、要用“填零法”清理备用扇区中的垃圾，自然要先确定“备用扇区“的位置及数目。  
  
这倒不难，用DISKGENIUS（此工具在WINDOWS和PE环境下均可使用）即可看到。下图中，红箭头标识的是硬盘扇区总数；绿箭头标识的就是 “备用扇区数”：  


注意：备用扇区数包含在扇区总数中。  
  
备用扇区范围的确定：  
（1）备用扇区的起始部：  
本例为硬盘扇区总数488397168减去备用扇区数5103=488392065  
  
因此，本例硬盘的第488392065扇区即为“备用扇区”的起始部。  
  
（2）备用扇区的尾部：  
  
当然是硬盘的最后一个扇区。本例为第488397168扇区。  
  
2、确认“备用扇区”可进行填零处理。具体操作是：用HD TUNE之类的工具查看“重映射扇区计数”。结果若如下图所示，才能考虑以“填零”这种简单的操作清理“备用扇区”。  


3、操作要慎之又慎！动手前，再看看硬盘备用扇区的头部是否真的是空的。下面这个图说明谨慎操作的必要。因为我用了Acronis True Image的MBR，所以NTx6类的MBR被移到了“备用扇区”的头部。填零操作应避开这个扇区，否则将导致严重后果（系统不能引导）。  
  


4、再怎么谨慎，也得动手啊！别急，下面马山就动手。填零法清除“备用扇区”中的垃圾，若用SECTOREDITOR，操作很简单。具体见下图。  
  


重启。检查系统及应用程序及数据分区的文件。一切正常。搞掂！