NTFS:

DBR及其保留扇区(EB 52 90) | MFT及前四个元文件备份 | Bitmap(FFFF) | 子目录(INDX) | 数据区 |

| MFT(通常在6291456) | 数据区 | LogFile | 数据区 | 备份DBR(EB 52 90)

重建NTFS DBR分区:

方法1:跳转到分区结尾，将备份复制回去

方法2:找一个好的NTFS DBR，复制回去，然后修改以下几个数据:

0D:每簇扇区数

1C-1F:当前DBR位置所在

28-2B:分区总大小

30-33:MFT所在簇号

提取文件：

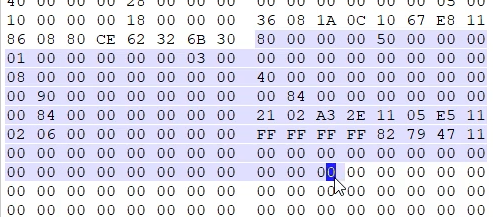
从DBR位置向下跳转6291524到达TXF处，向下找到文件记录

DATARUN位置，如果是21，则提取第3-4位置的数据;如果是31，则3-5

复制文件大小后，将文件簇号×簇大小得到文件所在位置，从DBR跳转

复制文件头尾

多段数据流文件提取:



以这个文件为例，目前看到FF前面有多段数据流

第一段:21 02 A3 2E

21中的1对应第二个字节的02，即长度

2对应着后面的A3 2E

第二段11 05 E5

第三段11 02 06

都是一样的

第一段数据流跳转到文件位置的方法和正常相同

第二段是建立在第一段数据流的基础之上

即提取第二段需要拿第一段的簇号+第二段簇号。

如果第二段簇号出现负数，依旧是相加，只不过加的是负数。

第三段同理。

跳分区:

从DBR位置向下跳转6291468来到Bitmap位置，复制DATARUN的数值，然后用该数值×8×簇大小

从分区起始位置向下跳转所的数值即可到达下一个分区的起始

Logfile 日志文件分析:

头:52 53 54 52 1E ( RSTR )

和正常提取文件方法相同，向下搜文件名，找到带有80属性的记录

其他方法均相同