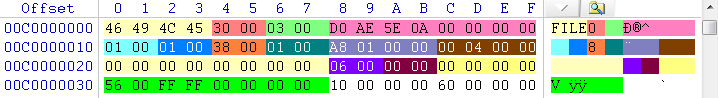
$MSF文件头基本上就是以下这些参数了

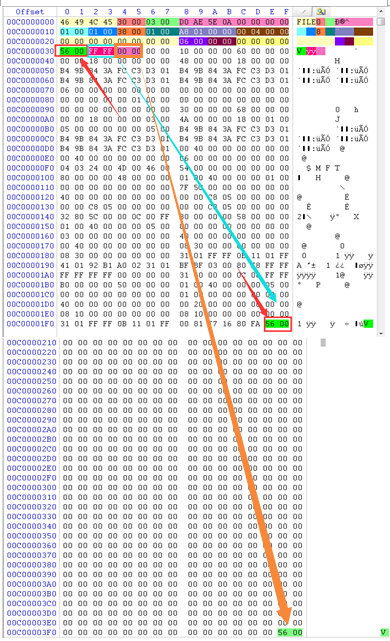


|  |  |  |
| --- | --- | --- |
| 偏移 | 长度（字节） | 含义 |
| **☆00-03H** | **4** | **FILE，文件记录的标志** |
| 04-05H | 2 | 更新的序列号的偏移 |
| 06-07H | 2 | 更新序列号的大小与数组 |
| 08-0FH | 8 | 日志文 件的序列号（每次修改文件都会改变这个位置的参数） |
| 10-11H | 2 | 序列号 |
| 12-13H | 2 | 连接数，有多少个目录指向该文件 |
| **☆14-15H** | **2** | **第一个属性的起始位置**  **2003、xp为38 2000及NT，为30** |
| **☆16-17H** | **2** | **标志（flags）00，表示文件已经删除，01表示正在使用，02表示这个文件记录为文件夹** |
| 18-1BH | 4 | 记录头和属性的总长度，也就是文件记录的总长度 |
| 1C-1FH | 4 | 分配给记录的长度（一般都为1024也就是两扇区） |
| 20-27H | 8 | 基本文件记录的文件索引号 |
| 28-29H | 2 | 下一个属性的ID |
| 2A-2B | 2 | 边界 |
| 2C-2F | 4 | MFT 记录编号（起始编辑为0）Windows XP中使用 |
| **☆2A-2B** | **2** | **2A-2B 是2000 为边界 30-31 在XP 2003下是边界** |
| **☆\* 2C-2F** | **4** | **文件记录编号** |
| 30-37 | 8 | 更新序列号数组 |
| 38-3FF | 456 | 属性和修下正值 |

下面讲一下最重要的几个参数

其文件头最重要的就是这两个参数，以为更新序列号占用了一项文件目录项的4个字节，所以原先要写入更新序列号位置(注：扇区最后一行的最后两个数值为更新序列号，它与文件属性头中偏移0x30的数值是一样的。)的数值就被搬运到文件属性头中的偏移0x32的位置，一共4字节，前两位字节表示第一个扇区被更新序列号占用的字节，后两个字节表示第二个扇区被更新序列号占用的字节。

↓光说不如上图来着实惠



第二个重要的参数就是标识Flag

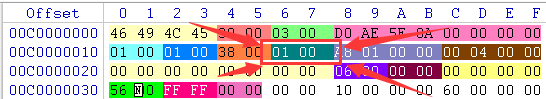
它一共有4种情况，常见的有

0x00文件被删除

0x01文件正在使用

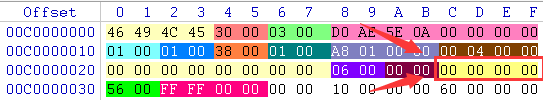
0x02文件目录被删除

0x03目录正在使用

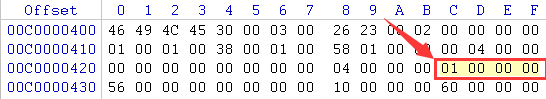


第三个重要的参数就是文件记录编号

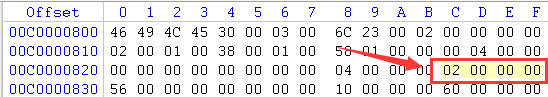
它就是表示文件记录的编号，从0开始第一个文件记录项为0，第二个文件记录项为1用这个值可以判断文件记录项的顺序



↑第一个文件记录项↑



↑第二个文件记录项↑



↑第三个文件记录项↑

第四个重要的参数就是第文件属性体开始位置

这里的这个参数表示了第一个文件属性的位置，也算的上是文件属性头的结束位置，我们在图中看出，橙色参数0x3800我们再看看偏移0x38的位置，正好是一个10属性的属性头，也就是文件属性头的结束位置，文件属性体的开始位置了

