Win7的特殊隐藏分区一探究竟Microsoft认证考试 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/643/2021_2022_Win7_E7_9A_84_E7_89_B9_c100_643997.htm Windows 7的用户，在安装完成后运行diskmgmt.msc打开磁盘管理器，可以看到在系统分区(一般为C分区)之前有一个大小为200MB的隐藏分区。这个特殊的隐藏分区与Windows 7系统有什么关联呢?下面就让我们一探究竟。 1、分区状态 该分区的格式为NTFS，没有磁盘卷标也没有分配驱动器号，其磁盘状态描述为：系统、活动、主分区。因为没有驱动器号，所以在资源管理器中是不可见的。 2、该分区中都有什么呢? 为了一探究竟，笔者为其分配了一个驱动器号F。操作方法是：在磁盘管理器中选中该分区，右键单击选择“ 更改驱动器号和路径 ”弹出更改向导。单击“ 添加 ”按钮在弹出的对话框中点选“ 分配以下驱动器号 ”，然后点击其后的下拉列表从中选择F，最后“ 确定 ”退出即可。接下来打开“ 计算机 ”可看到一个新的磁盘分区F，进入该分区发现有两隐藏目录Boot和System Volume Information，另外还有两个隐藏文件bootmgr和BOOTSECT.BAK。毫无疑问，Windows 7在该隐藏分区中保存了系统的引导文件。 3、添加分区号后是否会影响系统启动呢? 接下来我们重启系统，看看上述操作(添加盘符)是否会影响到Windows 7的启动。测试结果系统正常启动，可见上述修改不会影响系统启动。这是非常好理解的，为启动分区重新分配盘符的操作并没有修改系统的引导文件，也没有修改磁盘引导扇区。可见，微软之所以将Windows 7的引导文件放在一个独立的隐藏分区中，一定是出于对引导文件的保护。

4、能否将分区返回到隐藏模式呢? 既然隐藏分区是为了保护系统引导文件，下面我们进行测试看是否可以取消刚才为其赋予的驱动器号。右键单击该分区选择“ 更改驱动器号和路径 ”，尝试“ 更改 ”或者“ 删除 ”驱动器号都显示“ 无法删除/更改卷的驱动器号 ”，其原因是改卷是系统或者启动卷。由此可见，为Windows 7中的这个特殊的隐藏分区添加驱动器号的过程是不可逆的。 5、删除分区中的文件是否影响系统启动呢? 下面我们尝试删除该分区中的系统引导文件会怎样。笔者以administrator登录系统，进入F分区然后进行文件删除。在删除的过程中发现，其中有些文件是无法删除的，显示“ 文件正在使用 ”或者提示“ 没有删除权限 ”。然后又尝试了为administrator赋予“ 完全控制权限 ”，结果被拒绝。经过测试发现就连system没有完全控制权限，只有TrusterInstaller用户才有完全控制权限。该用户是Windows 7中特有的，其任务是单一的与系统安装有关，在Windows 7的用户和组(lusrmgr.msc)中是没有该用户的。下面我们看看，在删除了该分区中的某些文件之后是否会影响系统启动。重启系统，没有问题系统正常启动。可见，我们刚才删除的文件与系统启动无关，而真正与系统启动相关的文件是无法删除的。 6、删除分区中是否影响系统启动呢? 通过磁盘管理器，笔者尝试“ 格式化 ”、“ 删除卷 ”均不能成功，可见Windows 7对该分区的保护是做得很不错的。既然系统工具不行，那试试第三方工具。笔者用Acronis Disk Director Suite 10.0进行测试，利用该工具删除了分区及其上面的数据，然后重启系统。显示“ BOOTMBR is missing ”即主引导扇区丢失，系统无法启动。由此可见，该隐藏分区中保存了系统的引导文件和磁盘的

主引导分区信息。 总结：通过上面的测试揭开了这个隐藏分区的神秘面纱，这个大小为200MB的隐藏分区对于Windows 7至关重要，它保存了系统引导文件和磁盘引导扇区的信息。如果它丢失或者被破坏对于Windows 7来说将是灾难性的。总的来说，将Windows 7的引导文件保存在一个隐藏分区中无疑加强了其安全性。但是，因为目标单一也容易成为攻击的对象。因此，建议大家不要为该隐藏分区分配驱动器号，这样就能够在较大程度上杜绝人为或者病毒木马对其造成破坏。