基于 FAT32 文件系统的数据隐写实验



<u>渔网探索者</u> 于 2020-06-12 09:45:26 发布 852 收藏 15 版权声明:本文为博主原创文章,遵循 <u>CC 4.0 BY-SA</u> 版权协议,转载请附上原文出处链接和本声明。 本文链接: <u>https://blog.csdn.net/z1576393803/article/details/106708216</u> 版权 **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

格式化磁盘

格式化 U 盘 (F:)	×	~	(٦	搜索"此由脑"		Q
容量(P):		×	Uf	(F·)	安全防护已	
7.49 GB	×.		剩	≞(···) • • • • • • • • • • • • • • • • • •	Q±(0)/0)	<u>مر</u> ر
文件系统(F)				OS (C).lnk		
FAT32 (默认)	~			📙 Cisco Packet Tr	acer 6.2sv	
分配单元大小(A)						
4096 字节	~					
还原设备的默认值(D)						
卷标(L)			>			
格式化选项(O)						
☑ 快速格式化(Q)						
开始(S) 关闭(C)						
		~				

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

<u>\</u>			1 分钟以前			0+0+5 孓	(件,2个目录
文件名称▲	扩展名	文件大小	创建时间	修改时间	记录更新时间	文件属性	第1扇区
🕥 (根目录)		4.0 KB					32,768
System Volume Information		4.0 KB	2020/06/12 08:	2020/06/12 08:		SH	32,776
FAT 1		7.5 MB					2,120
FAT 2		7.5 MB					17,444
引导扇区		1.0 MB					0
空余空间 (net)		7.5 GB					
空闲空间		?					

2

https://blog.csdn.net/z1576393803

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。

	🚟 WinHex -	[5]导	扇区	.]																					-	-
	🧱 文件(F) 编	辑(E) 搜	[索(S	5) Ę	}航(N) :	查看	(V)	工具(F) 1	€业	I具(l) ź	5项(0)	窗口	(W)	帮助)(H)			19	.7 x86	Stror	ngW
	🗋 👅 🔚 🕹 8	è 😭		- M) B	•	<u> </u>	101 010	2	A 🖊	HEX	₹. B	IEX	-				3	\$ 🎧)	ρ	¢ (: 🥨	85		▶+
	驱动器 F: 驱动)器 F	: 驱	动器	F:]	驱动	器 F:	ŝl	异扇	X																
ľ	Offset	0	1	2	3	4	5	6	7	8	9	А	в	С	D	E	F			ANS	SI	ASC	I۸	2100	50	
ſ	000002A0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00							「日子を	RK	
L	000002B0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00							F:\		
1	000002C0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00							文件	tzh:	
	000002D0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00							-		
	000002E0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00							逻辑	t/h:	
	000002F0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00							~~		
	00000300	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00							替换棒	莫式!	
	00000310	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00							撤消线	6₩0.	
	00000320	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00							反向援	~~~· 歓消·	
	00000330	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00							121-511		
	00000340	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00							横式・		
	00000350	00	00	00	00	00	00	LS.	00	00	00	00	00	00	00	00	00							信科	btı⊦∙	
	00000380	00	00	00	00	00	00	0.0	00	00	00	00	00	00	00	00	00							毎百日	これ. 乞井娄か・	
	00000370	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00							400	- 1388.	
	00000390	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00							当前智	町口:	
	000003A0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00							窗口印	3数:	
	000003B0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00							有女们上来	5 .	
	000003C0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00							95,701	×.	
	000003D0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00							暂存3	て件夹:	
	000003E0	00	00	00	00	72	72	41	61	7C	ED	1D	00	06	00	00	00		r	rAa	í			sers\d	ear∖Ap	эрD
	000003F0	00	00	00	00	00	.90	.00	0.0	00	99	-00	00	00	00	55	AA		e -			1	υ			
	00000400	00	00	00	00	00	羽氏	60	Ψ̈́υ	00'	මරි	FOU	00	00	00	00	1991	用尨	矢							
	00000410	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00									
	00000420	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00									
	00000430	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00									
	00000440	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00									
	00000450	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00									
÷	~~~~~		~ ~ ~		~ ~ ~	~ ~	~ ~	~ ~ ~			~ ~	~ ~	~ ~	~ ~ ~	~ ~	~ ~										

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

撤消约		~~	~~	~~	~~	~~	~~	~~	~~~	~~	~~	~~	~~	~~	~~	~~	č
		00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	0
反问道		00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	0
		00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	0
模式:		00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	0
偏移出		00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	0
동품리		00							00					00			~
带贝子		00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	0
当前辞	rrAa <mark>{í</mark>	00	00	00	07	00	1D	ED	7B	61	41	72	72	00	00	00	0
소미는	υ	AA	55	00	00	00	00	00	00	00	00	00	00	00	00	00	0
國口尼		00	<u> </u>	00	00	00	00	00	00	00	00	00	00	00	00	00	0
自立用上标		00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	0
95 XA10		00	00	0.0	0.0	00	0.0	00	0.0	00	00	00	00	00	00	00	0
新たて		00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	0
		00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	0
oolsers\d	s://piog.csdn.net/z15/	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	0

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。

🚟 WinHex -	· [FAT	1]																					_			×
🧱 文件(F) 🕴	编辑(E)	搜	溹(S) Ę	≩航(I	N) i	查看(V)	工具(1	F) 7	€业	I具(l) ដំ	先项(O)	窗口(W) 看	帮助(H))	1	9.7 x8	6 Stro	ngV	VinHex	-	ъ×
🗅 👅 🗔 🕹	۵ 😭				1 🕀	6	101- 010	2	A M	HEX	2.G	Nex	-	-121			34	i 🥋 🖿		🕫 🔬 🤇	u	35 副 -	Ē			
驱动器 F: 驱症	动器 F:	驱	动器	F:]]	驱动	器 F:	 	扇	K FA	T 1																
Offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15		Al	ISI .	ASCI /		• 1				
00000000	F8	FF	FF	0F	FF	FF	$\mathbf{F}\mathbf{F}$	FF	FF	F	FF	0F	FF	FF	FF	0F	øÿÿ	ŸŸŸŸ	ŶŶŶŶ	ŸŸŸ	E-1	1				
00000016	FF	FF	FF	0F	FF	FF	FF	0F	00	Ø 0	00	00	00	00	00	00	ŸŸŸ	ΫΫΫ			1.1					
00000032	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00					文件	大小:			7.	5 MB
00000048	00	00	00	00	00	00	00	00	00	00	9	00	00	00	00	00								7,845	5,888)字节
00000064	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00					逻辑	大小:		7,845	5,384	字节
00000000	00	00	00	00	00	00	00	00	00	00	00	60	00	00	00	00					****	4世-121				
00000112	00	00	00	00	00	00	00	00	00	00	00	ŏõ	00	00	00	00					省势	engitu:				
00000128	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00					撤消	级数:				0
00000144	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00					反向]撤消:			智力	信息
00000160	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00										ALL Hall
00000176	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00					使了 (点)が				+7	で进制
00000192	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00					偏移	5-10-11: [今:###5		2		
00000208	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00					щμ			50	5X10	-000
00000224	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00					当前	窗口:				6
00000256	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00					窗口	总数:				6
00000272	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00					前肌	t板・				可田
00000288	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00					±€+			20	7 00	
00000304	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00					首付	*又14兴; door\ 4	: 	29 \ata\1.c		· 仝宋
00000320	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00					isers	dear (A	ppr		cal/I	emp
00000336	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00										
00000352	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00										
00000384	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00										
00000400	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00										
00000416	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00										
00000432	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00										
00000448	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00										
00000464	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00										
00000480	00	00	00	00	00	00	00	00	00	00	00	00	20	00	00	00										
00000496	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00										
00000528	00	00	00	00	00	00	00	00	00	00	00		00	00	00	00										
00000544	00	00	00	00	00	00	00	00	00	00	00	6	00	00	00	00										
00000560	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00										
00000576	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00				~	·					
<											1									>						
页1/12,905					偏	移地	址:			24	ł				=	0 送	缺:				24 - 2	25 大小	Mala i	nei/z15	7639	13302

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。

C 🔲 👁				-) 4			900	010	ana M	HEX	⊖⊶¥B	HEX		5	<u> </u>		99 G	a fun	~	70 I	-046
力器 F: 驱云	为器 F	-: 30	【动器	름 F:	驱动	嚻	: 3	导扇	K F/	AT 1											
Offset	0	1	. 2	3	4	5	e	57	8	9	10) 11	12	13	14	15		AN	SI i	ASCI	~
0000000	F8	FF	FF	0F	FF	FF	FF	FF	' - PP	- FF	- FI	- OT	FF	FF	FF	' 0F	øÿÿ	ŸŸŸŸ	ŸŸŸ	ŸŸŸ	į
)000016	FF	FF	FF	0F	FF	FF	FF	OF	FF	FF	FF	' 0F	· 🚺 0	00	00	00	ŸŸŸ	ŸŸŸ	ŸŸŸ		
)000032	00	00	00	00	00	00	00	00	00	-00	-00	- 00	-00	00	00	00					
)000048	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00					
000064	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00					
0800000	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00					
1000006	0.0	00	00	00	00	00	00	00	0.0	00	00	00	00	00	00	00					
																	-				
ة 😓 🔜 🦷	8 😭		1) 📠	8	6 I	B 101- 010	2	A 🖊	HEX	A A	iex	-	-100	← -		ి ఫి	📾 🥋	P 📢	ð 🔬	4
器 F: 驱动	器 F:	BRi	动器	F: 3	区动制	器 F:	FA	T 1	FAT 2	2					_						
ffset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15		ANS	ΙA	SCI	~
000000	F 8	FF	FF	0F	FF	\mathbf{FF}	\mathbf{FF}	FF	FF	FF	FF	0F	FF	FF	FF	0F	øÿÿ	ŸŸŸŸŸ	ΫŸ	ŸŸŸ	
000016	FF	FF	FF	0F	FF	FF	FF	0F	FF	FF	FF	0F	00	00	00	00	ŸŸŸ	ŸŸŸ Y	ΫŸ	- 1	
000032	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00					
000048	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00					
000064	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00					
200000	00	0.0	00	00	0.0	0.0	00	0.0	0.0	00	00	0.0	0.0	0.0	00	00					

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

	😃 文件(F) 编辑(E) 搜索(S) 导航(N) 🗄	查看(V) 工具(T) 专业工具(I) 选项(O) 窗	囗(W) 帮助(H)	19.7 x86 💶 🖉 🗙
DC.	🗅 🖉 🗐 🥝 🎘 🖀 🖉 📑 🗎 🖄 🛤	🖻 1017 🎮 🚧 🖧 🎲 💥 🕂 🕂 🔶 🔶	li 🖉 🖉 📾 🧼 🕹	🦇 🛛 🕄 🔠 🔺 🕨 🖉
	驱动器 F: 驱动器 F: 驱动器 F: 驱动器 F:	FAT 2 FAT 1		
11	Λ	4 分钟以前		0+0+5 文件, 2 个目录
0F	文件名称▲	扩展名 文件大小 创建时间	修改时间 记录更	臣新时间 文件属性 第1扇区
0F	🐚 (根目录)	💫 4.0 KB		32,768
00	System Volume Information	4.0 KB 2020/06/11 19:	2020/06/11 19:	SH 32,776 B
00	FAT 1	7.5 MB		2,120 5
00	FAT 2	7.5 MB		17,444 5
~~	副引导扇区	1.0 MB		0
	空余空间 (net)	跳至扇区	X	
<u>-</u>	空闲空间			D
羽区				
此		●逻辑(L): 扇区:32800		
罟		= 簇: 6		i) ا
н' 				al
ĮΛ			-	В
	\			6 6 月
后-		₩ 确定(<u>O</u>) 取消(<u>A</u>)		₽
				c
141				
	Offset 0 1 2 3 4 5	6 7 8 9 10 11 12 13 14	5 / ANSI AS	
	0001085440 F8 FF FF 0F FF FF	FF FF FF FF FF OF FF FF FF	F ØVV VVVVVV V	兆动器 ト: 100% 空余
接	0001085456 FF FF FF 0F FF FF	FF OF FF FF FF OF 00 00 00 0	0 000 000 000	又件系統: FAT32
1×L	0001085472 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00 00	00	缺省编辑模式
、釵	0001085488 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00 0	00	状态
	0001085504 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00 0	00	TMPS://blog.osdn.net/z1a/75999803
	I I			

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

1																				
0	Offset	0	1	2	3	4	5	6	7	8	9	A	в	С	D	Е	F	ANSI ASCI A	驱动器 F:	100% 空余
6	001003FD0	50	FF	15	E8	71	40	00	89	35	88	0B	42	00	5E	C3	39	Pÿèq0 ‰5° B ^A	文件系统:	FAT32
	001003FE0	66	66	66	66	66	66	66	66	66	66	66	66	66	66	66	66			
	001003FF0	66	66	66	66	66	66	66	66	66	66	66	66	66	66	66	66		缺省编辑模式	
	001004000	66	66	66	66	66	66	66	66	66	66	66	66	66	66	66	66		状态:	原始的
	001004010	66	66	66	66	66	66	66	66	66	66	66	66	66	66	66	66		描述当 级 数·	0
	001004020	66	66	66	66	66	66	66	66	66	66	T ^o	66	66	66	66	66		后向撤消	
	001004030	66	66	66	66	66	66	66	66	66	66	620	66	66	66	66	66			
	001004040	66	66	66	66	66	66	66	66	66	66	66	66	66	66	66	66			
	001004050	66	66	66	66	66	66	66	66	66	66	66	66	66	66	66	66	±±±±±±±±±±±±	570 ALLE 1 5 1 4575	HUNDER
	001004060	66	66	66	66	66	66	66	66	66	66	66	66	66	66	66	66	fffffffffffff	簇号:	6
	001004070	66	66	66	66	66	66	66	66	66	66	66	66	66	66	66	66	fffffffffffff		空余空间
	001004080	66	66	66	66	66	66	66	66	66	66	66	66	66	66	66	66	ffffffffffff		Λ.
ł	001004090	FF	PP.			PP.			PP.		P P	00	00	P P		PP	FF	<u> 199999999999999999999</u>	磁盘体昭创建于	12 分轴以前
6	0010040A0	В3	CC	D0	F2	20	20	20	20	20	20	20	10	00	42	FD	A 8	°ÍÐÒ BÝ		L D MAKE
6	0010040B0	CB	50	СВ	50	00	00	0A	9D	CB	50	0E	01	00	00	00	00	ËPËP ËP	逻辑扇区号code.n	et/z15 32,800 .0
6	001004000	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00		物理局区早	37 020

在本簇结尾处写入66

■新建文件夹(2	2)									4.0) KB	202	0/06	5/12	07:.	20	020/06/1	1 19:				32,808	1
Offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	_	ANSI 2	ASCI	^ <u>av</u>	the co	0.0% 穴仝	
16797536	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00			_	30	以面に	50/0 王示	
16797552	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00				X	十余机;	FA152	
16797568	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00				41	省编辑模式		
16797584	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00				<u>лт</u> х-		(百+465	.
16797600	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00				1	2X.	尿始的	1
16797616	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00				撤	消级数:	0	
16797632	00	00	00	00	00	00	00	00	0.0	00	00	00	00	00	00	00				反	向撤消:	暂无信息	
16797648	00	00	00	00	0.0	0.0	0.0	0.0	0.0	00	0.0	0.0	00	00	0.0	00							
1679766	66	66	66	66	66	66	66	66	66	66	66	66	66	66	66	66	FREEF	ffffff	FFFF		见磁盘空间中	中的分配表:	
167976	66	66	66	66	66	66	66	66	66	66	66	66	66	66	66	66	fffff		FFF	· 名芒.	므.	6	N
16797696	200	20	20	20	20	20	20	20	20	20	20	10	00	75	D1	2	11111			加失	· -	0 西田西河)
16707710	20	5.0	20	20	20	20	20	20	20	20	20	10	00	ALC:	0.0	0.0	, tptp	à-tr	01			오씨오면	1
16797712	0.0	20	20	20	00	00	02	20	-00	-50	207	10	00	20	00 D1	20	IFIF	0-19	C 11				
16797728	ZE	ZE	20	20	20	20	20	20	20	20	20	10	00	AE	DI	30	****	à ÷=	GN	磁	盘快照创建一	- 9 分银以前	i
16/9//44	CC	50	cc	50	00	00	D2	3D	CC	50	00	00	00	00	00	00	TETE	0=15				20.007	.
16797760	41	42	4F	55	54	44	4C	47	43	50	50	20	18	В1	D1	3D	ABOUT	DLGCPP	±N	逻	旗扇区号:	32,807	
16797776	CC	50	CC	50	00	00	E4	A8	25	38	08	00	7A	02	00	00	IPIP	ä~%8	z	物	埋扇区号:	37,927	
16797792	41	42	4F	55	54	44	4C	47	48	20	20	20	18	в5	D1	ЗD	ABOUT	DLGH	μÑ	_			
16797808	CC	50	CC	50	00	00	EA	95	9E	37	09	00	C1	04	00	00	ÌPÌP	ꕞ7	Á	E	用空间:	141 MB	
16797824	43	4C	45	41	4E	55	50	20	42	41	54	20	18	BA	D1	3D	CLEAN	UP BAT	°Ñ			147,529,728 字节	03
16707040	00	EO	00	EA	00	00	пΛ	4 15	1 17	27	07	00	1 7	01	00	00	tntn	(M 7		× .			

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

66 (
66 0	Offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	× 1	ANSI ASCI 🔺	제 <u>구</u> 뉴물론 E·
00 0	16794080	66	66	66	66	66	66	66	66	66	66	66	66	66	66	66	66	ffffff	fffffff	立住玄弦・
FF I	16794096	66	66	66	66	66	66	66	66	66	66	66	66	66	66	66	66	ffffff.	fffffff	XIT:890
20 2	16794112	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00			缺省编辑模:
00 0	16794128	66	66	66	66	66	66	66	66	66	66	66	66	66	66	66	66	ffffff	fffffff	状态:
00 0	16794144	66	66	66	66	66	66	66	66	66	66	66	66	66	66	66	66	ffffff	fffffff	
先前	16794160	66	66	66	66	66	66	66	66	66	66	66	66	66	66	66	66	ffffff	fffffff	撤消级数:
2 G (19	16794176	66	66	66	66	66	66	66	66	66	66	66	66	66	66	66	66	ffffff	fffffff	反向撤消:
徐	16794192	66	66	66	66	66	66	66	66	66	66	66	66	66	66	66	66	ffffff	fffffff	
	16794208	66	66	66	66	66	66	66	66	66	66	66	66	66	66	66	66	ffffff	fffffff	可见磁盘空
	16794224	66	66	66	66	66	66	66	66	66	66	66	66	66	66	66	66	ffffff	fffffff	簇号:
	16794240	66	66	66	66	66	66	66	66	66	66	66	66	66	66	66	66	ffffff	fffffff	200 20
	16794256	66	66	66	66	66	66	66	66	66	66	66	66	66	66	66	66	ffffff	fffffff	
	16794272	66	66	66	66	66	66	66	66	66	66	66	66	66	66	66	66	ffffff	ffffffff	
	16794288	66	66	66	66	66	66	66	66	66	66	66	66	66	66	66	66	ffffff	ffffffff	磁盘快照创
	16794304	66	66	66	66	66	66	66	66	66	66	66	66	66	66	66	66	ffffff	ACFFFFFFF	逻辑扇区县
	16704320	Ge	66	66	66	66	66	66	66	66	66	66	66	66	66	66	66		££££££££	と構成して
	16704320	66	66	66	66	66	66	66	66	66	66	66	66	66	66	66	66			1/小生/的区方。
	16794336	66	66	66	66	66	66	66	66	66	66	66	66	66	66	66	66			已田内间・
	16794352	66	66	66	66	66	66	66	66	66	66	66	66	66	66	66	66	IIIIII		
	16794368	66	66	66	66	66	66	66	66	66	66	66	66	66	66	66	66	İİİİİİ	<u>ttttttt</u> t	
	16794384	66	66	66	66	66	66	66	66	66	66	66	66	66	66	66	66	ffffff	ffffffff	空余空间:
	16794400	66	66	66	66	66	66	66	66	66	66	66	66	66	66	66	66	ffffff	fffffff	
												_					_		>	
1417-0	扇区 32,801 / 1	5,72	23,52	20		偏	移地	址:	1	16,794	,320)				= 1()2 送	缺:fips://ol	og.csdn.net/z15	763无 大小
															0		-		11070	(.

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

3 V ^		修改日期		举刑		大小					
		2016/42		~1		~					
	▲ 头验18: 定时器1中断	2016/12/	🖪 已完成	4%				_			×
	▶ 实验6: 动态数码管显示	2016/12/									
	📙 实验15: 外部中断0	2016/12/	正在将	1,844 个项目	从桌面	复制到 U 🕯	盘 (F:)				
	1 抢答器	2020/6/9	已完月	戓 4%					П	×	
	▶ 秒表	2016/12/	名称: 封 剩余项	接线图.jpg 间: 正在计算 目: 1,794 (77.	5 MB)			速度	度: 414	KB/秒	
		L	◇ 简	略信息	_			_		_	

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。

没有被删除

检查 0x006 簇数据

Offset		0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	Z A	ANS	ASCI	~	IV 动怒 C·	100% 索子
167930	00	66	66	66	66	66	66	66	66	66	66	66	66	66	66	66	66	ffffff	fff	fffff		池40話「. 文供受法、	
167930	16	66	66	66	66	66	66	66	66	66	66	66	66	66	66	66	66	ffffff	fff	fffff		又什杀统。	FATS
167930	32	66	66	66	66	66	66	66	66	66	66	66	66	66	66	66	66	ffffff	fff	fffff		缺省编辑模式	
167930	48	66	66	66	66	66	66	66	66	66	66	66	66	66	66	66	66	ffffff	fff	fffff		状本・	唐始的
167930	64	66	66	66	66	66	66	66	66	66	66	66	66	66	66	66	66	ffffff	fff	fffff		100/24	лаханн.
167930	80	66	66	66	66	66	66	66	66	66	66	66	66	66	66	66	66	ffffff	Eff	fffff		撤消级数:	
167930	96	66	66	66	66	66	66	66	66	66	66	66	66	66	66	66	66	ffffff	fff	fffff		反向撤消:	暂无信息
16793	12	66	66	66	66	66	66	66	66	66	66	66	66	66	66	66	66	ffffff	Eff	fffff			() #]_ +
16793	28	F 5	0B	7⊾	85	5.5	00	00	FF	도도	도도	토토	0 F	00	3₽	도도	FF	3 7 ^	ŵ.	ÿ >ÿ		可见磁盘空间中的统	了配表:
167937	744	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	00	00	FF	FF	FF	FF	2222222	YYYY	YYY		簇号:	
167937	760	E5	CC	D0	F2	20	20	20	20	20	20	20	10	00	7B	2F	9B	åÌĐò		{/			空余空间
167937	776	СВ	50	СВ	50	00	00	CD	78	C4	50	D5	00	00	10	00	00	ËPËP Í	ÍxÄI	õ			
167937	792	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00				Ų,	磁盘枯昭台ば妻王	0 公钟心言
		0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0		0.0	0.0	0.0	0.0	0.0	0.0						12211111111111111111111111111111111111	リガザ以降

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

30 20	0 01 00	1 FF 00	2 C4 00	3 00 00	4 1F 00	5 00 00	6 00	7 01 01	8 05 02	9 01 03	A 01 04	B 01 05	C 01 06	D 01 07	E 01 08	F 00 09	Z ANSI ASCI A ŸÄ	驱动器 F: 文件系统:	99% 空余 FAT32
00 20	0A 05	0в 04	FF 04	C4 00	00 00	В5 01	10 7D	00 01	02 02	01 03	03 00	03 04	02 11	04 05	03 12	05 21	ÿÄμ }	缺省编辑模式 状态:	原始的
70 00 10	31 42 18	41 BL	06 C1	13 15 25	51 52 26	61 D1 27	07 F0 28	22 24 29	71 33 2A	14 62 34	32 72 35	81 82 36	91 09 37	A1 0A 38	08 16 39	23 17 3A	1A Qa "q 2 '; B±Á 1Ňð\$3br, %s'()*456789	撤消级数: 反向撤消:	0 暂无信息
20 30	43 63	44 64	45 65	46 66	47 67	48 68	49 69	4a 6a	53 73	54 74	55 75	56 76	57 77	58 78	59 79	5a 7a	CDEFGHIJSTUVWXY cdefghijstuvwxy	可见磁盘空间中的分	〉配表:
10 50	83 9A 88	84 A2 89	85 A3 BA	86 A4	87 A5	88 A6	89 A7	8A A8 C6	92 A9 C7	93 AA C8	94 B2	95 B3	96 B4 D2	97 B5 D2	98 B6	99 87 05	f,+‡^%s'`"• 𢣤¥¦§"©ª²°´μ¶ 1°àãăåæcèŕŕèòóô	簇号:	7 接线图.jpg
70 30	D6 F2	D7 F3	D8 F4	D9 F5	DA F6	E1 F7	E2 F8	E3 F9	E4 FA	E5 FF	Е6 С4	E7 00	E8 1F	E9 01	EA 00	F1 03	ÖרÙÚáâãäåæçèéê òóôõö÷øùúÿÄ	(头预18: 磁盘快照创建于	20 分钟以前
90 ₹0	01 02	01 03	01 04	01 05	01 06	01 07	01 08	01 09	01 0A	00 0B	00 FF	00 C4	00 00	00 B5	00 11	01 00	Ϋ́Äμ	逻辑扇区号: 物理扇区号:	32,808 37,928

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