

操作系统课程设计

****

**题 目**

学生姓名

学 号

学 院 计算机学院、网络空间安全学院

专 业

指导教师 闫雷鸣

**二Ｏ四零年十二月**

**DiskGenius 数据恢复**

目录

[题 目 1](#_Toc25005)

[一、 U盘的格式化与文件系统选择 4](#_Toc12447)

[1. 1 U盘的格式化 4](#_Toc20538)

[二、 读取和修改U盘主引导扇区 4](#_Toc9798)

[2.1读取主引导扇区（MBR） 4](#_Toc14072)

[2.2创建文件并观察记录变化 6](#_Toc30734)

[2.3计算文件在磁盘中的地址 7](#_Toc6204)

[2.3.1获取文件的起始簇号 8](#_Toc5776)

[2.3.2计算文件数据的物理地址 8](#_Toc9065)

[2.4计算文件在磁盘中的地址 9](#_Toc14353)

# U盘的格式化与文件系统选择

## 1 U盘的格式化

首先，选择一个空U盘，进行格式化并选择不同的文件系统格式，包括NTFS、FAT32和EXT4。由于Windows本身不支持EXT4格式，此处在Windows下使用FAT32。插入U盘，打开我的电脑右键点击U盘，选择“格式化”，如图1所示。

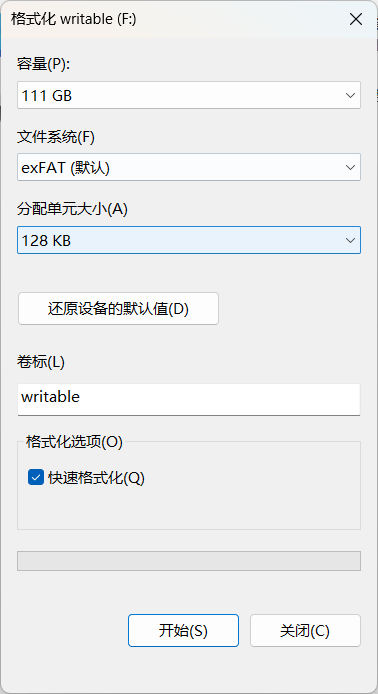
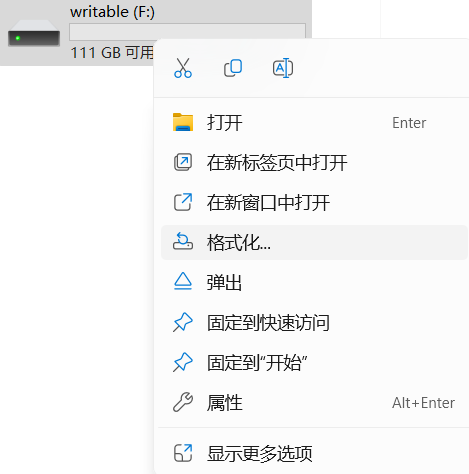


图 1 图 2

如图2所示，此处选择FAT32格式，适合较小的存储设备。U盘常用此格式，兼容性好，但单文件大小限制为4GB，格式化后，U盘变为一个空的存储设备。

# 读取和修改U盘主引导扇区

## 2.1读取主引导扇区（MBR）

主引导扇区（MBR） 位于磁盘的第一个扇区，也就是磁盘的物理偏移量为 0 的地方。MBR 是磁盘的第一个 512 字节（包括 446 字节的启动程序、64 字节的分区表和 2 字节的魔术数）部分。

使用DiskGenius工具读取U盘的主引导扇区。

1.打开DiskGenius，选择U盘所在的磁盘。

2.右键点击U盘，选择“打开磁盘”查看磁盘结构。

3.找到U盘的主引导扇区（MBR），主引导扇区（MBR）位于磁盘的第一个扇区，偏移量为 0x0000，也就是磁盘的第一个 512 字节区域，并查看其中的分区表和引导代码。

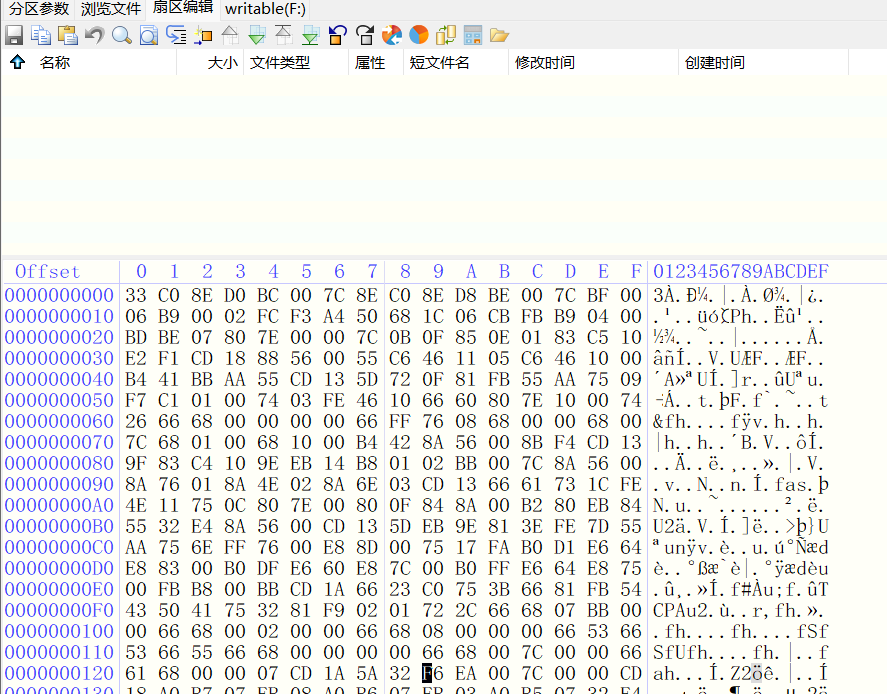


图 3 MBR记录

如图3所示，能够观察到在不同偏移位置上的存储数据。其中Offset 指的是扇区在磁盘上的位置。它是从磁盘的开始位置（即主引导扇区，MBR）到当前扇区的偏移量，以十六进制表示。数据以 16 个字节为一行，并且每行会显示从 0 到 F 的十六进制数据。

右边的字符串部分显示的是当前扇区内容的ASCII 字符表示，只显示那些能转化为可打印字符的字节。如果一个字节对应的 ASCII 字符无法打印，则会显示为 .（点），表示该字节不能直接转换为字符。分析16进制下的内容能够得知MBR记录的位置。

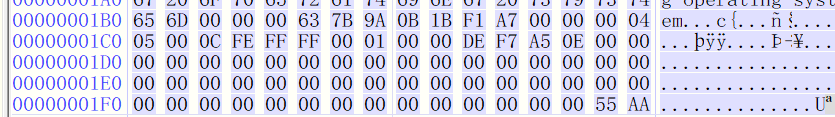


图 4 MBR分区标志

55 AA 是典型的 MBR（主引导记录） 引导扇区的标志，表示扇区的开始。MBR 中通常会包含引导程序和分区表等信息。在这里，55 AA 是扇区标记，指示着扇区的有效性。这通常表示这段数据是引导扇区的一部分，而不是未格式化的数据。在MBR中包含了以下两种结构：

分区表（Partition Table）：

分区表通常会出现在 MBR 中。它包含了磁盘的分区信息，如分区类型、起始和结束位置等。

引导代码（Boot Code）：

负责启动操作系统。在这段数据中能找到一些与引导过程相关的机器代码。

另外，有一部分16进制码能以ASCII码形式翻译成如下信息。

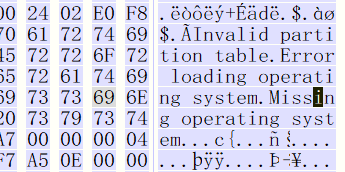


图 5 MBR中能够被翻译的部分

这是以 ASCII 可打印字符的形式显示出来的内容，翻译后为：

"validation partition tableError loading operating systemMissioning operating system"

这里似乎包含了一些文本信息。可以看到有一部分是 错误信息，表示可能在该区域保存了一些操作系统或分区信息。

## 2.2创建文件并观察记录变化

在U盘中创建一个新文件empty.txt如下图所示：



图 6 空文件创建

查看当前的分区信息如下：

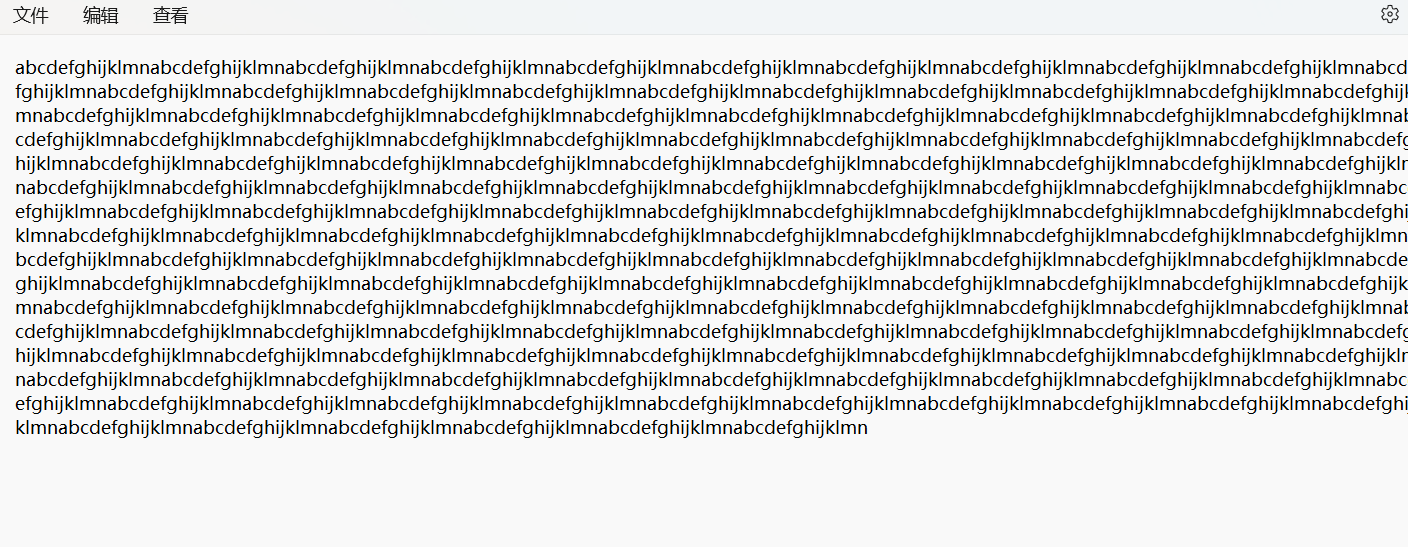


图 7 分区情况

由上图得知在 FAT32 文件系统中，数据是以 簇（Cluster） 为单位存储的，每个簇由若干个扇区组成（通常为1到64个扇区，具体取决于文件系统的配置）。图中每个簇是 64 KB，即一个簇包含 128个扇区（512字节/扇区）。

此处已用簇数变为1 个簇，说明现在U盘上已经创建了一个小文件（文件可能没有内容，但FAT32仍为其分配一个完整的簇）。新文件会占用一个簇，并在FAT表中标记为已使用，簇号会记录在FAT表中。

再次新建一个文件，观察后续的变化。新建一个文件名为file.txt，并在其中输入内容。



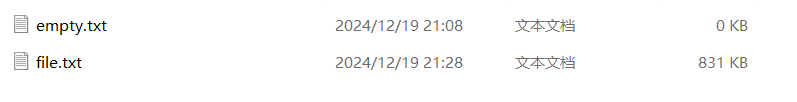


图 8 新建有内容文件

这里连续复制多次使文件大小达到100kb以上，观察变化。

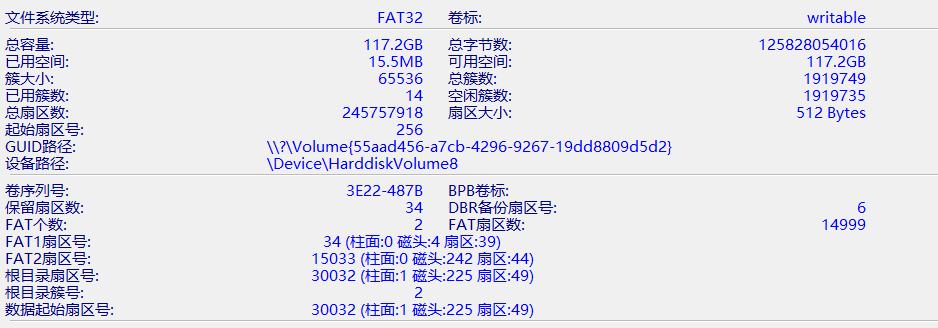


图 9 再次新建文件后的分区信息

能够发现已用簇数从1变为了14。这是由于新建文件的大小超过了一个簇的大小65536 (换算后为64KB）因此其占据了不止一个簇。此处文件大小为831KB ，大约占用了 13 个簇，文件的起始簇号在 FAT 表 中记录，并且通过簇链来链接所有的簇。

## 2.3计算文件在磁盘中的地址

在 FAT32 文件系统中，通常涉及以下几个步骤：

1.获取文件的起始簇号。

2.计算文件数据的物理地址，也就是文件数据在磁盘上的实际扇区地址。

3.追踪簇链，直到文件占用的所有簇都被遍历完。

### 2.3.1获取文件的起始簇号

在 FAT32 文件系统中，文件的起始簇号保存在文件的 目录表项 中。通过 DiskGenius 或其他工具，查看文件的 起始簇号。



图 10 起始簇号及扇区查看

此处能够看到在改文件系统中，起始簇号为2。起始扇区为30032。

### 2.3.2计算文件数据的物理地址

FAT32 文件系统中的每个簇占据一定数量的扇区，通常是 1 个簇 = 1 个或多个扇区（通常每个簇的大小为 16KB、32KB 或更大，具体大小取决于磁盘格式）。每个簇有一个对应的物理地址，它指向磁盘上的一块实际区域。

根据之前截图可知：簇的大小是 65536 字节（即 64KB），每个扇区的大小是 512 字节。这样每个簇包含 128 个扇区（65536 / 512 = 128）。

公式：

簇的起始扇区地址 = 起始扇区号 + (簇号 - 2) \* (簇大小 / 扇区大小)

簇号为 2，文件的实际物理扇区地址就是 256，因此它占据了磁盘的第 256 个扇区开始，接着每个簇会占据 128 个扇区。此处起始扇区为起始扇区为30032。由于之前先创建了一个 0 KB 文件，文件系统会分配一个簇占用 64 KB 的空间，但是没有实际数据。它占用簇 2。因此后面创建的文件的起始簇号应该为3。因此，使用上述公式计算，实际有文件的物理起始扇区为 30160，结束扇区为 31822。在Diskgenius中查找扇区检验是否正确。



图 11 输入地址查询

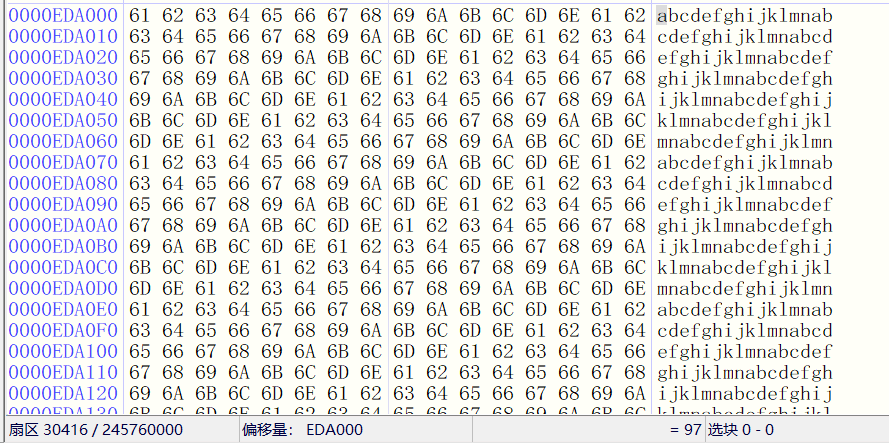


图 12 起始位置扇区查询

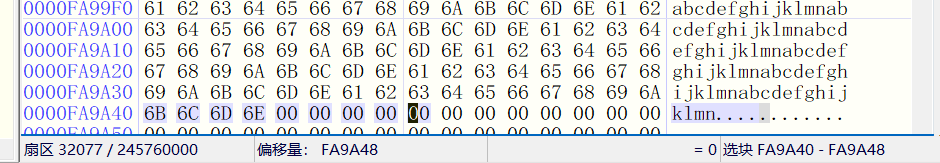


图 13 终止位置扇区查询

起始扇区能够看到abcd...，终止扇区能够看到klmn....。因此能够看到成功地计算了文件的地址信息。

## 2.4删除后尝试恢复文件

操作系统中删除文件时，文件并不会立即从磁盘中物理删除，而是操作系统会将该文件的目录项标记为“已删除”，并且标记相应的簇为可用。只要这些簇没有被其他数据覆盖，理论上是可以恢复文件的。

删除该文件时，操作系统会在 FAT 表中标记文件所占用的簇为“可用”。删除文件的目录项（包括文件名和起始簇号），但是数据并未被清除。

将上述831KB的测试文件删除

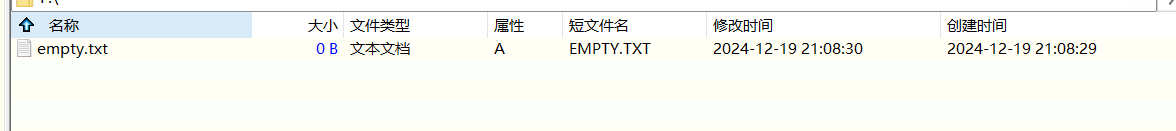


图 14 删除后的文件目录



图 15 删除后已用簇数

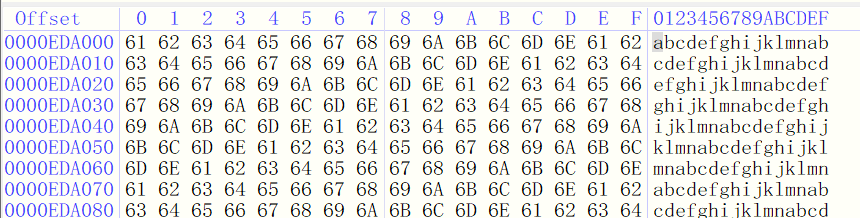
可见该文件的目录项会从根目录（或者相关目录）中移除，已用簇数 会减少，而 空闲簇数 会增加。文件已被删除。但实际上查看刚刚计算出的物理地址并进行跳转查询，能够看到物理上数据并未被删除。

图 16 删除后扇区位置的数据

因此只要这些簇没有被其他数据覆盖，理论上是可以恢复文件的。

此处可以使用使用 DiskGenius 或其他数据恢复工具(或者直接手动修改分区表）

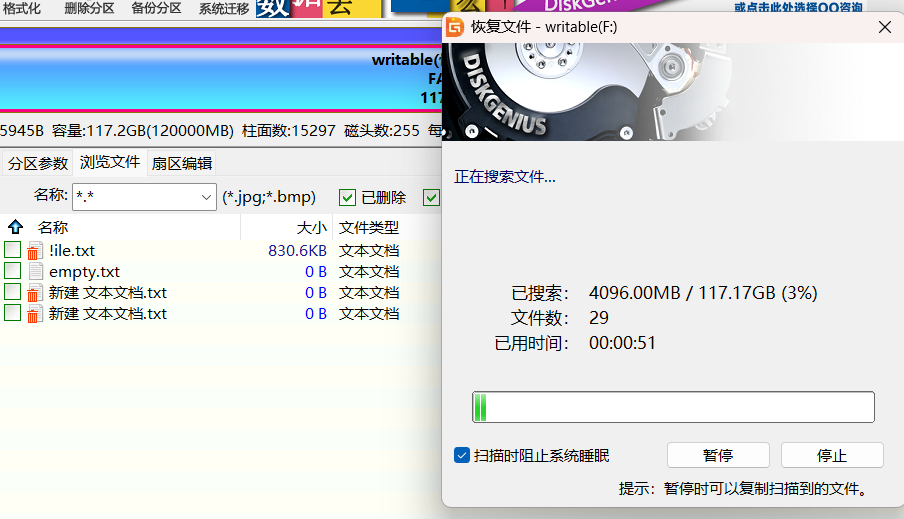


图 17 文件恢复

1.启动 DiskGenius 并选择对应的 U 盘。

2.扫描已删除的文件：使用 DiskGenius 的恢复工具，选择对 U 盘进行深度扫描。扫描文件簇链，并标识出已删除但未被覆盖的数据块。

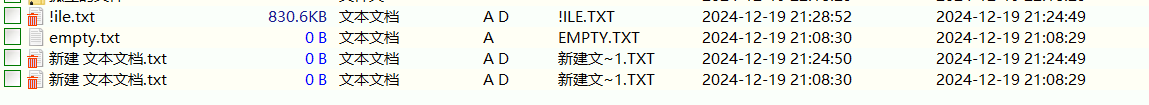


图 18扫描出的可恢复文件

在扫描结果中，DiskGenius 列出已删除的文件和簇。通过查看文件大小、修改时间等信息来确定是否是删除的文件。

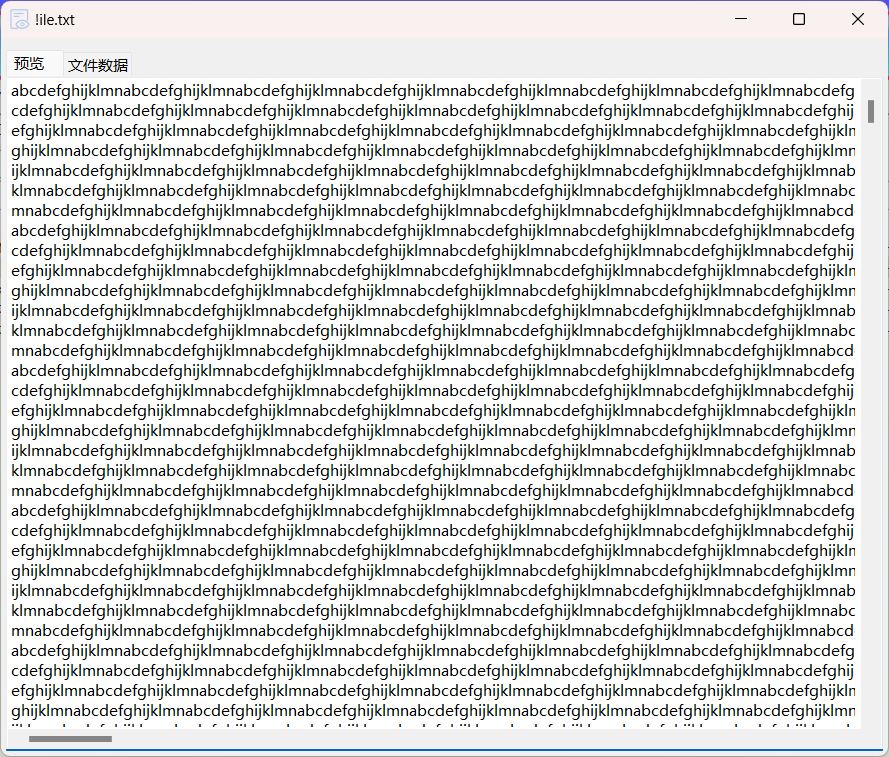


图 19 恢复后的文件

查看恢复后的831KB的测试文件，能够看到文件内容完好无损，但文件名有些许损坏，file变成了！ile，可能是其他内容进行了覆盖，但无伤大雅。

# U盘的格式化与文件系统选择