基于 FAT32 文件系统的数据隐写实验

原创

渔网探索者 于 2020-06-12 09:45:26 发布

1 实验目的

本实验的目的是深入理解 FAT32 文件系统管理文件的方式，验证通过修改文件系统的 保留扇区、

FAT 分区表等关键结构，能够实现将数据隐写在分区，并且不会被新写入文件 覆盖、不易被用户发现等功能。

2 实验内容及环境

1. 实验内容

本实验要求通过修改采用 FAT32 文件系统的分区结构，实现将数据隐写在分区中的空

闲扇区，并且该隐写数据不会被新拷入文件覆盖。

2. 实验环境

(1) Win 10操作系统，以及实验

用的 WinHex 工具；

(2) Kinsgton 8G 优盘：该优盘采用 FAT32 文件系统；

3. 实验工具

WinHex 中文版：WinHex 是一款以通用的 16 进制编辑器为核心，专门

用来对付计算机取证、数据恢复、低级数据处理、以及 IT 安全性、各种日常紧急情况的

高级工具：用来检查和修复各种文件、恢复删除文件、硬盘损坏、数码相机卡损坏造成的

数据丢失等。

3 实验步骤

本实验的思路是从优盘 FAT 表项中找一个未分配的簇，将其标志为“占用”或“坏

簇”，然后在该簇内写入数据。为了保证数据的隐藏性，不修改优盘的目录结构。

具体修改位置包括：

(1) 引导扇区中的“空闲簇总数”和“下一个可用簇”；

(2) FAT1 表和 FAT2 表中找到“标识为 0” （4 字节）的簇，将其改为标志为“占

用”或“坏簇”，并计算其簇号；

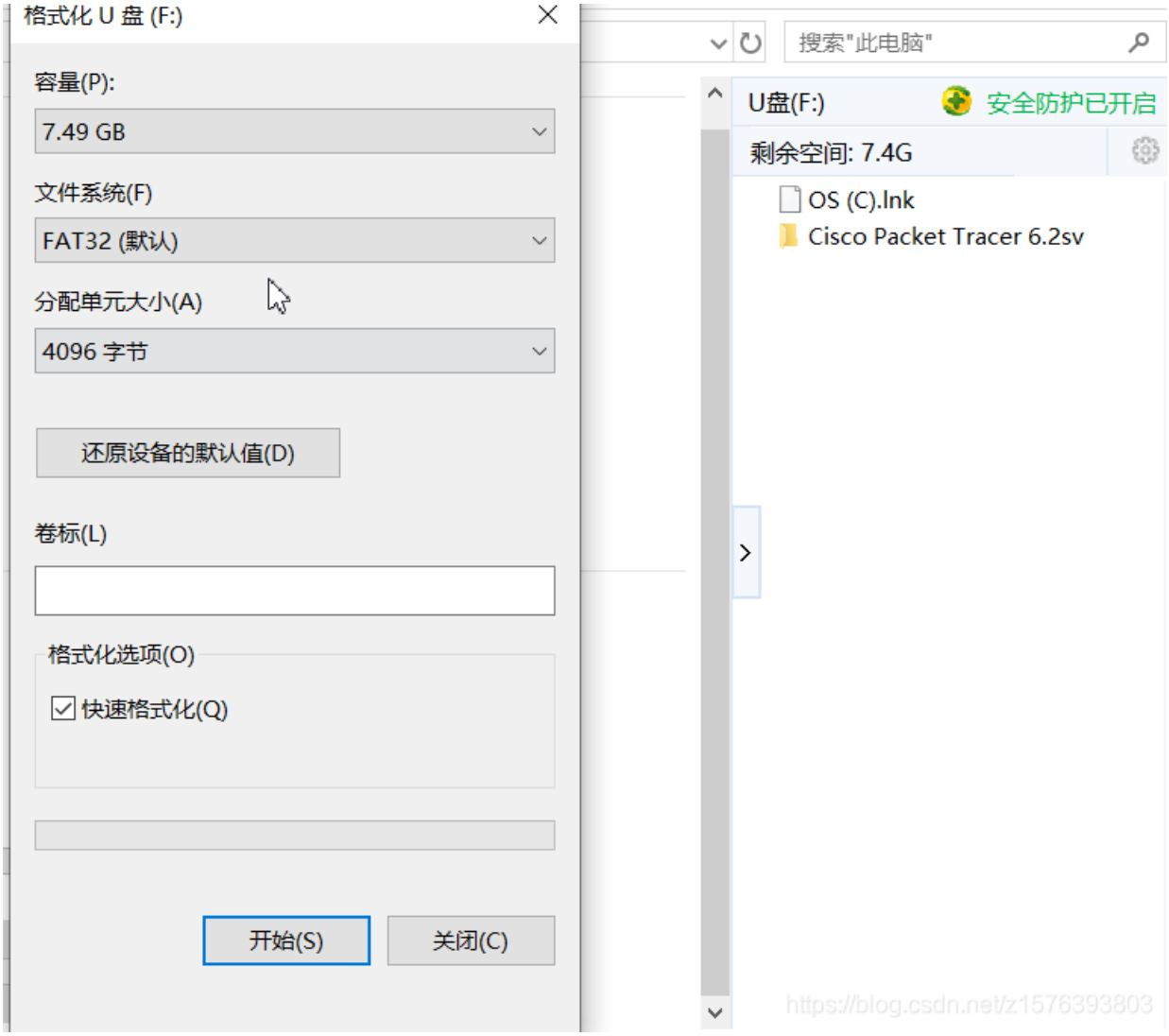
(3) 根据其簇号，找到其所在数据区部分，并对该簇内若干字节进行数据的填写；

1. 初始化优盘

将优盘插入主机的 USB 接口，待主机识别后，双击“我的电脑”，找到优盘所在分

区，右键点击，选择“格式化”如图所示。

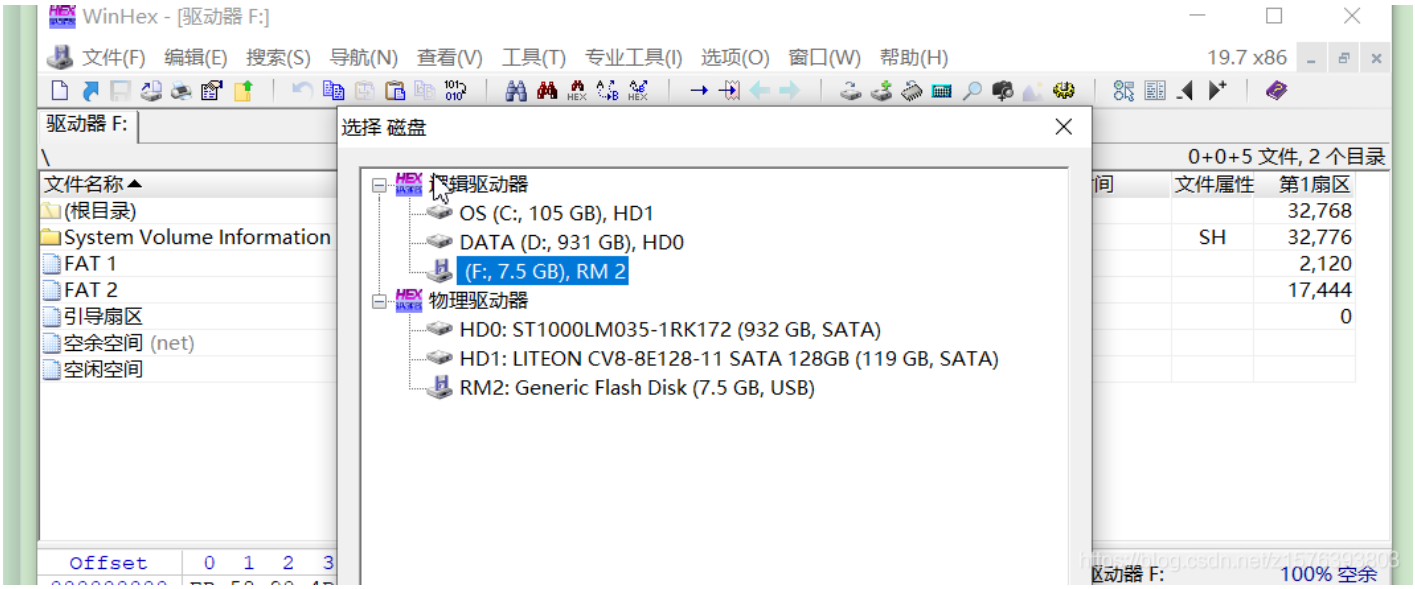
格式化磁盘



2. 利用 WinHex 打开优盘

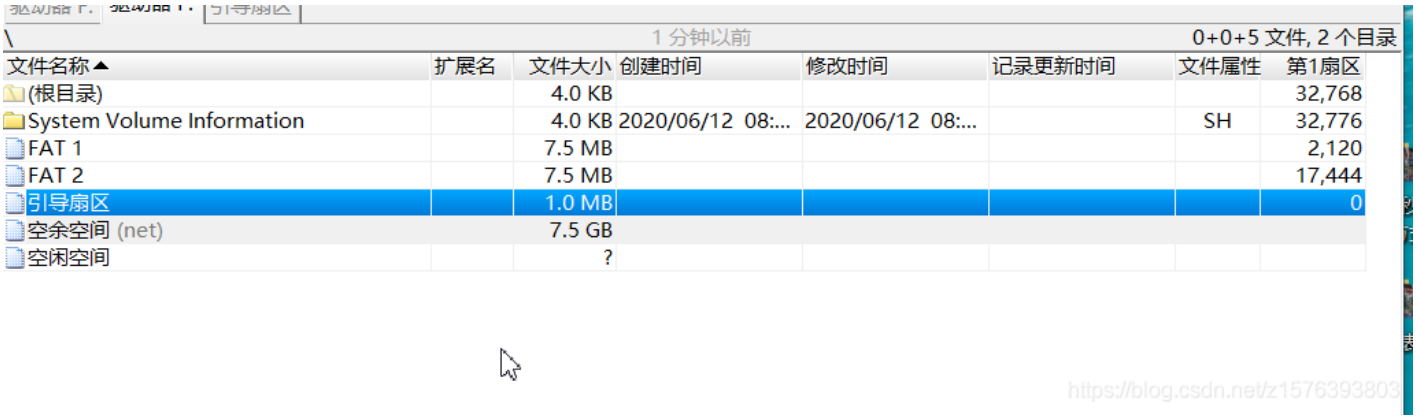
双击 WinHex.exe，进入操作界面。点击菜单→“工具”→“打开磁盘”，选择优盘所在 分区

如图所示。 Winhex 选择目标磁盘, 打开优盘

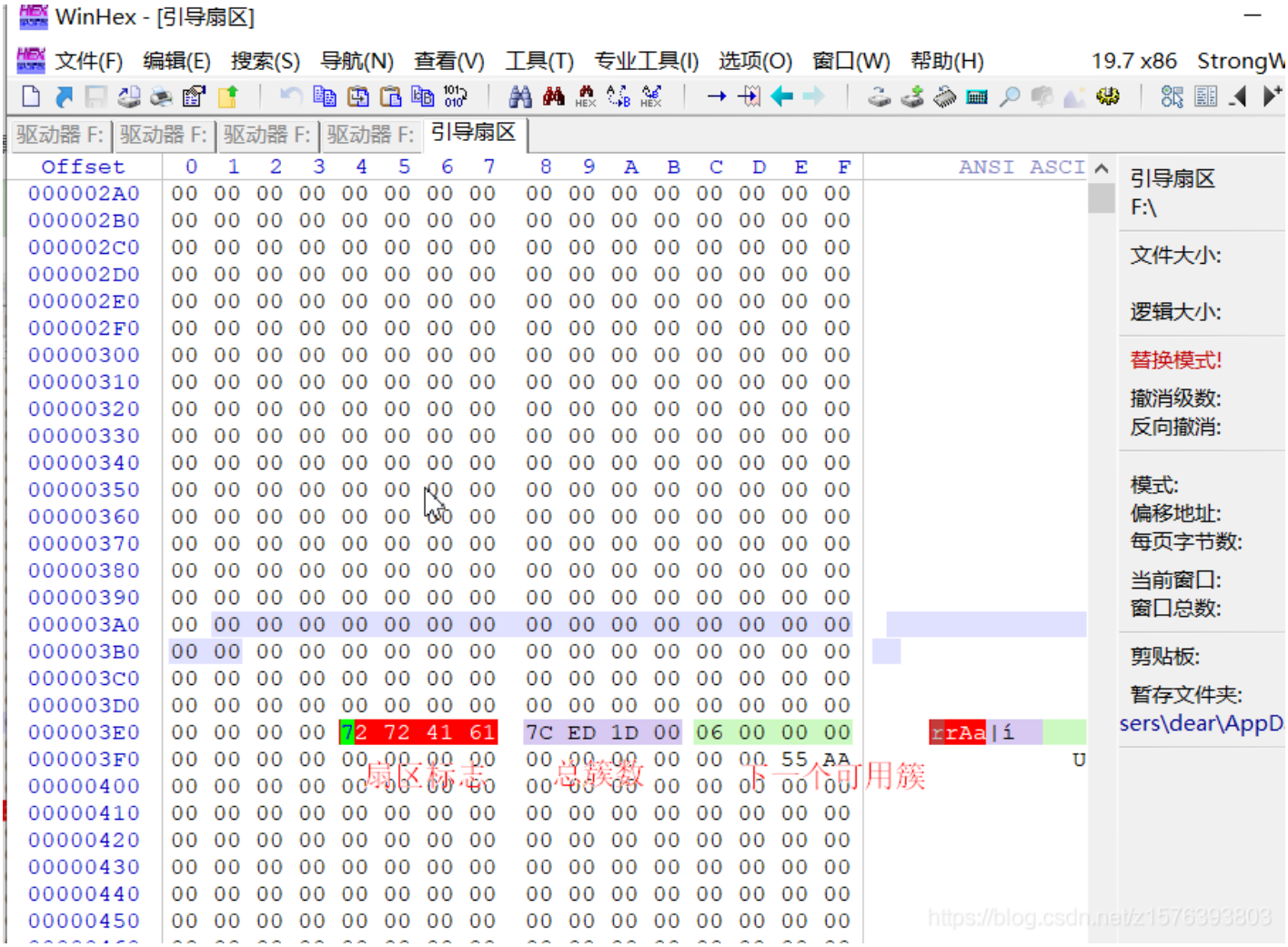


3.修改 FSINFO 保留扇区

1.为了找到可以写入数据的空闲空间，打开右击打开引导扇区



在引导扇区往下面找到 4 个字节 “72 72 41 61”（扇区标志）来判断定位的 FSINFO 扇区是否正确。

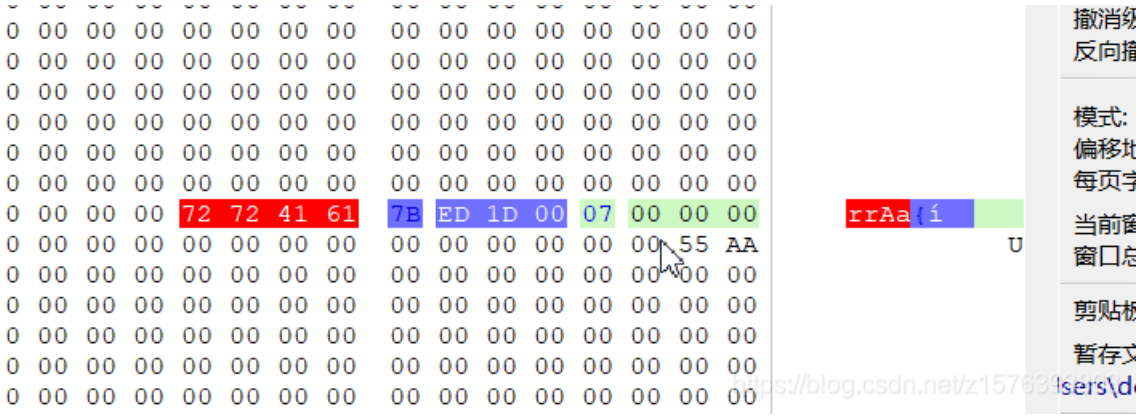


根据 FAT32 文件系统结构，该扇区后连续的 4 个字节即为当前分区所有的可用簇总数，得值为“7C ED 1D 00”，由于需要将数据写入一个空闲簇，因此将其值减 1，得到“7B ED 1D 00”；同理，

总簇数值后连续 4 个字节为当前分区内“下一个可用簇”的字段，值为“06 00 00

00”。注意该簇 0x0006 (从后往前数)即为我们要写入数据的空闲簇。

如图 修改 FSINFO 扇区



通过 FAT 表找到连续 4 个全零字节所在簇，我们这里找到的是 0x0006，将“下一个可

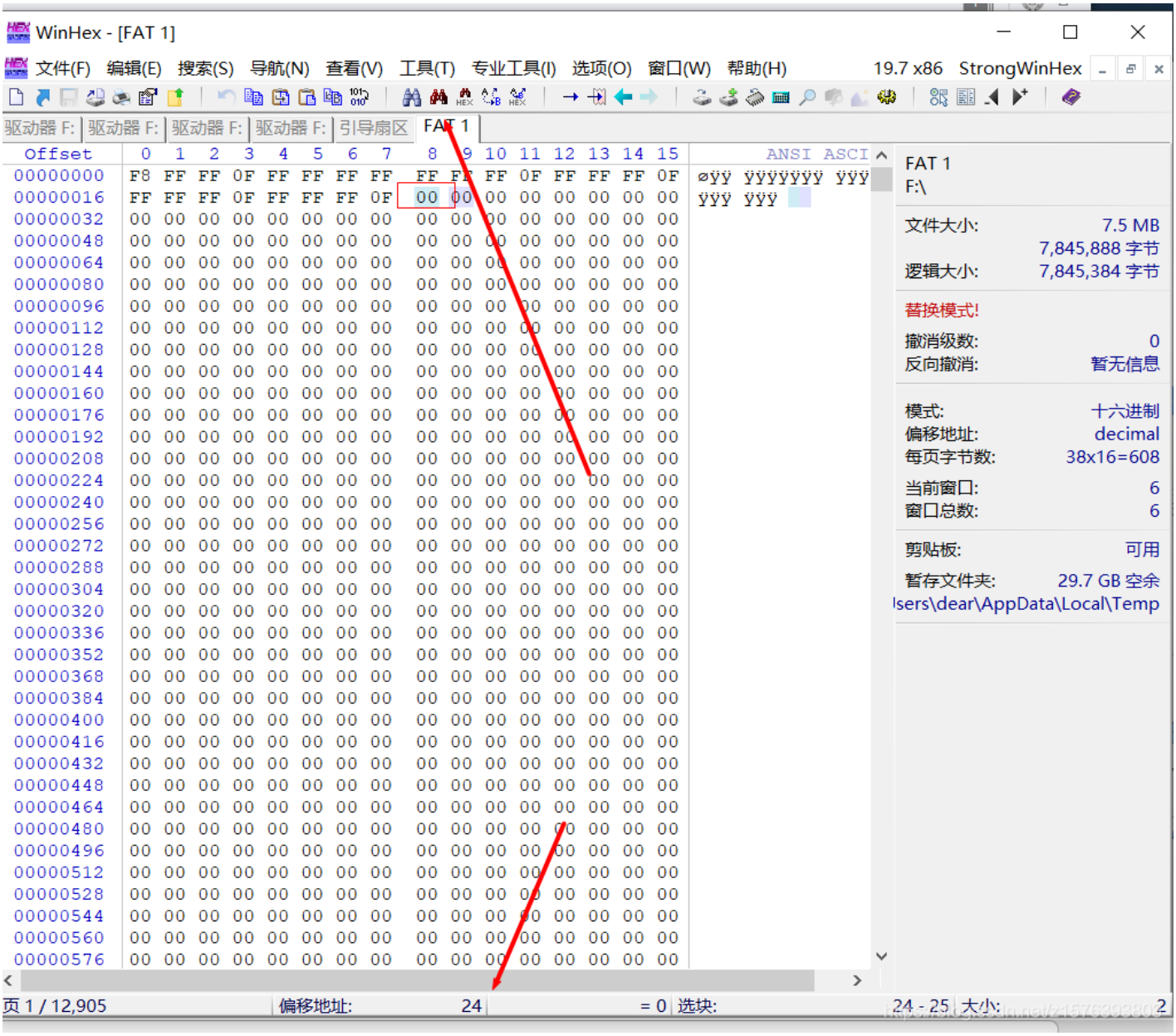
用簇”的值 0x0006 改为 0x0007，将“空闲簇总数”的 0x001DED7C 改为 0x001DED7B。

4. 修改 FAT 表

接下来需要修改 FAT 表中的空闲簇，在 Winhex 文件显示窗口中点击“FAT1”来到

FAT1 表的初始位置。

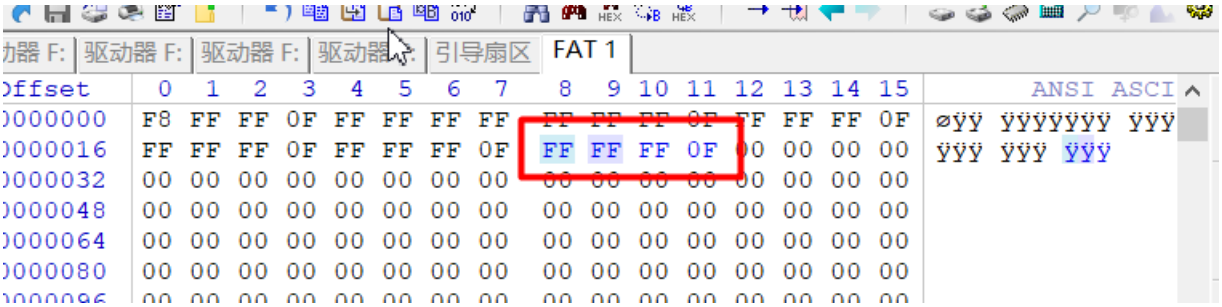
如图所示。

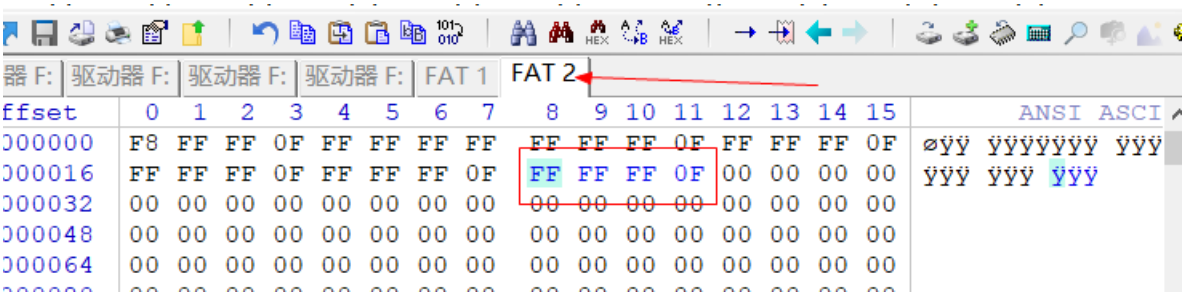


在 FAT1 表中，找到 0x0006 簇的状态字符，即相对起始处偏移 0x0006×4=24(十进制)的指

示的 4 个字节，将其值“00 00 00 00”改为“FF FF FF 0F”或者“F7 FF FF FF”,前者

表示该簇已被占用，后者表示该簇已坏,将该簇状态标志为坏簇或占用簇主 要为了让系统认为该簇已使用而不会被新写入的数据覆盖。FAT2 是 FAT1 的备份，为了保 险起见，FAT2也采用与 FAT1 同样的处理方式。

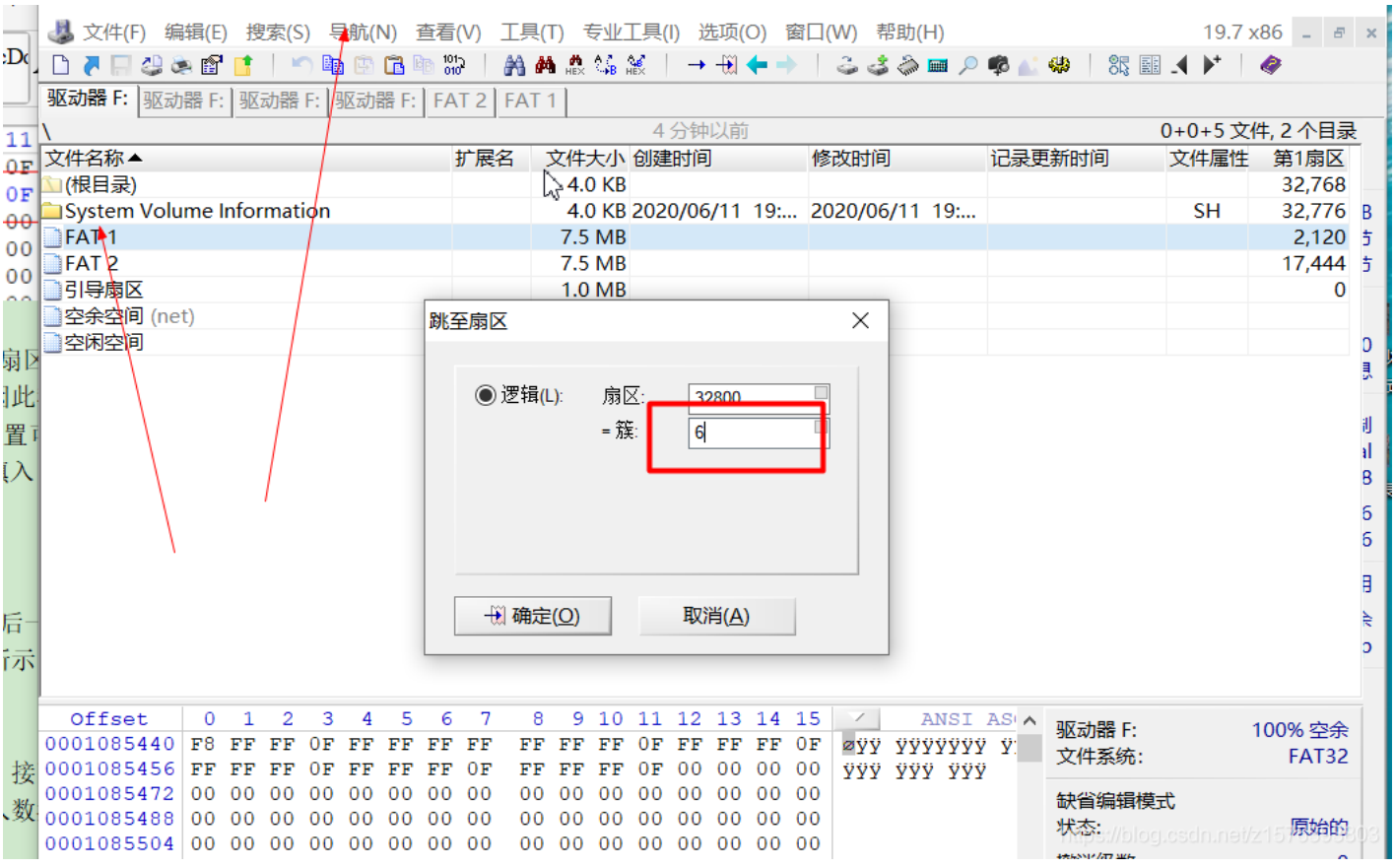




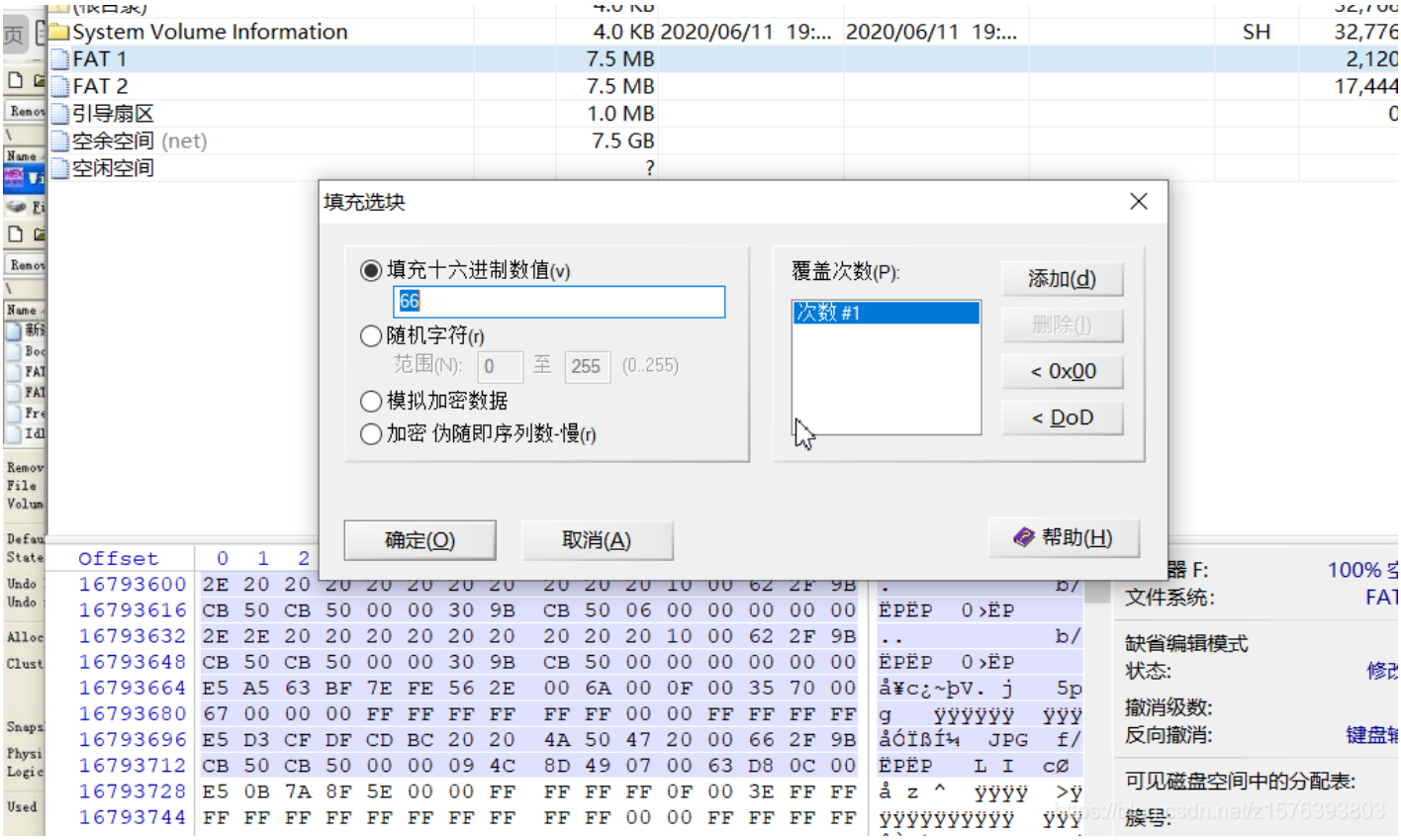
5. 填写数据

找到数据区“0x0006”簇开始的位置，将连续的 8 个扇区内容填入需要隐藏的数据，由于本实验只是为了验证写入数据不会被新文件覆盖，因此我们手工将每个扇区的开始部分改为连续的 0x66,即字符”f”。数据区的 0x0006 簇位置可利用 WinHex 菜单中提供的工具查找，选择菜单“à导航à跳至扇区”,在“簇”处填入 0x0006 转换为十进制的数字 6 即可，如图所示。

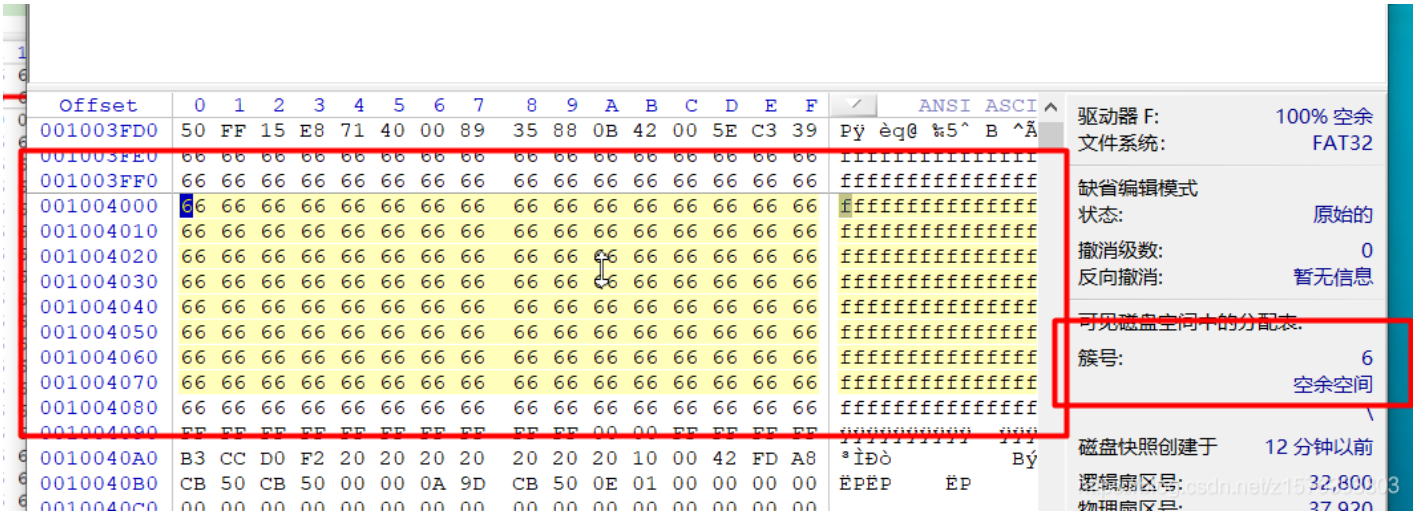
定位数据区指定簇



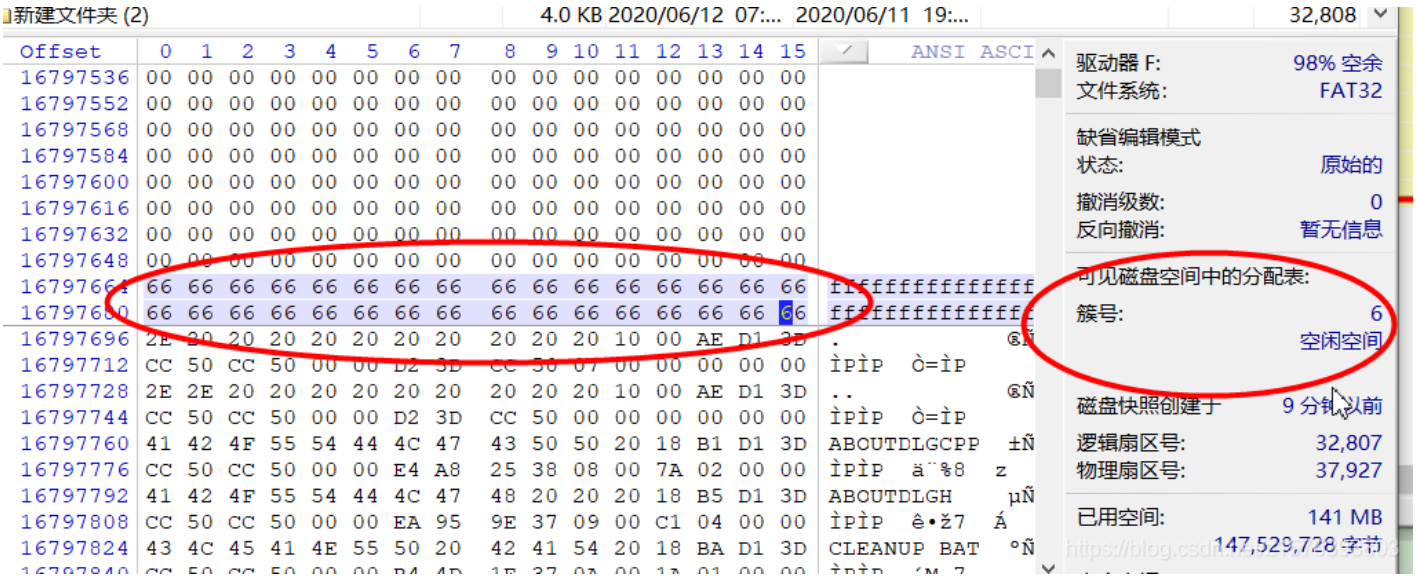
在本簇内开头和结尾写入0x66，右击鼠标→编辑→填充磁盘扇区→填充十六进制66 来验证此簇内不会被写入的数据覆盖 。在结尾写入数据以区别与下一个可用簇的界线。



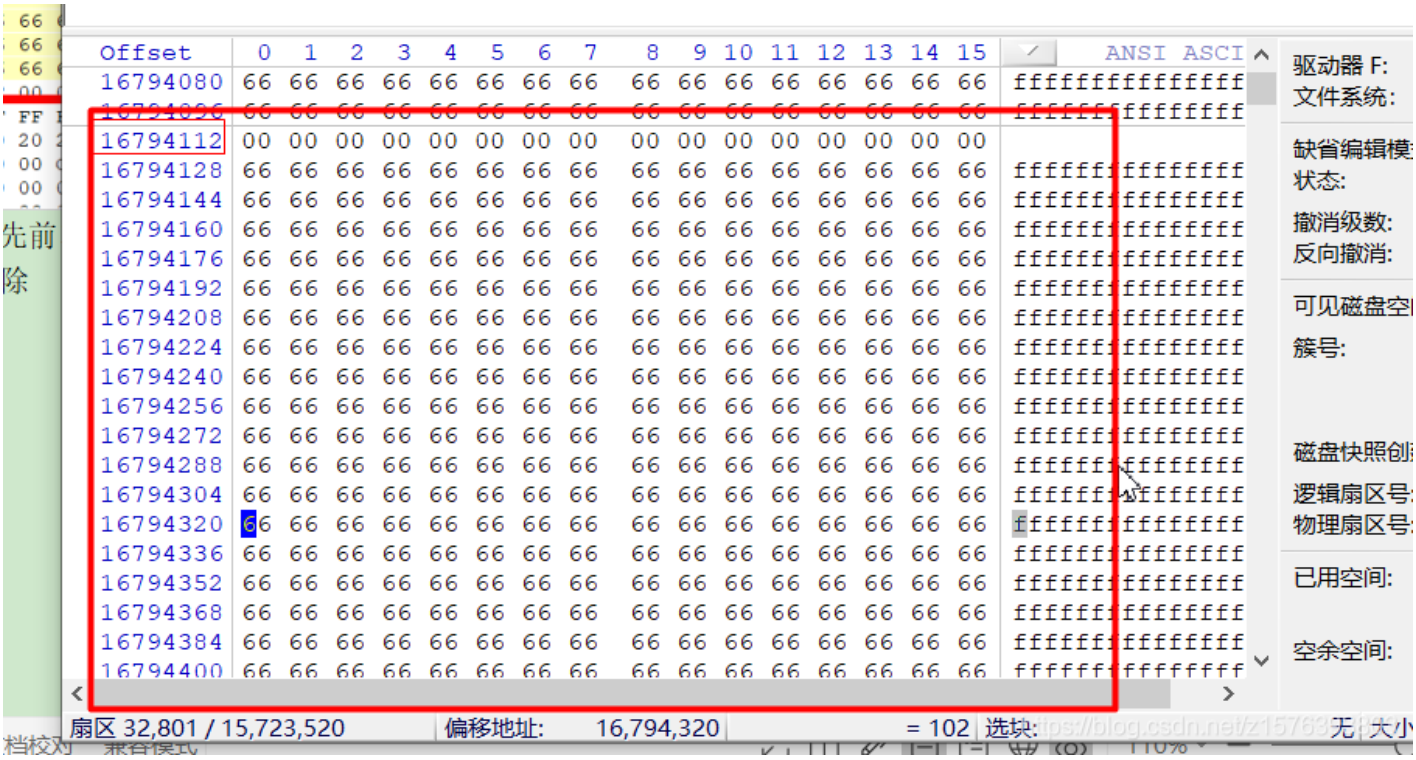
在本簇开头写入66



在本簇结尾处写入66



在下一个可用簇也写入数据，用来验证，这个簇在写入数据之后，写入的内容被覆盖



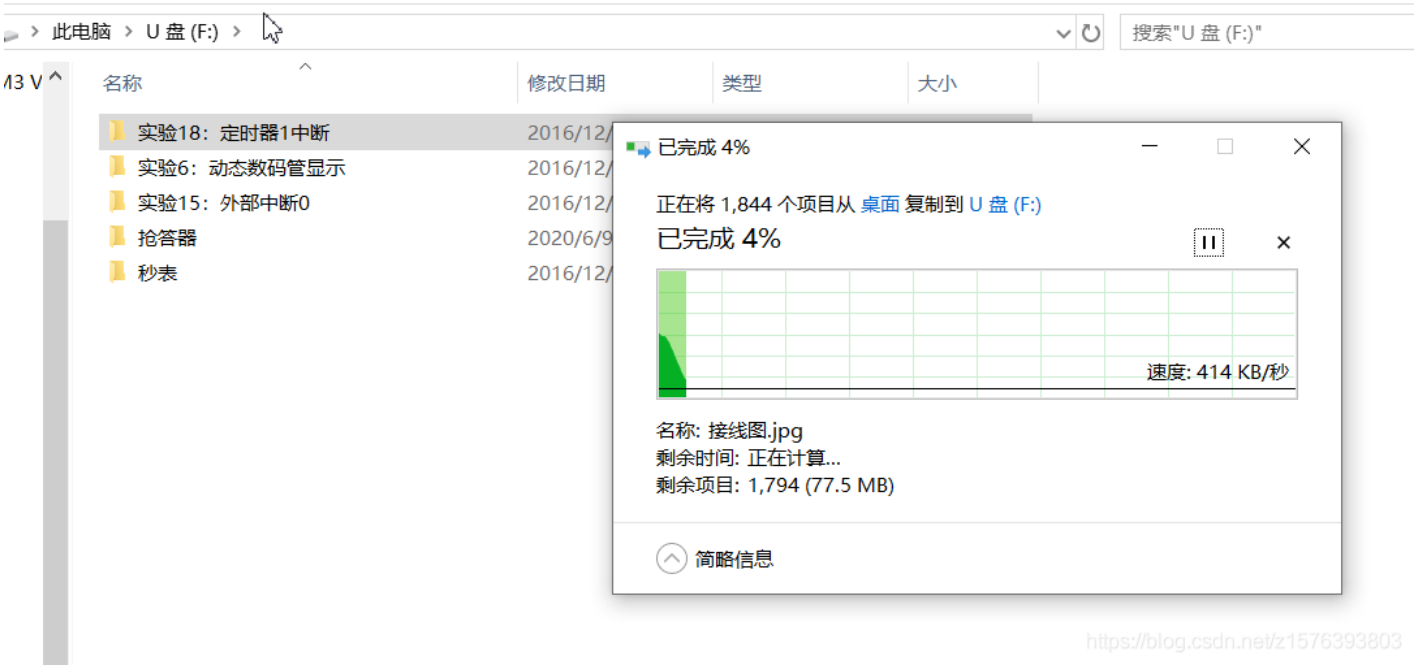
6. 保存与验证

点击菜单“文件→保存”将写入的数据保存。接下来需要往优盘中写入新的

文件，以用来验证之前写入的数据不会被覆盖。在拷入数据前，注意先将优盘从系统中正

常退出，重新插拔。

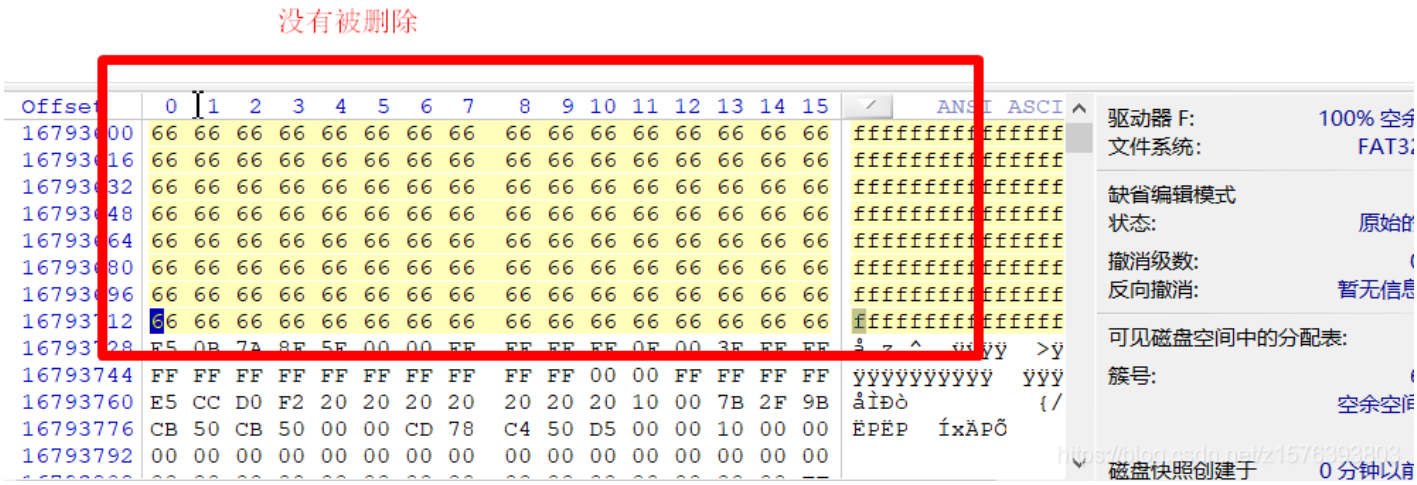
向U 盘随便复制进一些数据



再次用 WinHex 将优盘所在分区打开。定位到数据区的 0x006 簇的最后一个扇区，检查

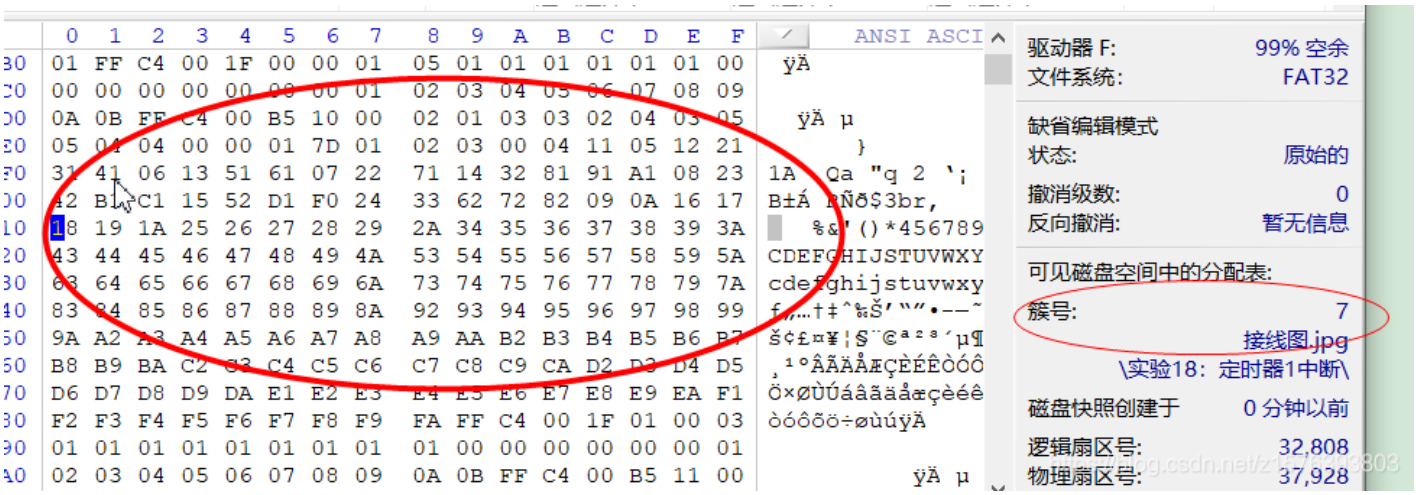
一下看看先前在 0x0066 簇写入的数据是否被覆盖，如图所示。

检查 0x006 簇数据



由图 可以看出，先前写入的0x006 处的隐藏数据没有被新文件覆盖，从

0x007 处内容开始被删除



4 实验结论

通过修改可用簇的值可以使写入的数据跳过本簇，不会覆盖里面的数据内容，在下一个簇开始写入数据