第一次作业

1. 简述MBR磁盘主分区表的结构。

主分区表占用64个字节, 4个分区表项，每项16个字节，因此最多可以有4个主分区。

分区表结构：

|  |  |  |
| --- | --- | --- |
| 字节偏移 | 字段长度  （字节） | 字段名和定义 |
| 0x00 | 1 | 分区状态 |
| 0x01 | 1 | 分区起始磁头号 |
| 0x02 | 2 | 分区起始扇区和柱面号 |
| 0x04 | 1 | 分区类型 |
| 0x05 | 1 | 分区结束磁头号 |
| 0x06 | 2 | 分区结束扇区和柱面号 |
| 0x08 | 4 | 在线性寻址方式下的分区相对扇区地址 |
| 0x0C | 4 | 分区大小（总扇区数） |

1. 简述MBR磁盘扩展分区的结构，并举例说明。

扩展分区可划分为一个基本分区和一个新的扩展分区，直至最后一个扩展分区，只包含一个基本分区。

扩展分区表项的第一个项包括数据的开始地址在内的与扩展分区中当前逻辑驱动器有关的信息；第二个项包含有关扩展分区中的下一个逻辑驱动器的信息，包括包含下一个逻辑驱动器的EBR的扇区的地址。如果不存在进一步的逻辑驱动器的话，该字段不会被使用。

举例：



1. 简述FAT32文件系统文件查找的过程。
2. 若为根目录下的文件：

根目录的第一个扇区（共512字节数据）开始，每次读取32字节的数据，前8字节为文件名，接着3个字节为扩展名，对于文件名和拓展名，若第一字节为0x00（表示空间未使用）或0xe5(文件已删除)则继续检查后面32字节的文件信息，如果在第一扇区没有找到目标文件，按上述步骤继续检查下一个扇区，直至遍历整个根目录下的所有扇区，如果依然未找到，说明文件不存在；如果找到文件，返回文件的首簇号；

1. 若为文件夹中的文件：

如果文件夹在根目录下：首先，用(1)中方法在根目录中找到文件夹的首簇，进入文件夹的首簇，其内容为子目录，与根目录相似，同样用(1)中方法在子目录中查找文件；如果目标文件在多级目录下，方法类似。

1. 简述FAT32文件系统文件恢复的基本思想。

FAT32文件系统文件删除原理：将FDT中该文件的目录项首字节更改为E5，FAT表中该文件对应簇号的登记项内的表项值全部更改为0，对应数据区变为可写状态；

文件恢复：在根目录中寻找该文件的文件名，根据文件名所在的目录项找到文件对应首簇号及大小，根据首簇号找到文件内容在硬盘中的起始地址，根据大小确定文件内容在硬盘中的结束位置，拷贝数据内容；

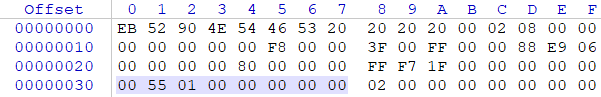
1. 简述NTFS文件系统文件查找的过程。

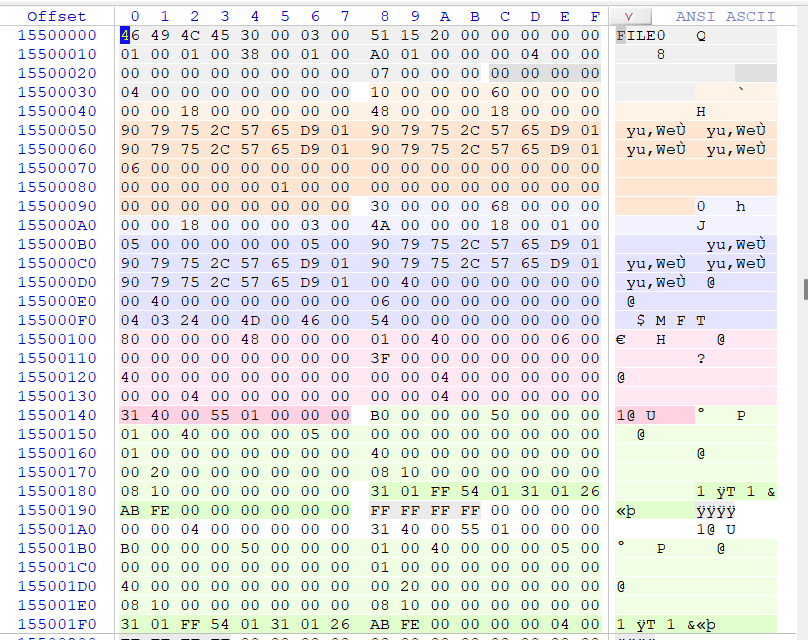
举例说明：



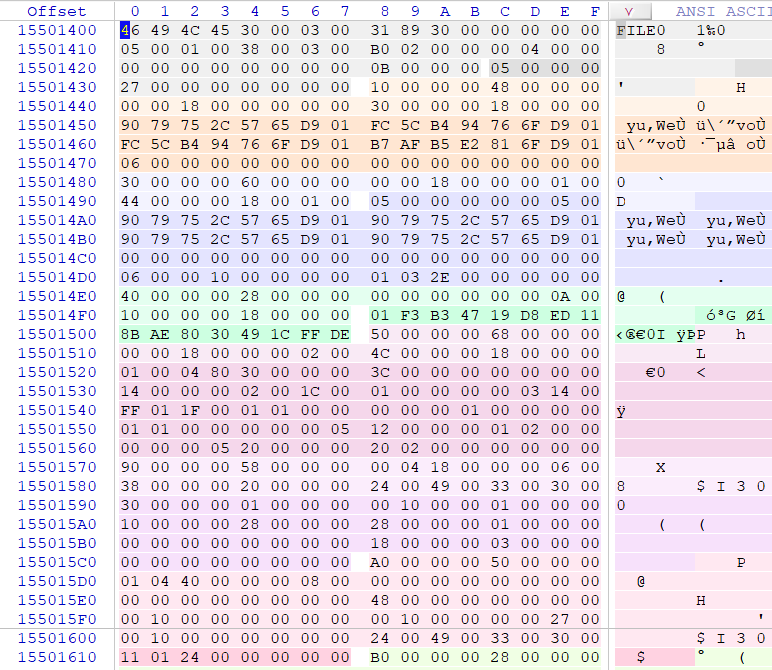


1. 在30H处查找到MFT 首簇号并跳转；

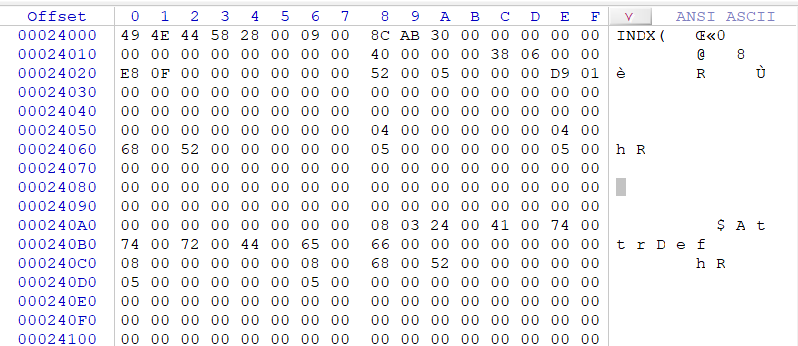




1. 由于每一项文件记录占两个扇区，根目录在第六项，则根目录位置为MFT的起始偏移+2\*5个sector；

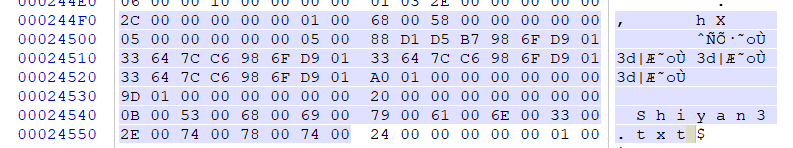


3、查看文件记录的90属性和A0属性，如果90属性没有目录项就看A0属性里的Run list，找到索引缓冲区的起始簇号,图中为0x(24\*8)个sector处;

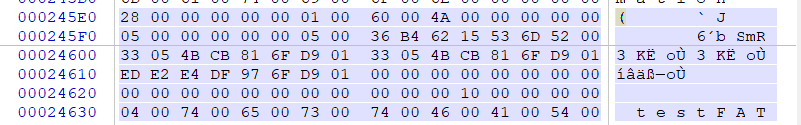


4、根据文件名或文件夹名找到索引项，以索引项的MFT文件参考号低六位作为MFT编号；计算出目标文件或文件夹的文件记录的偏移：MFT的起始偏移+MFT编号\*2个sector；

文件：MFT编号为0x2B

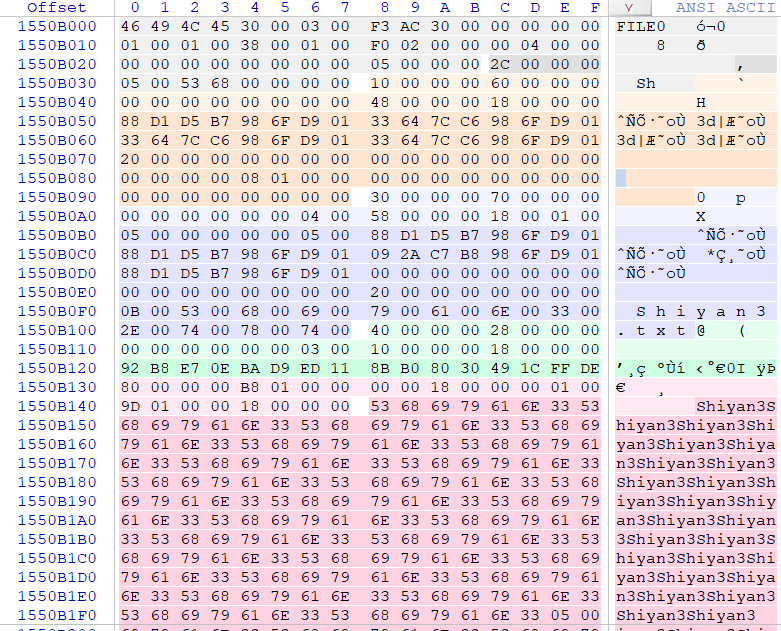


文件夹：MFT编号为0x28

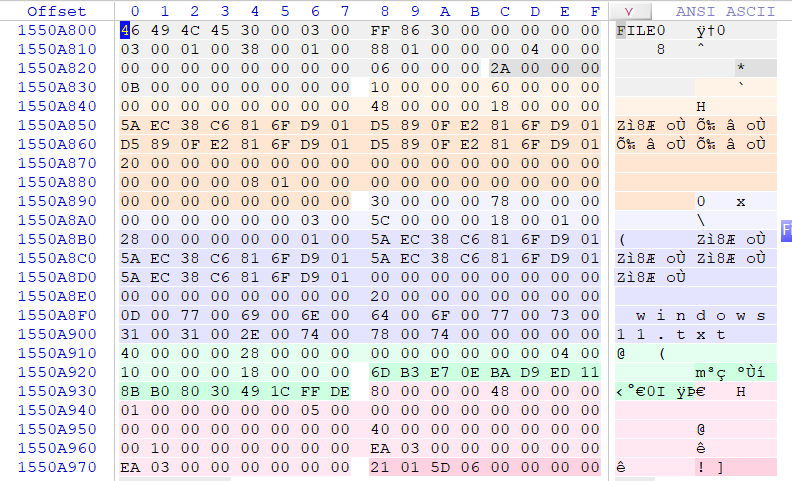


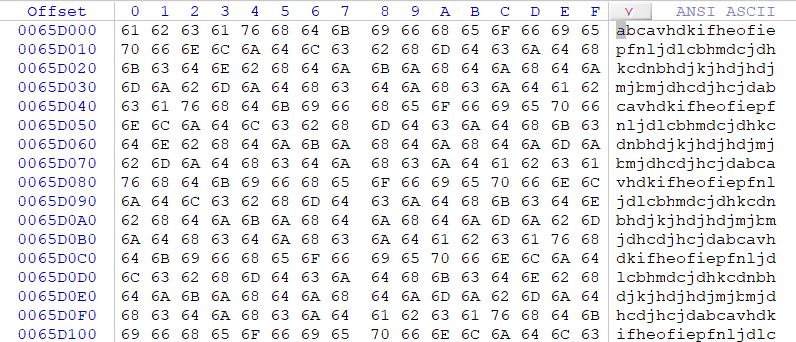
5、（1）若为文件，查看80属性，若为常驻属性，文件内容直接显示在80中；





若为非常驻属性，查看80属性里的Data run ,跳转到文件起始首簇号；





（2）若为文件夹，重复3、4、5的步骤；

