



计算机安全与维护

Windows 系统数据安全与维护



本章内容提要

- 磁盘、分区和卷
- NTFS的恢复支持
- 误删除数据的手工恢复
- 数据备份方案
- 加密文件系统（EFS）的安全性



计算机硬件组成回顾——节选自优秀学生作业





计算机硬件组成回顾——节选自优秀学生作业



blog.sina.com.cn/u/1912519370



计算机硬件组成回顾——节选自优秀学生作业





存储介质（设备）

• 储存信息的硬件设备

- 利用电能方式存储信息的设备如：各式存储器，如各式随机存取存储器（RAM）、只读存储器（ROM）等
- 利用磁能方式存储信息的设备如：硬盘、软盘、磁带、磁芯存储器、磁泡存储器
- 利用光学方式存储信息的设备如：CD或DVD
- 利用磁光方式存储信息的设备如：MO（磁光盘）
- 利用其他实体物如纸卡、纸带等存储信息的设备如：打孔卡、打孔带等



持久化存储 VS. 非持久化存储

- 是否在断电后可以继续保存数据（信息）
- 典型代表设备
 - 持久化存储：硬盘、U盘、光盘
 - 非持久化存储：内存、CPU缓存



是否可擦除（反复读写）

- 硬件限制
 - 光盘
- （操作）系统限制
 - 手机操作系统所驻留的存储介质



访问存储介质的硬件接口标准

- 硬件（直连）接口

- USB
- IDE（电子集成驱动器）
- SATA（串行ATA）
- SCSI（小型计算机系统接口）
- FC（光纤通道）
- SAS（串行连接SCSI，向下兼容SATA）

PC

服务器



访问存储介质的硬件接口标准

- 网络接口
 - NAS
 - SAN



操作系统与硬件设备

- BIOS 与 UEFI
 - 先于操作系统启动，引导操作系统启动
 - 低阶“操作系统”
- 操作系统的设备驱动
 - 针对不同类型设备开发和运行对应的设备驱动程序，负责管理硬件设备



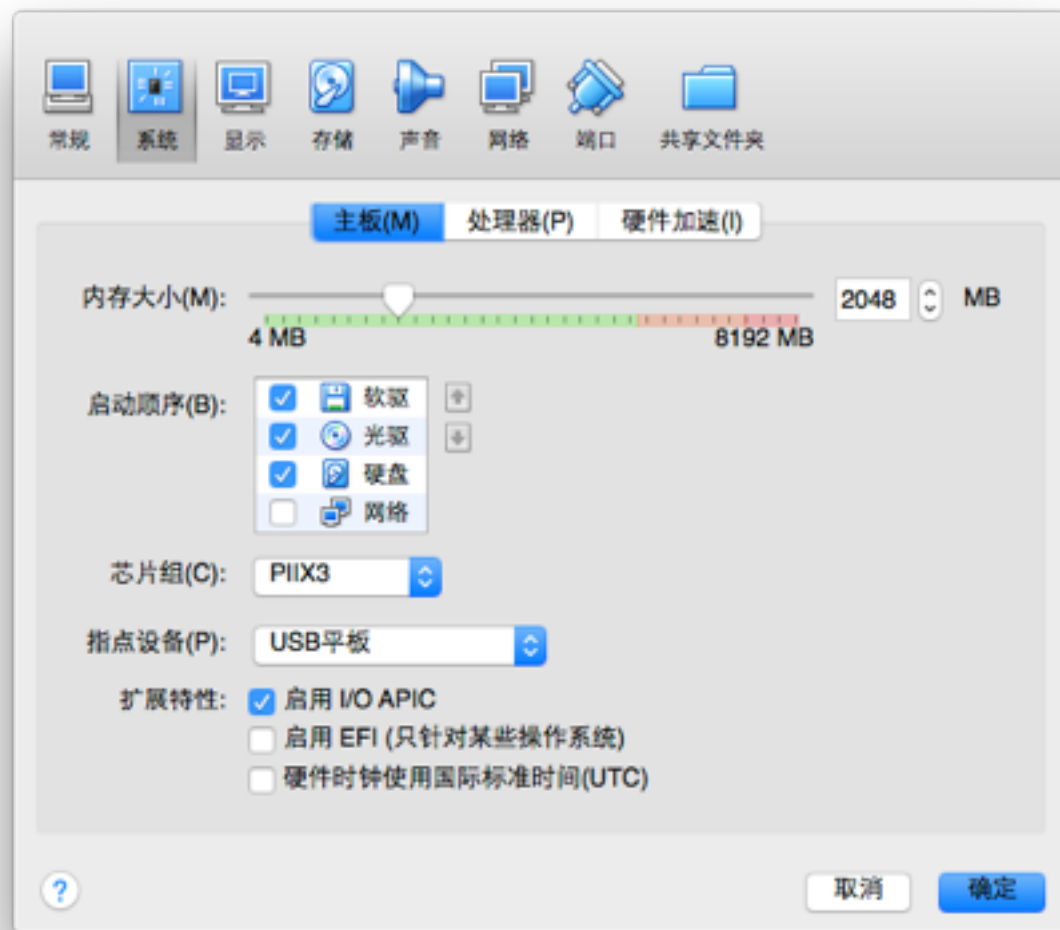
BIOS

- 在PC启动的过程中，BIOS担负着初始化硬件，检测硬件功能，以及引导操作系统的责任
 - 在早期，BIOS还提供一套运行时的服务程序给操作系统及应用程序使用
- BIOS程序存放于一个掉电后内容不会丢失的只读存储器中，系统加电时处理器的第一条指令的地址会被定位到BIOS的存储器中，便于使初始化程序得到执行



EFI与UEFI

- BIOS的升级换代技术
- 支持32位或64位运行模式
- 功能更多，容错和纠错特性更强





磁盘

- Windows对可持久化存储设备的统一命名
- 基本磁盘
 - 大多数个人计算机都配置为基本磁盘，该类型最易于管理
- 动态磁盘
 - 面向高级用户和IT专业人员



基本磁盘

- 使用主分区、扩展分区和逻辑驱动器来组织数据
- 格式化的分区也称为卷（术语“卷”和“分区”通常互换使用）
- 在大多数Windows PC版本中，基本磁盘可以有四个主分区或三个主分区和一个扩展分区。扩展分区可以包含多个逻辑驱动器（最多支持 128 个逻辑驱动器）
- 基本磁盘上的分区不能与其他分区共享或拆分数据
- 基本磁盘上的每个分区都是该磁盘上的一个独立的实体



动态磁盘

- 动态磁盘可以包含大量的动态卷（大约 2000 个），其功能类似于基本磁盘上使用的主分区
- 在 Windows 的某些版本中，可以将多个独立的动态硬盘合并为一个动态卷（称为分卷），将数据拆分到多个硬盘（称为分拆）以提高性能，或者在多个硬盘之间复制数据（称为镜像）以提高可靠性



分区和逻辑驱动器

- 分区（有时也称为卷）是硬盘上的一个区域，可以使用文件系统进行格式化并使用字母表的字母标识。例如，大多数 Windows 计算机上的驱动器 C 就是一个分区
- Windows 系统只能安装在主分区上
- 扩展分区是解决基本磁盘可以含有的主分区数量限制的方法。它是一个可以容纳一个或多个逻辑驱动器的容器。除不能用于启动操作系统之外，逻辑驱动器的功能与主分区的功能相似



格式化磁盘和驱动器

- 硬盘是计算机上的主要存储设备，使用前需要进行格式化
- 格式化磁盘是指使用文件系统配置磁盘，以便 Windows 能够在磁盘上存储信息
- 在格式化硬盘之前，必须先在上面创建一个或多个分区
- “快速格式化”是一种格式化选项，它能够在硬盘上创建新文件表，但不会完全覆盖或擦除磁盘。快速格式化比普通格式化快得多，后者会完全擦除硬盘上现有的所有数据。



分区和卷

- 分区是硬盘上的一个区域，能够进行格式化并分配有驱动器号。在基本磁盘（个人计算机上最常见的磁盘类型）上，卷是格式化的主分区或逻辑驱动器
- 系统分区通常标记为字母 C。字母 A 和 B 留给可移动驱动器或软盘驱动器。某些计算机将硬盘分区为单个分区，这样整个硬盘就用字母 C 表示。其他计算机可能有一个包含恢复工具的附加分区，以免 C 分区上的信息被损坏或不可用



GPT磁盘与MBR磁盘

- GPT(Globally Unique Identifier Partition Table Format)一种由基于 Itanium 计算机中的可扩展固件接口 (EFI) 使用的磁盘分区架构
 - 允许每个磁盘有多达 128 个分区，支持高达 18 EB的卷大小，允许将主磁盘分区表和备份磁盘分区表用于冗余，还支持唯一的磁盘和分区 ID (GUID)
- MBR(Master Boot Record)磁盘
 - 最大卷为2TB
 - 每个磁盘最多4个主分区（或3个主分区，1个扩展分区和无限制的逻辑驱动器）



本章内容提要

- 磁盘、分区和卷
- NTFS的恢复支持
- 误删除数据的手工恢复
- 数据备份方案
- 加密文件系统（EFS）的安全性



NTFS的恢复支持

- NTFS的恢复支持可确保，如果发生断电或者系统失败，文件操作不会遗留在未完成的状态，磁盘卷的结构仍然完好无损，无需运行磁盘修复工具
- NTFS使用一种事务处理方案实现可恢复性，确保即使对于非常大的磁盘，磁盘的恢复也会绝对快速，恢复过程仅限于文件系统数据



NTFS的恢复支持

- 文件系统设计的演变
 - 谨慎写 (careful write) 文件系统
 - 对写操作进行排序
 - 即使系统失败，整个卷仍然处于一致和可用的状态
 - 延迟写 (lazy write) 文件系统
 - 把文件的修改写到缓存中，再刷新到磁盘
 - 使性能提高，但是风险更高



NTFS的恢复支持

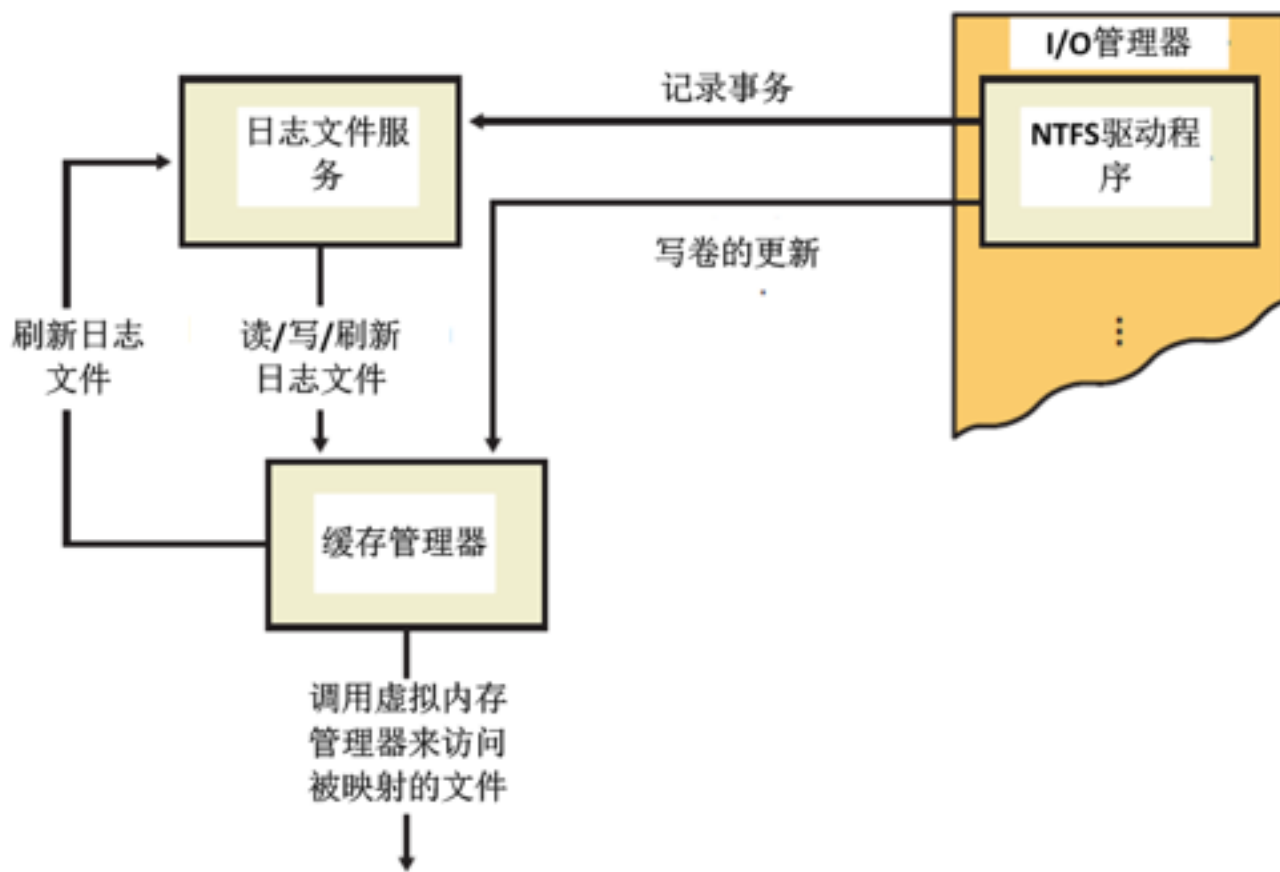
- 可恢复的文件系统

- 超过谨慎写文件系统的保险性，获得延迟写文件系统的性能优势
- 使用最初为事务处理发展起来的日志技术确保卷的一致性
- NTFS可恢复性确保其卷结构不会被破坏
- 在一次直写操作或者缓存刷新以后，用户数据将是一致的，并且立即可以使用



NTFS的恢复支持

- 日志记录





NTFS的恢复支持

- 日志文件服务 (LFS)
- 日志记录类型
 - 更新记录
 - 每一条记录包含重做信息和撤销信息
 - 创建，删除，扩充，截短，设置文件信息，重命名，改变文件的安全性
 - 检查点记录
 - 周期性的写入检查点记录
 - 用于回滚系统设置信息



NTFS的恢复支持

- 恢复

- 恢复过程依赖NTFS在内存中维护的两张表

- 事务表（记录启动但是未提交的事务）

- 脏页表（记录缓存中页面的未被写到磁盘上的修改信息）

- NTFS扫描日志文件三遍

- 分析扫描

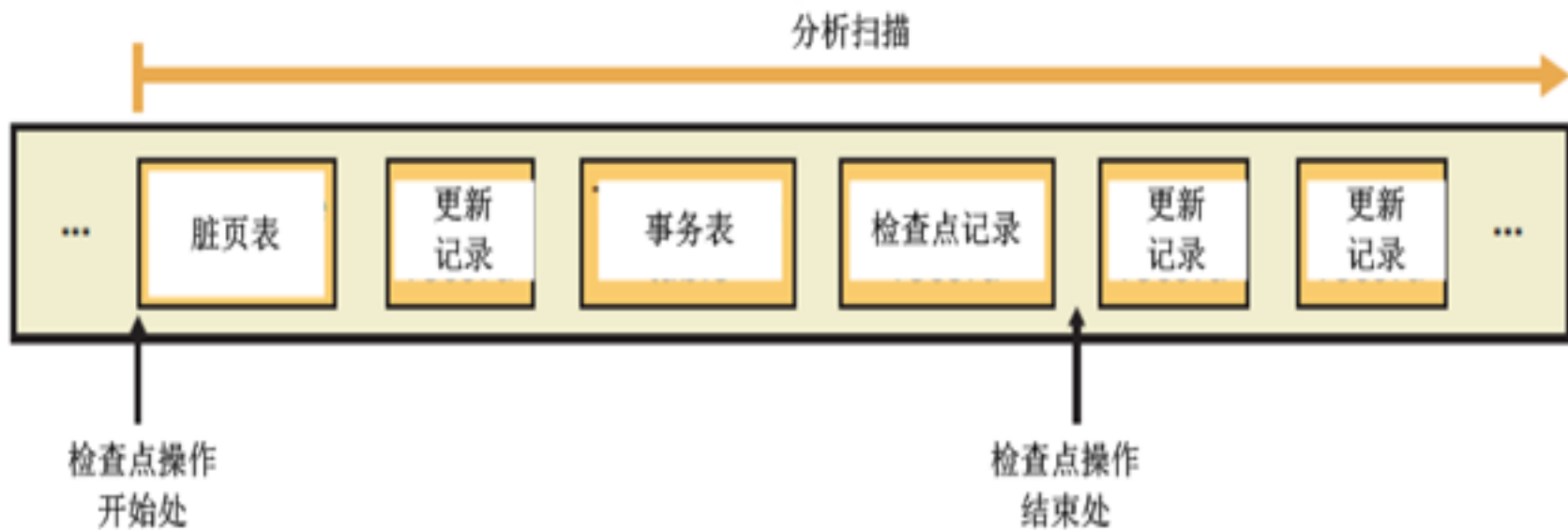
- 重做扫描

- 撤销扫描



NTFS的恢复支持

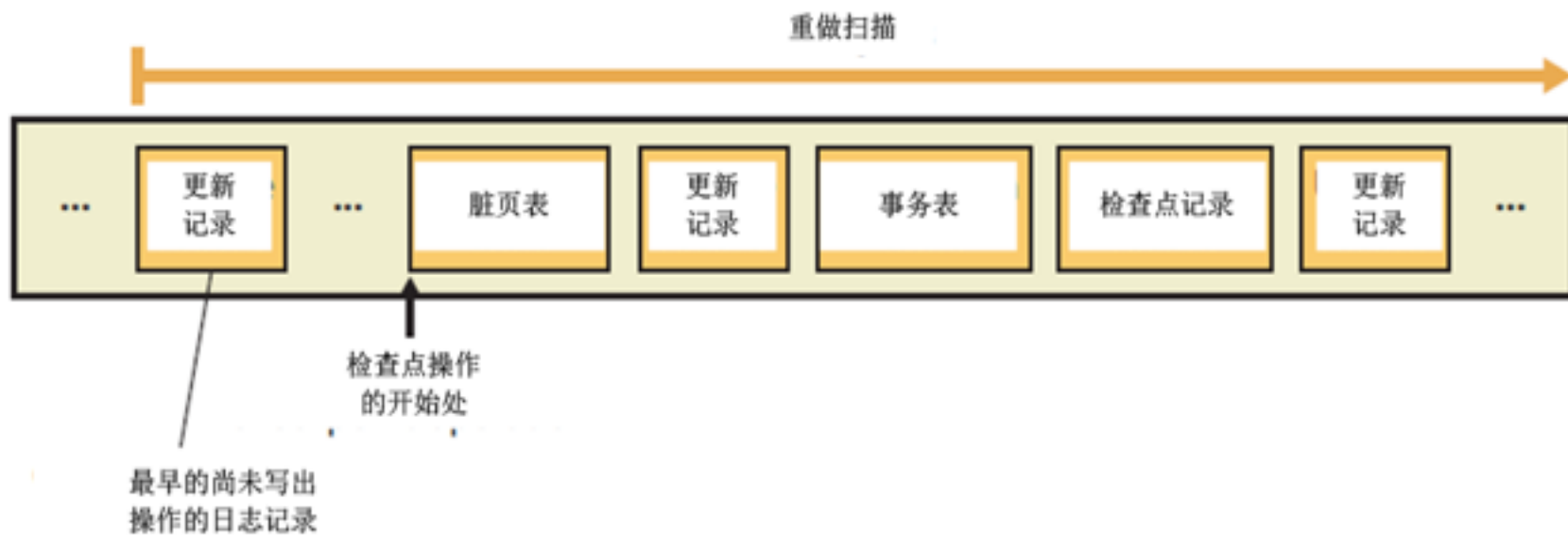
- 分析扫描





NTFS的恢复支持

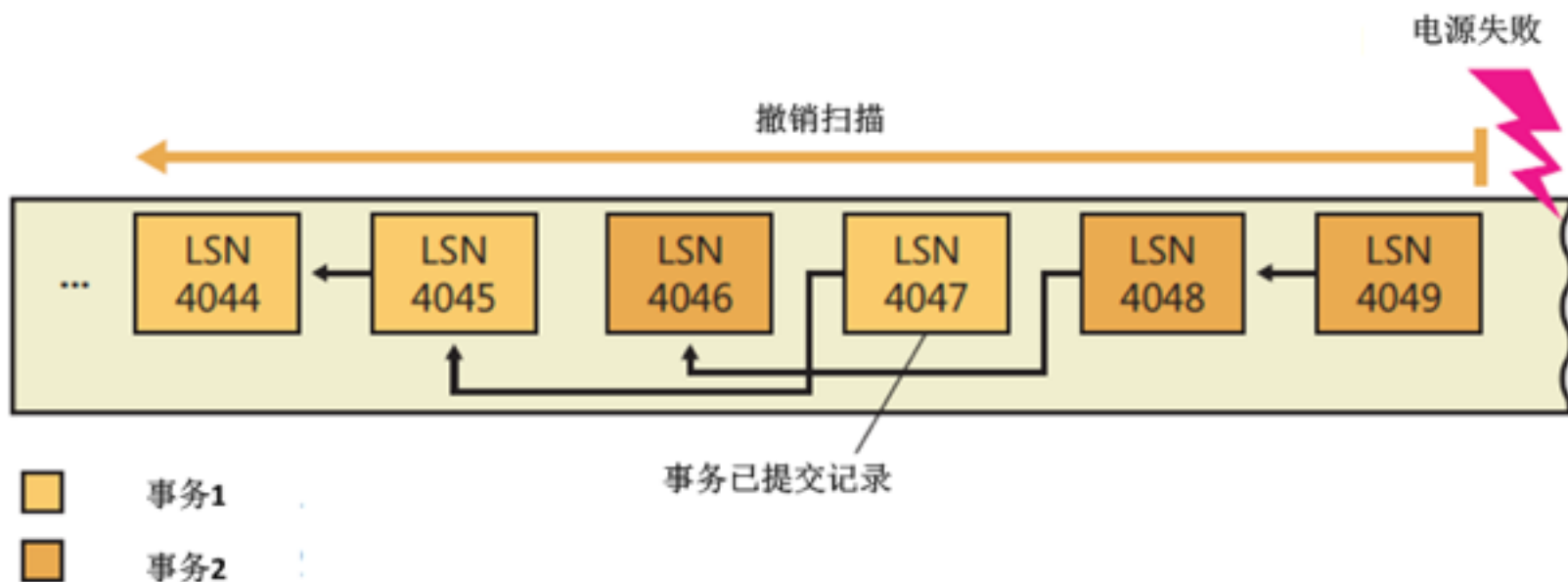
- 重做扫描





NTFS的恢复支持

- 撤销扫描





NTFS的恢复支持

- NTFS的坏簇恢复

- NTFS动态的替换掉包含坏扇区的簇，跟踪记录这一坏簇，以后不会重用

- 容错卷

- 恢复数据

- 替换掉坏扇区

- 非容错卷

- 不能恢复数据

- NTFS执行簇重映射，数据丢失



NTFS的恢复支持

- 自我恢复

- SET_REPAIR_ENABLED

- 开启卷的自我恢复功能

- SET_REPAIR_WARN_ABOUT_DATA_LOSS

- 如果文件不能完全恢复，是否通知用户

- SET_REPAIR_DISABLED_AND_BUGCHECK_ON_CORRUPTION

- 系统崩溃抛出0x24错误



本章内容提要

- 磁盘、分区和卷
- NTFS的恢复支持
- 误删除数据的手工恢复
- 数据备份方案
- 加密文件系统（EFS）的安全性



误删除数据的手工恢复

- 数据手工恢复的两种形式

- 硬恢复

- 硬盘出现物理性损伤，导致普通用户不能取出里面的数据，通过修理硬件的同时保留和恢复里面的数据

- 软恢复

- 硬盘本身没有物理损伤，由于人为或者病毒破坏造成数据丢失，通过软件进行数据恢复

- 本节介绍通过winHex软件进行数据软恢复的方法



误删除数据的手工恢复

- WinHex介绍

- 十六进制编辑软件

- 完善的分区管理功能和文件管理功能

- 自动分析分区链和文件簇链，对硬盘进行不同方式不同程度的备份，甚至克隆整个硬盘

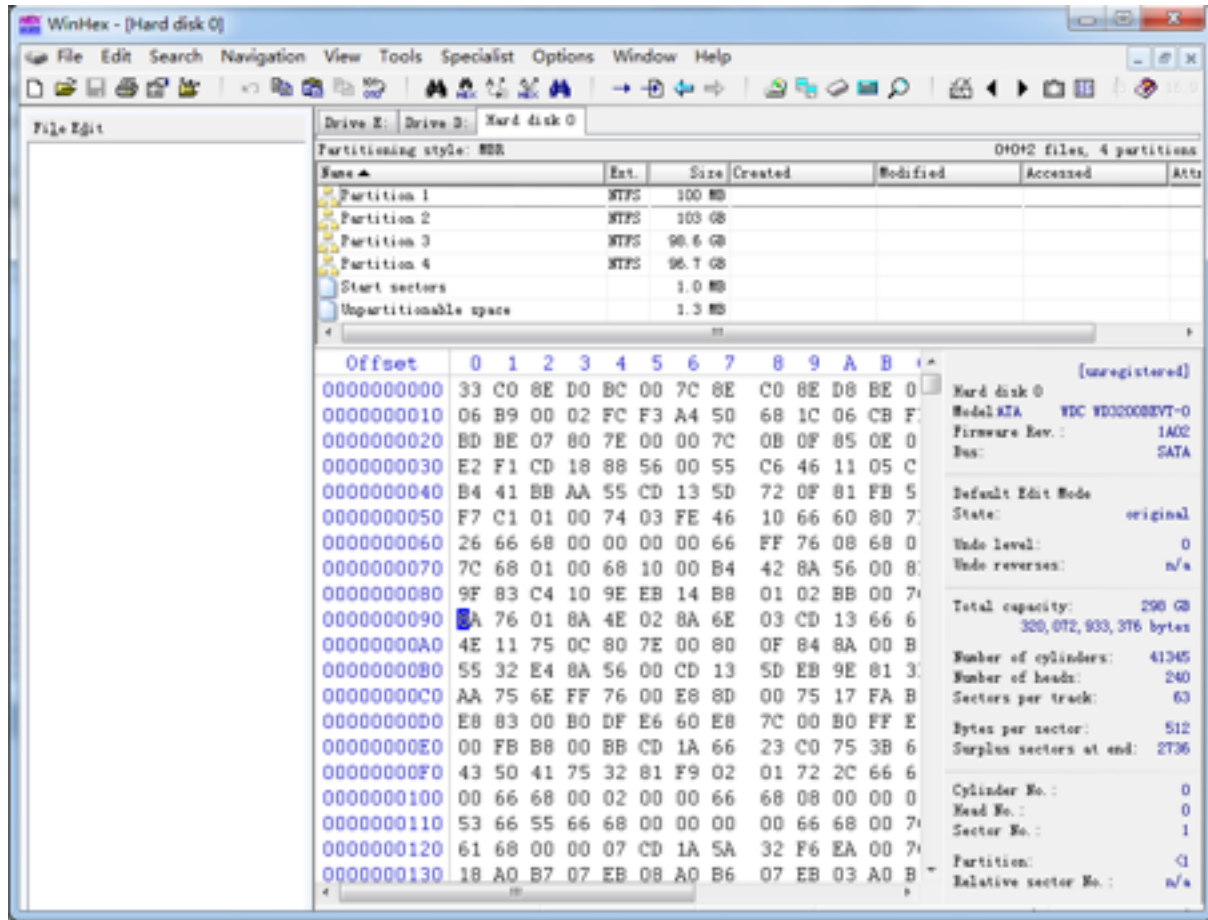
- 编辑任何一种文件类型的二进制内容

- 磁盘编辑器可以编辑物理磁盘或逻辑磁盘的任意扇区



误删除数据的手工恢复

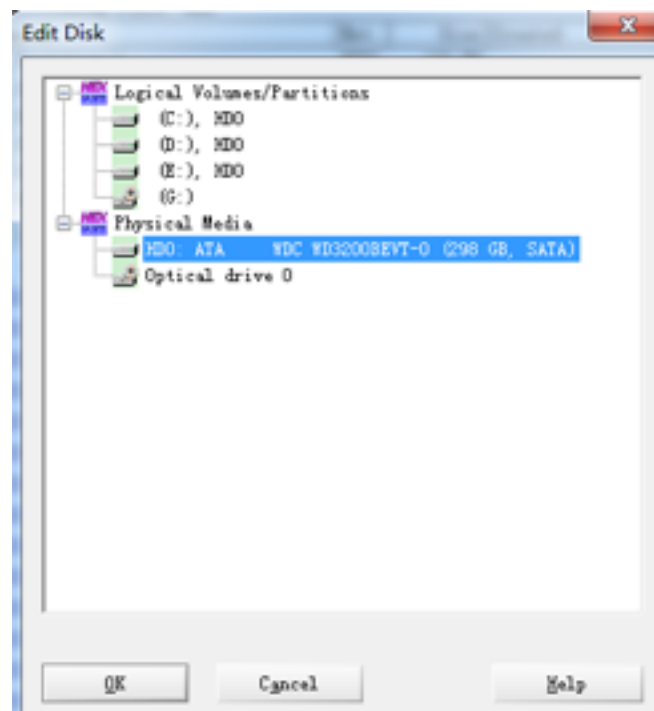
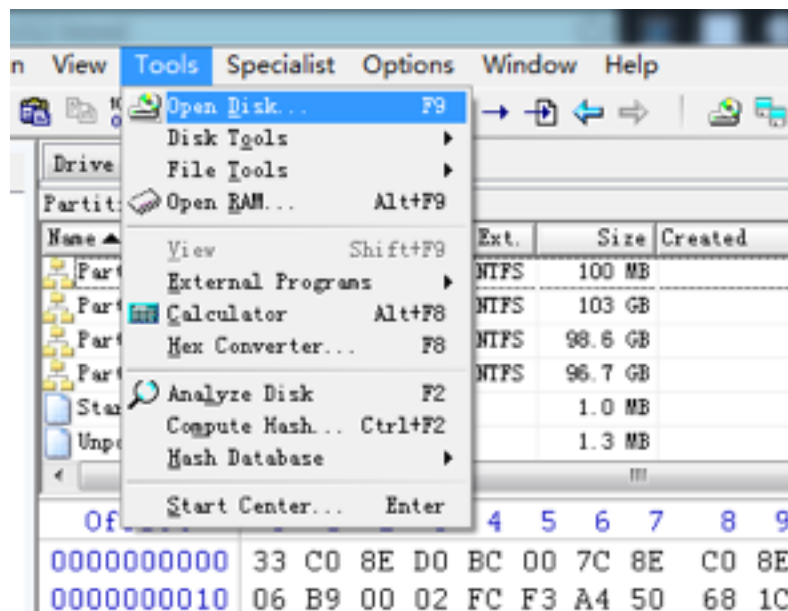
- WinHex主界面





误删除数据的手工恢复

- 可以选择对整个硬盘或者单独的分区进行恢复





误删除数据的手工恢复

- 界面的各部分信息类型

Partitioning style: MBR

Name	Ext.	Size	Created on	Modified	Accessed	Attr.	1st sector
Partition 1	NTFS	100 MB					2,048
Partition 2	NTFS	103 GB					208,848
Partition 3	NTFS	98.6 GB					215,5...
Partition 4	NTFS	96.7 GB					422,3...
Start sectors		1.0 MB					0
Unpartitionable space		1.3 MB					625,1...

硬盘分区情况

Offset: 0 1 2 3 4 5 6 7 8 9 A B C D E F 10 11 12 13

0000100924 83 C6 04 66 8B 04 A3 16 00 83 C6 04 1E 07 E8 E0 F7 66 2B F0 1E f1 E 1E 00=f+0

0000100938 0F 84 08 0D F7 26 0B 03 03 D8 E8 D9 66 8B 3E 6A 02 1E 07 E8 1 -G 00Uf1> j &

000010094C BF FD 66 A1 6A 02 66 B8 80 00 00 00 66 B9 00 00 00 00 66 B8 cyfij f=1 f: f1

0000100960 D1 E8 81 FB 66 0B C0 0F 84 FF F7 66 8B D8 66 58 66 56 E8 2C 8e 0f A 1y-f10XfV0.

0000100974 01 66 5E 66 0B C0 0F 84 05 00 66 5B 66 5B C3 66 59 66 5A E2 f~f A 1 f[f[ArYfZa

0000100988 84 66 33 C0 C3 06 1E 66 60 66 50 66 51 66 33 D2 66 0F B6 1E If3AA f~fPQf30f *

000010099C 0D 00 66 F7 F3 66 52 66 57 E8 53 FF 66 5F 66 0B C0 0F 84 B9 f~ofRfW0Syf_f A 1

00001009D0 F7 66 0F B6 1E 0D 00 66 F7 E3 66 5A 66 03 C2 66 A3 11 00 66 ~f * f~3fZf Arf f

00001009C4 59 66 0F B6 1E 0D 00 66 3B CB 0F 8E 13 00 89 1E 16 00 66 2B Yf * f:E 1 1 f~

00001009D8 CB 66 58 66 03 C3 66 50 66 63 FF 14 50 66 58 66 03 C1 66 50 EF0E ArPQ0 f0f Arf

00001009E0 00 0E 1E 00 66 50 00 00 66 63 FF 14 50 66 58 66 03 C1 66 50 * -f -f 0f 0f0f0f

0000100A00 0E C0 00 C1 E1 04 03 C7 58 07 E8 1E 07 00 3E 07 58 03 3E 32 ArAr: qf * f~ f~ f~

0000100A14 02 66 59 66 58 66 83 F9 00 0F 8F 70 FF 66 61 90 1F 07 C3 06 fYfXf1a pyfa A

0000100A28 1E 66 60 66 F7 26 56 02 66 8B 0E 56 02 E8 55 FF E8 D2 FC 66 f~f~GV f1 V 0Uy00uf

0000100A3C 61 90 1F 07 C3 06 1E 66 60 66 F7 26 72 02 66 0B 1E 36 02 66 e A f~f~Gr f1 6 f

0000100A50 8B 0E 72 02 66 8B 36 2A 02 1E 07 66 8B 3E 46 02 E8 81 FB E8 1 r f16* f1>F & 0a

0000100A64 A7 FC 66 61 90 1F 07 C3 66 50 66 53 66 51 66 8B 1E 4A 02 66 Sufe ArPfsQf1 J f

0000100A78 8B C8 66 C1 E8 03 66 83 E1 07 66 03 D8 66 B8 01 00 00 00 66 fER0a f1a f 0f, f

0000100A8C D3 E0 67 84 03 0F 84 04 00 F8 EB 02 90 F9 66 59 66 5B 66 58 0ag1 1 00 0fYf[fX

0000100AA0 C3 67 80 78 08 01 0F 84 04 00 66 2B C0 C3 67 66 8D 73 10 67 Ag1{ 1 f~AAgf a g

0000100AB4 66 8B 56 08 66 3B C2 0F 87 0B 00 67 66 8B 16 66 3B C2 0F 83 f1V f: A 1 g1 f: A 1

0000100AC8 04 00 66 2B C0 C3 67 03 5E 10 66 2B F6 67 80 3B 00 0F 84 3E f~AAg ~ f~0g1; 1>

0000100ADC 00 E8 81 00 66 03 F1 E8 39 00 66 03 CA 66 3B C1 0F 8C 21 00 e f 8e9 f Ef: A 11

0000100AF0 66 8B D1 66 50 67 66 0F B6 0B 66 8B C1 66 83 E0 0F 66 C1 E9 f1NfPgf * f1Af1a fA0

Hard disk 0 [unregistered]

Model: ATA YDC YD3200SEV7-0

Firmware Rev.: 1A02

Bur: 5A5A

Default Edit Mode

State: original

Undo level: 0

Undo reversion: n/a

Total capacity: 290 GB

320, 072, 933, 376 bytes

Number of cylinders: 41345

Number of heads: 240

Sectors per track: 63

Bytes per sector: 512

Surplus sectors at end: 2736

Cylinder No.: 0

Head No.: 32

Sector No.: 37

Partition: 1

Relative sector No.: 4

Mode: hexadecimal

Character set: CP 936

Offsets: hexadecimal

Bytes per page: 24x20=480

Sector 2082 of 625142448

Offset: 100988

= 102 | Block: n/a | Size: n/a



误删除数据的手工恢复

- 通过WinHex查看硬盘的MBR
 - MBR 是位于：0 扇区（逻辑扇区），大小为 512 bytes
 - 在 MBR 里的后 64 个字节里是磁盘的分区表结构，可定义 4 个分区，每个分区 16 bytes，从 0x1be ~ 0x1fe 共 64 bytes

位置 (hex)	大小 (bytes)	描述
000 - 162	354 bytes	硬盘 MBR 引导记录 (代码区)
162 - 1BD	92 bytes	MBR 数据区域
1BE - 1CD	16 bytes	分区表 1
1CE - 1DD	16 bytes	分区表 2
1DE - 1ED	16 bytes	分区表 3
1EE - 1FD	16 bytes	分区表 4
1FE - 1FF	2 bytes	MBR 标志 (55AA)



误删除数据的手工恢复

• 磁盘分区表结构

位置 (hex)	大小 (bytes)	意义	描述	
1BE	1	分区的启动标志	80 =	可启动分区
			00 =	不可启动区
1BF - 1C1	3	分区的起始扇区	1BF =	heads, 起始 heads (1 个 bytes)
			1C0 =	sector, 低 6 bits 表示起始 sector, 这里只用该节字的低 6 bits 来表示 sector
			1C1 =	cylinder, 1C0 的高 2 bits 加上 1C1 的 8 bits 组成 10 bits 表示起始 cylinder
1C2	1	文件系统	如: 07 表示 ntfs 系统, 详见: 文件系统	
1C3 - 1C5	3	分区的结束扇区	其意义和起始扇区一致	
1C6 - 1C9	4	此分区前扇区数	这 4 bytes 表示此分区前有多少扇区 (实际上等于此分区的起始扇区号), 以 little-endian 排列的。	
1CA - 1CD	4	此分区扇区数	这 4 bytes 用来表示此分区共有多少扇区, 同样是以 little-endian 排列的。	



误删除数据的手工恢复

- 以第一分区表为例

000000001A4	65 72 61 74 69 6E 67 20 73 79 73 74 65 6D 00 00 00 63 7B 9A	erating system c{I
000000001B8	02 1C B5 DF 00 00 80 20 21 00 07 A3 13 0D 00 08 00 00 00 20	µß ! £
000000001CC	03 00 00 A3 14 0D 07 EF FF FF 00 28 03 00 00 C0 D5 0C 00 EF	£ iyy (Å Õ i
000000001E0	FF FF 07 EF FF FF 00 E8 D8 0C 00 38 54 0C 00 EF FF FF 07 EF	yy iyy è0 8T iyy i
000000001F4	FF FF 00 20 2D 19 00 C0 15 0C 55 AA 00 00 00 00 00 00 00 00	yy - Å Ua
00000000208	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
0000000021C	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	



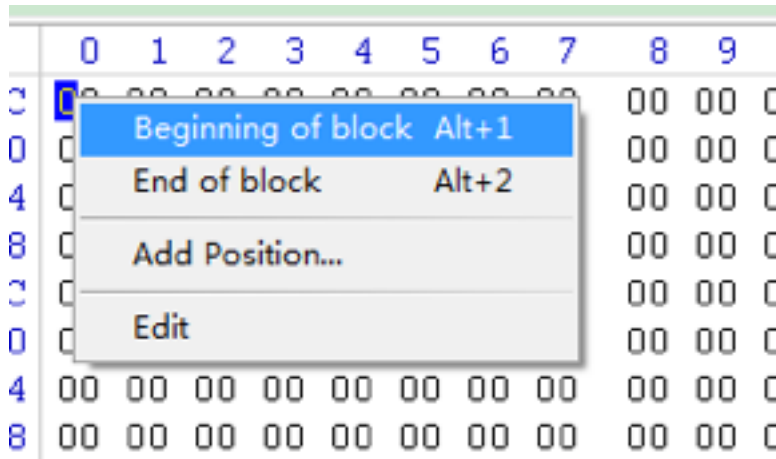
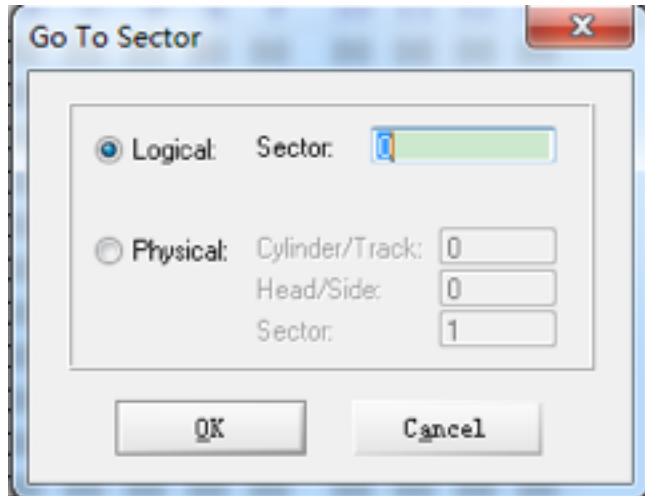
误删除数据的手工恢复

000001BE 80	可启动分区	000001BF
20	起始 header 号	
000001C0 21	起始 sector 号	
000001C1 00	起始 cylinder 号	000001C2
07	NTFS 格式	
000001C3 DF	结束 header 号	
000001C4 13	结束 sector 号	
000001C5 0C	结束 cylinder 号	
000001C6 00080000	此分区前的扇区总数	
000001CA 00200300	此分区的扇区总数	



误删除数据的手工恢复

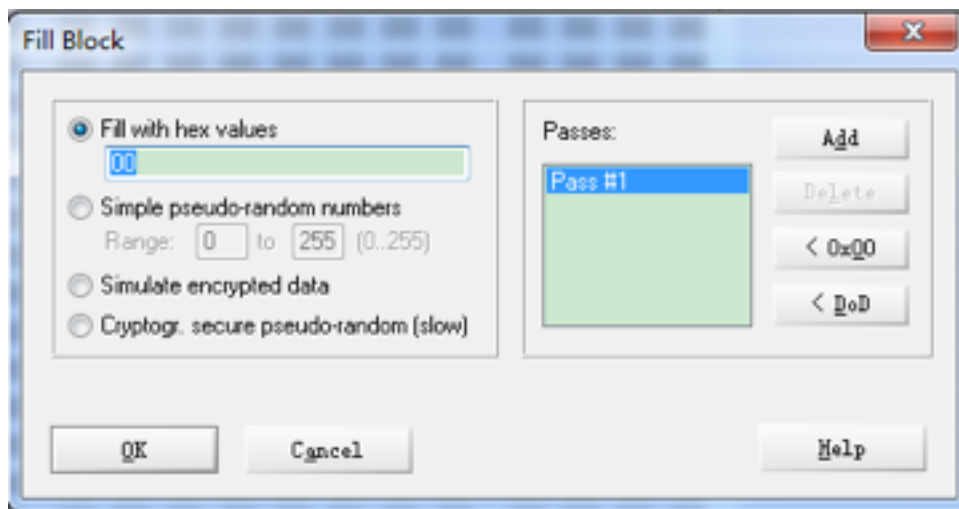
- 通过计算就可以转到对应的扇区进行处理
- 在需要编辑的位置右键开始对选块进行选择





误删除数据的手工恢复

- 使用填充数据或者复制剪贴板的数据来对选定的数据块进行修改





本章内容提要

- 磁盘、分区和卷
- NTFS的恢复支持
- 误删除数据的手工恢复
- 数据备份方案
- 加密文件系统（EFS）的安全性



数据备份方案

- 数据备份对于个人和企业用户都是至关重要的，数据本身的脆弱性或者丢失或者损坏会直接的威胁到用户的利益
- 目前威胁数据安全的因素
 - 系统的漏洞
 - 系统的硬件故障
 - 人为的操作失误
 - 供电系统故障
 - 网络的非法访问



- 正常备份模式

- 优点是自动筛选备份文件

- 缺点是效率不高，费时

- 对需要备份的文件在文件属性中标记为存档，当执行备份操作时，对标记过的文件进行备份操作，备份之后自动取消“存档”属性

- 若文件没有被改动过，则在备份时会自动跳过



- 副本备份模式
 - 优点是备份快速
 - 缺点是备份的方式是非智能的
 - 只是简单的将备份的目标文件复制下来，作为副本添加到备份文件中
 - 采用副本备份模式执行备份操作后，目标文件的“存档”属性不受影响



- 增量备份模式

- 优点是有针对性，速度快

- 缺点是备份的数据份数较多

- 对于需要反复修改的文件比如设计图或者文档等，增量备份是最佳的备份方式

- 对发生变化的文件根据修改的顺序依次进行备份



- 差异备份模式

- 优点是恢复速度快

- 缺点是占用空间

- 差异备份和增量备份在第一次使用时都需要配合完整的普通备份，针对新建或修改的文件

- 若文件自上次完整备份后曾被更新过，接下来每次做差异备份时，都会被备份，直到下次完整备份

- 差异备份的大小会随时间不断增加



- 每日备份模式

- 优点是无需干预，自动备份

- 缺点是占用空间

- 每日备份模式省去了手动备份重要文件的操作，添加计划任务就可以

- 每日备份模式的目标是当天创建或修改的文件



数据备份方案

- Windows 自带的备份工具
- 在系统的“控制面板”中“备份和还原”选项





数据备份方案

- 备份和还原的主界面，点击“更改设置”进行备份的设置

备份或还原文件

备份

位置:

(D:)

立即备份(B)



78.83 GB 可用，共 98.63 GB

备份大小: 80.49 MB

管理空间(M)

下一次备份:

2013/2/24 19:00

上一次备份:

2013/2/19 16:34

内容:

库中的文件和所选用户的个人文件夹

计划:

每星期日的 19:00

更改设置(C)

还原

可以还原在当前位置备份的文件。

还原我的文件(R)

还原所有用户的文件(A)

选择要从中还原文件的其他备份(N)

恢复系统设置或计算机(Y)





数据备份方案

- 选择备份数据的位置，可以选择上传到网络服务器
- 下一步选择需要备份的目标文件

选择要保存备份的位置

建议将备份保存到外部硬盘上。 [备份目标选择指南](#)

保存备份的位置(B):

备份目标	可用空间	总大小
 本地磁盘 (D:)	78.83 GB	98.63 GB
 本地磁盘 (E:)	21.41 GB	96.68 GB

刷新(R)

保存在网络上(V)...

您希望备份哪些内容?

☐ 让 Windows 选择(推荐)

Windows 将备份保存在库、桌面和默认 Windows 文件夹中的数据文件。将定期备份这些项目。
[Windows 如何选择要备份的文件?](#)

☒ 让我选择

可以选择库和文件夹，以及是否在备份中包含系统映像。将定期备份所选项目。

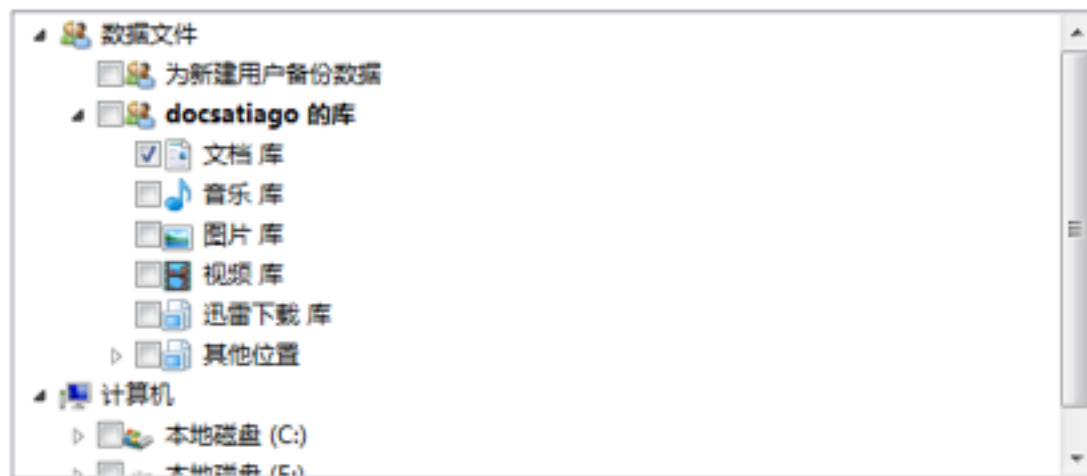


数据备份方案

- 选择备份的数据

您希望备份哪些内容？

选中要包含在备份中的项目对应的复选框。[默认情况下从备份中排除哪些文件？](#)



☐ 包括驱动器 系统保留, (C:), (D:) 的系统映像(S)

选定备份位置不支持创建系统映像。



- 添加备份计划

您希望多久备份一次？

根据您在下面设置的计划，会将自上次备份后已更改的文件和新创建的文件添加到备份中。

☒ 按计划运行备份(推荐)(S)

频率(H): 每周

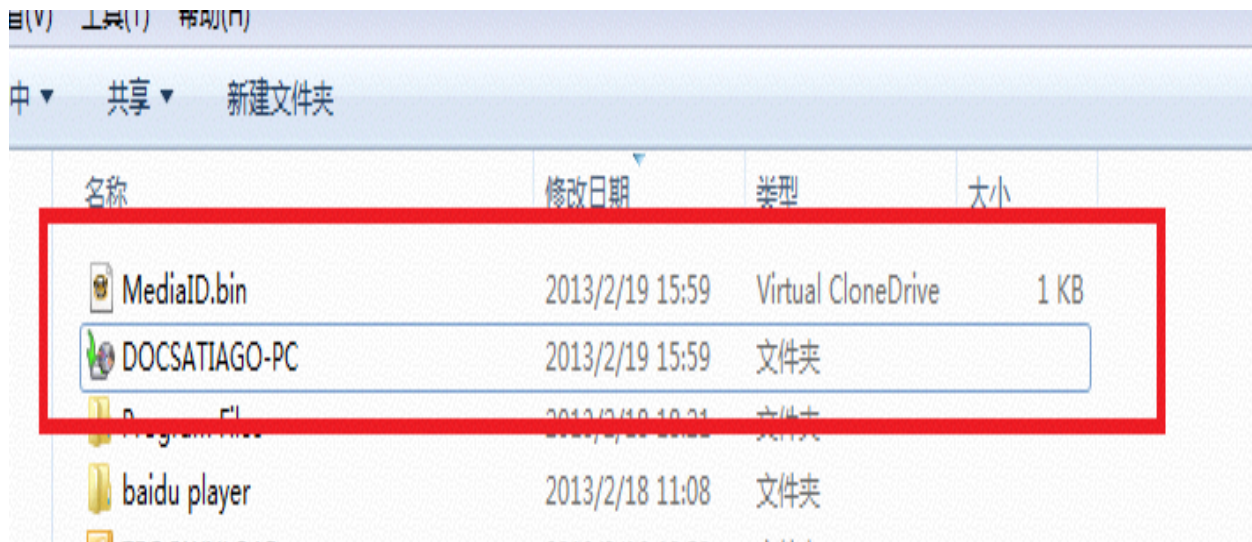
哪一天(W): 星期日

时间(T): 19:00



数据备份方案

- 备份文件保存在指定的磁盘中





本章内容提要

- 磁盘、分区和卷
- NTFS的恢复支持
- 误删除数据的手工恢复
- 数据备份方案
- 加密文件系统（EFS）的安全性



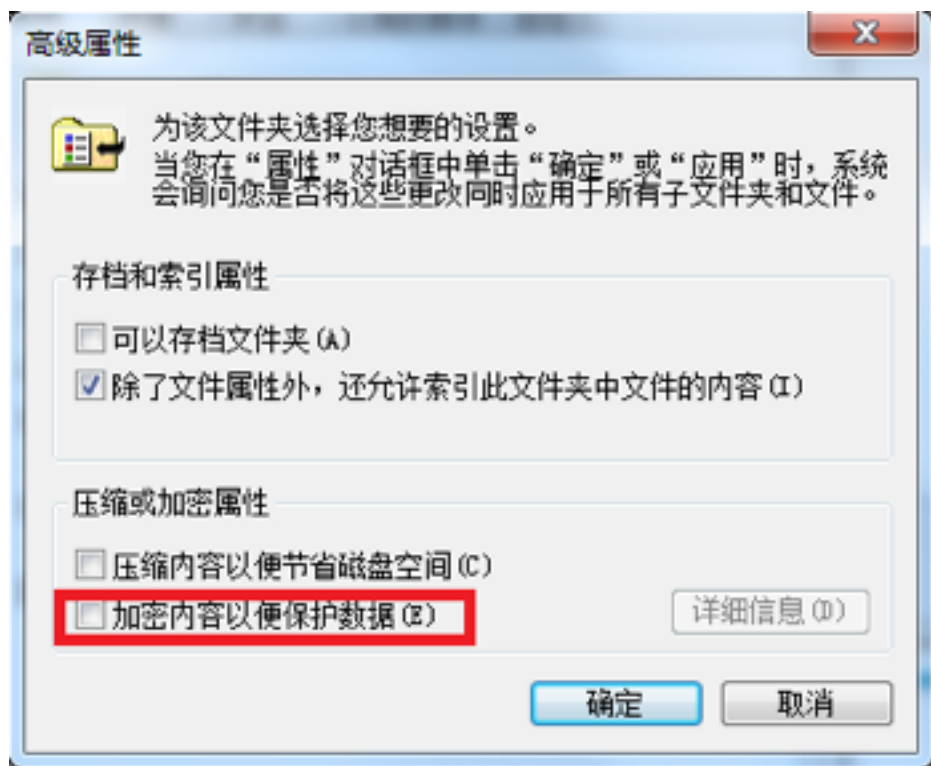
加密文件系统（EFS）的安全性

- EFS的安全性依赖于密码学支持。当一个文件被加密时，EFS为执行此次加密的用户账户分配一对私钥/公钥，以便在加密过程中使用
- 一个文件被加密时，EFS为该文件生成一个随机数，作为文件加密密钥（FEK）
- 加密算法：DES算法的更强变形
- Windows 2000：DESX
- Windows XP及以上：DESX，3DES，AES



加密文件系统（EFS）的安全性

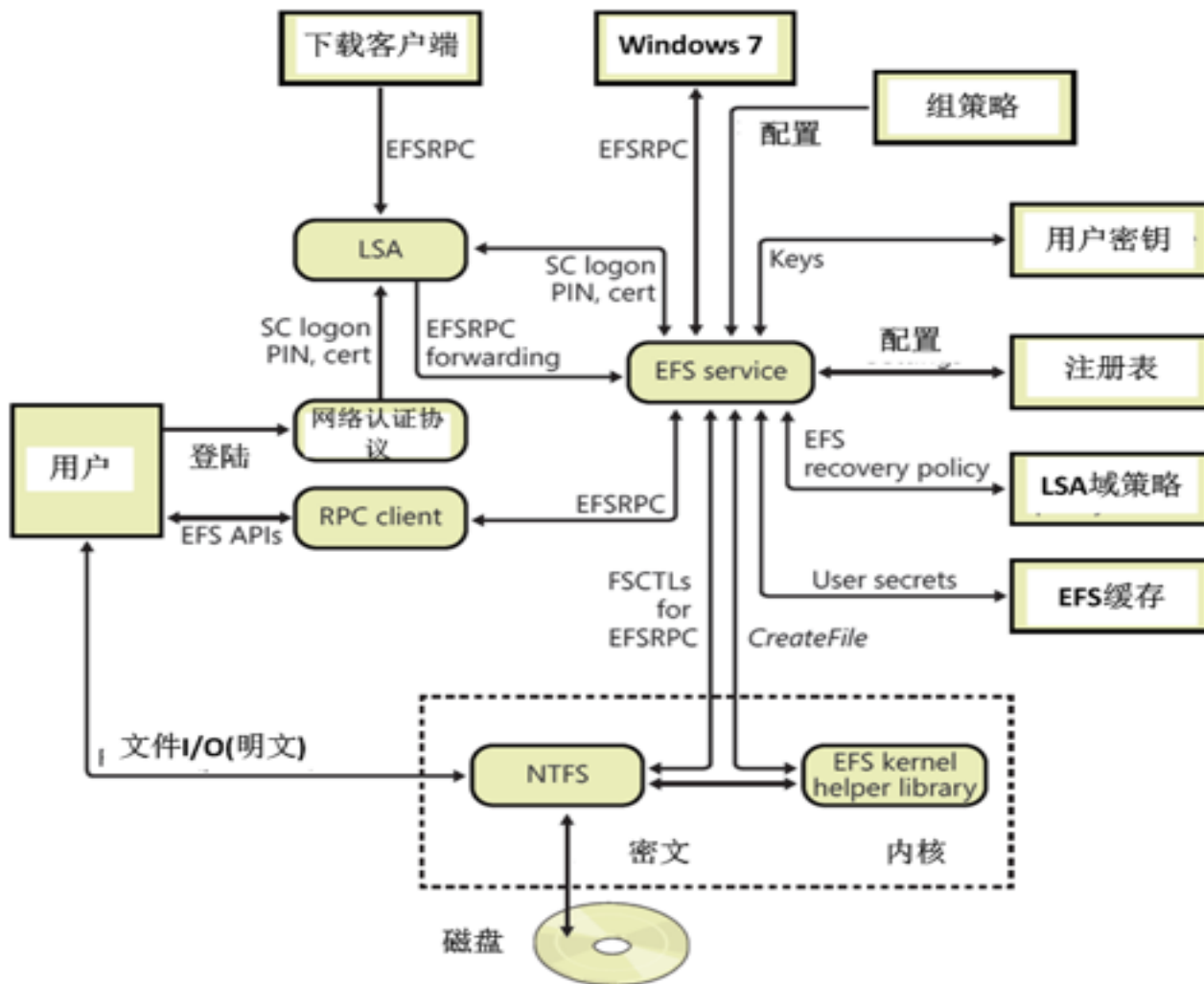
- 使用windows对话框来加密文件





加密文件系统（EFS）的安全性

- EFS的架构





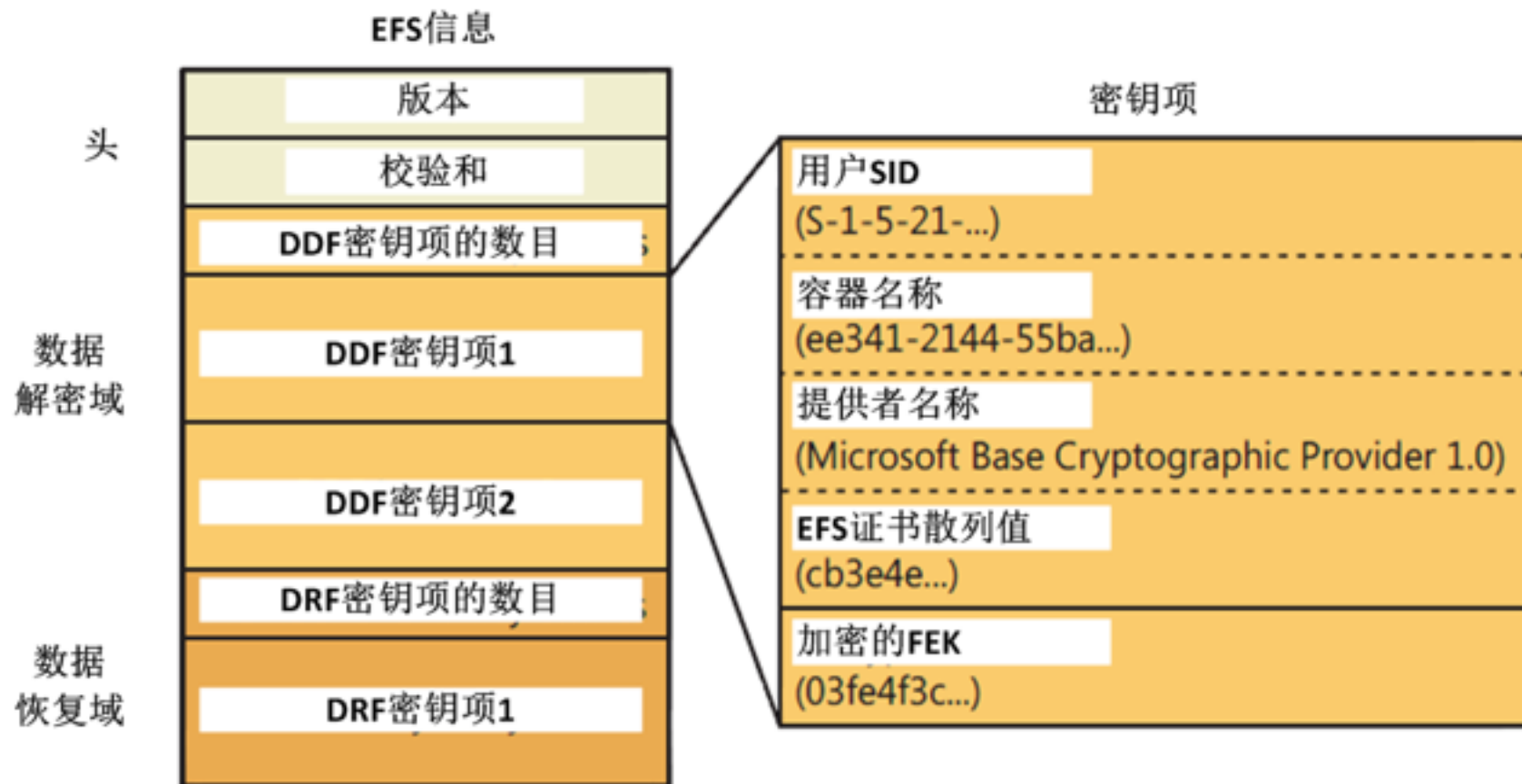
加密文件系统 (EFS) 的安全性

- NTFS驱动程序碰到加密文件时，调用EFS的函数，依赖于Advapi32.dll导出的EncryptFile Windows API函数
- LSASS(本地安全权威子系统)不仅负责管理登陆会话，而且处理与EFS密钥相关的杂务，Lsassrv(LSASS的本地安全权威服务器)组件在监听远过程调用 (RPC) 请求，使用CryptoAPI中的函数来解密此FEK
- CryptoAPI包含了密码服务提供者 (CSP) DLL，使得各种密码服务为应用程序所使用



加密文件系统（EFS）的安全性

- EFS信息格式和密钥项格式





加密文件系统（EFS）的安全性

- 加密过程

- 应用程序请求将数据写到一个加密文件中
- NTFS把数据放在文件系统缓存中
- 缓存管理器延迟把数据写到磁盘
- NTFS请求EFS驱动程序，把将要写到磁盘上的文件内容进行加密
- NTFS将加密的文件写到磁盘上



加密文件系统（EFS）的安全性

- 解密过程

- NTFS识别加密的文件发送请求到EFS驱动程序
- EFS返回DDF（数据解密域）传递到EFS服务器
- EFS服务器返回用户的私钥并解密DDF获得FEK
- EFS服务器传递FEK到EFS驱动程序
- EFS驱动程序利用FEK解密程序需要的文件部分



加密文件系统（EFS）的安全性

- 加密文件的备份
 - 备份工具不必具备解密文件数据的能力，在其备份过程中无需解密文件数据
 - 备份工具使用EFS API函数
OpenEncryptedFileRaw, ReadEncryptedFileRaw, WriteEncryptedFileRaw和CloseEncryptedFileRaw来访问一个文件的加密内容



加密文件系统（EFS）的安全性

- 复制加密文件

- 当加密文件被复制时，系统并不解密文件再重新加密文件到指定的地址，仅仅拷贝加密的数据和EFS交换数据流到指定的地址
- 复制的地址必须支持加密文件格式，如果不支持，EFS交换数据流将丢失，导致文件只能以非加密的形式被复制



课后实验

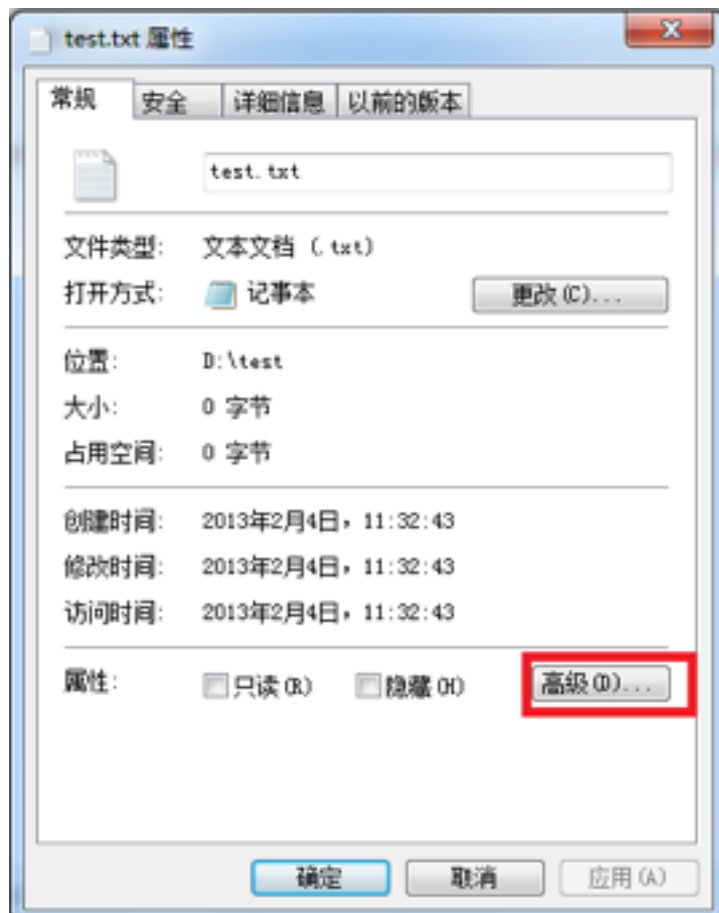
- 实验一 通过界面EFS加密文件





课后实验

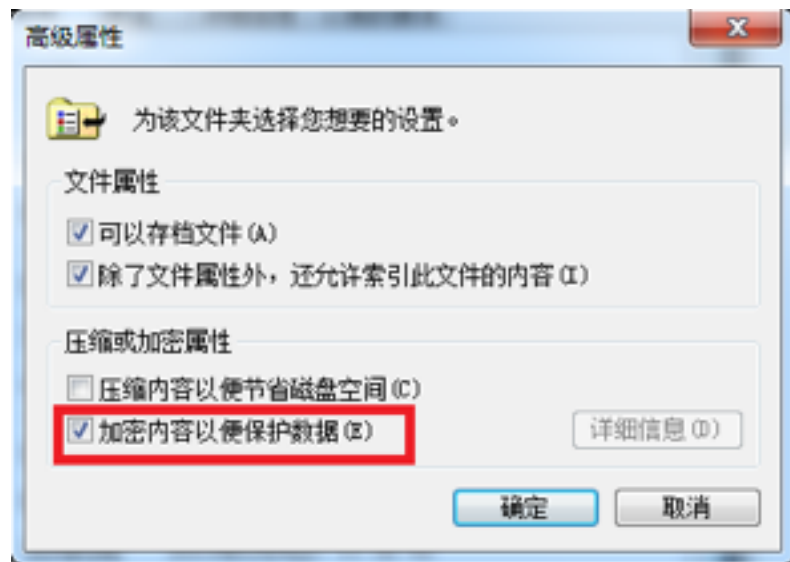
- 点击“高级”按钮





课后实验

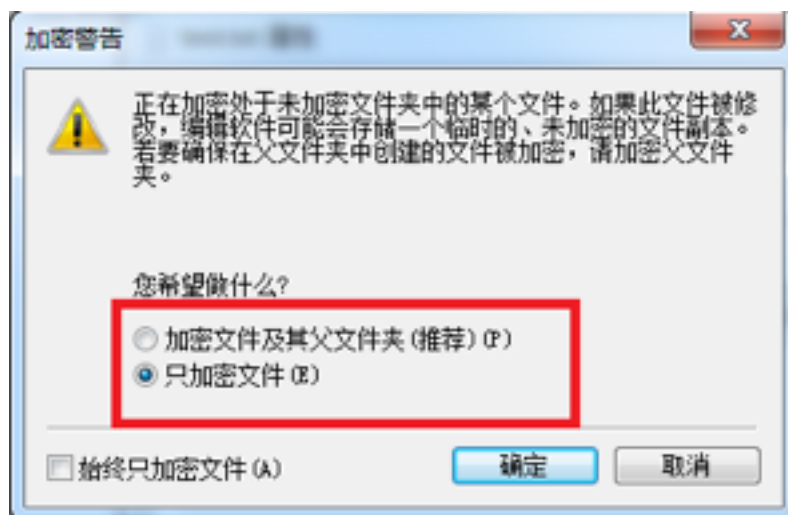
- 在“加密内容以便保护数据”选项前勾选





课后实验


- 点击确定后，根据需求选择加密的方式，点击“确定”





课后实验

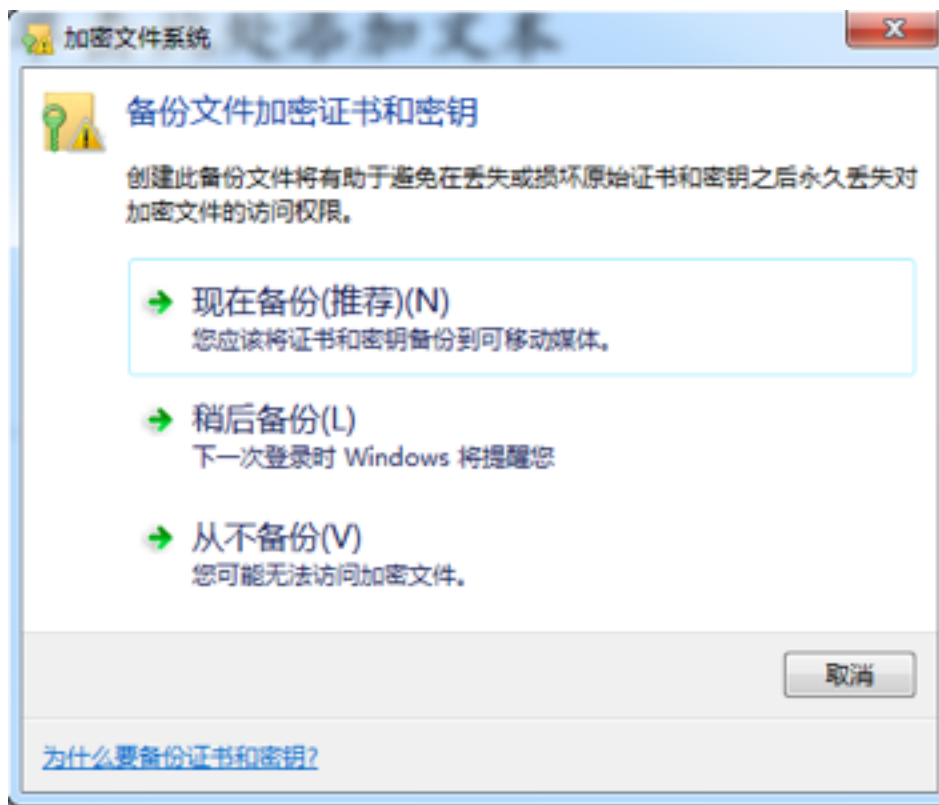
- 加密后的文件颜色发生变化

名称	修改日期	类型	大小
 test.txt	2013/2/4 11:32	文本文档	0 KB



课后实验

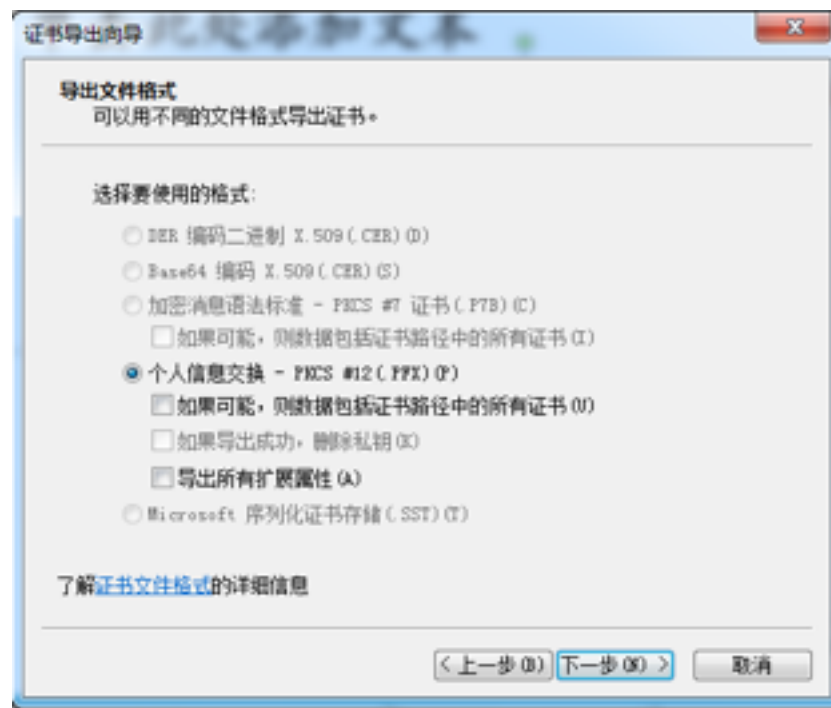
• 实验二 备份文件加密证书和密钥





课后实验

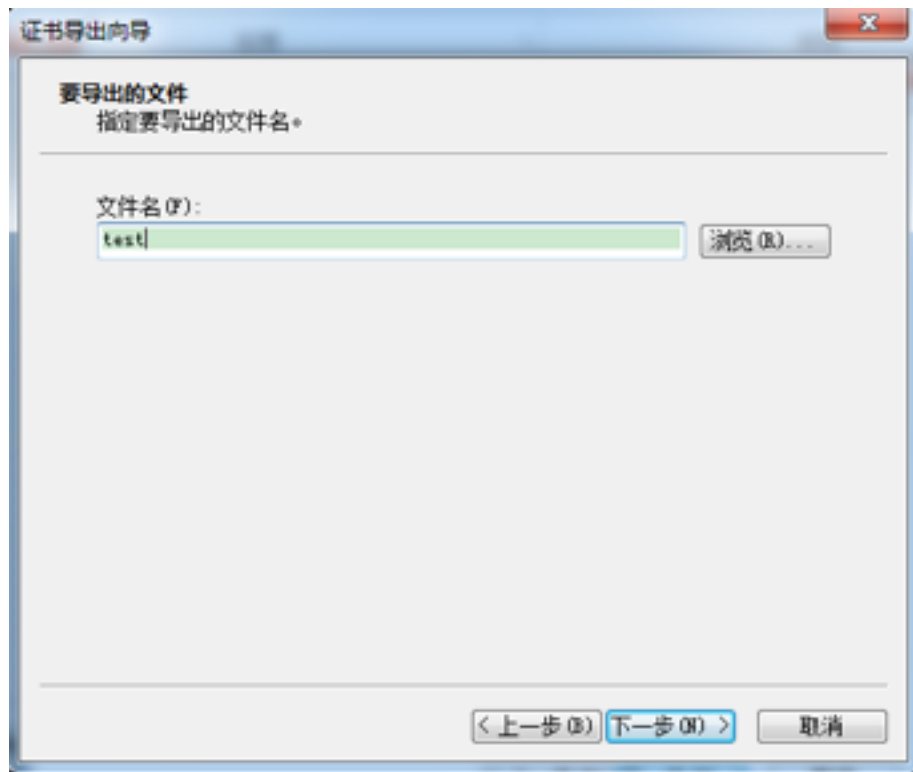
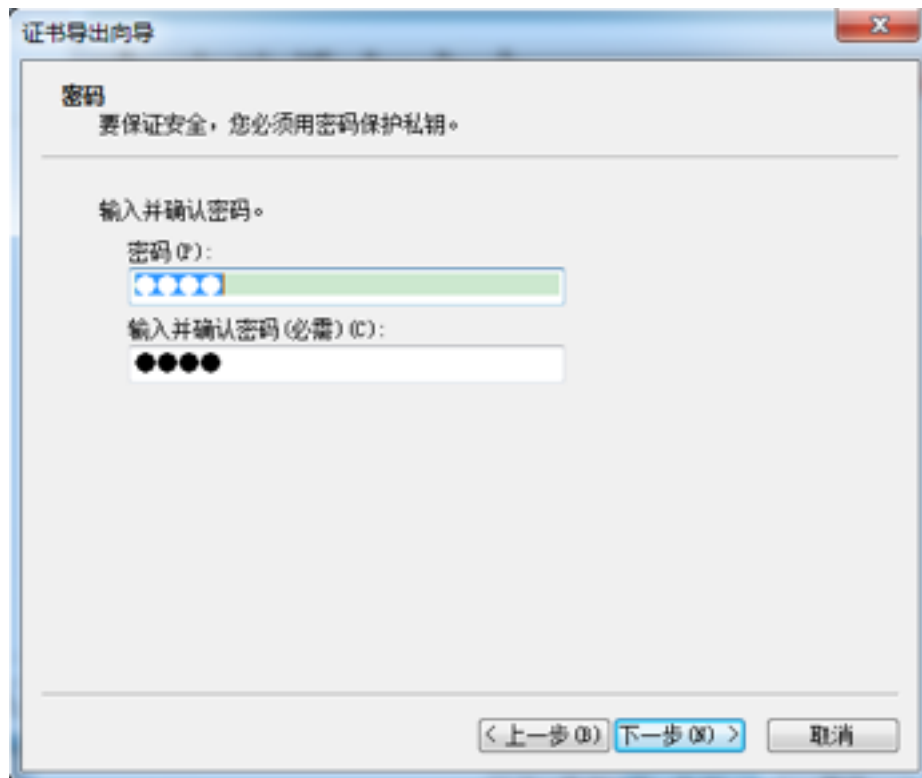
- 证书导出，选择导出的格式





课后实验

- 填写密码和导出证书的文件名





课后实验

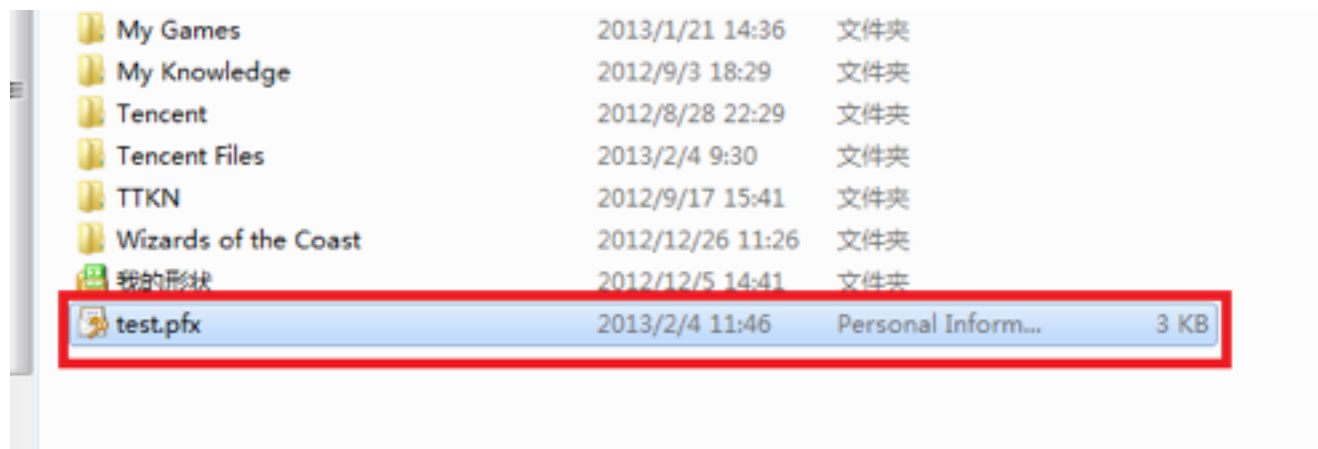
- 导出的证书文件

My Games	2013/1/21 14:36	文件夹	
My Knowledge	2012/9/3 18:29	文件夹	
Tencent	2012/8/28 22:29	文件夹	
Tencent Files	2013/2/4 9:30	文件夹	
TTKN	2012/9/17 15:41	文件夹	
Wizards of the Coast	2012/12/26 11:26	文件夹	
我的形状	2012/12/5 14:41	文件夹	
test.pfx	2013/2/4 11:46	Personal Inform...	3 KB



课后实验

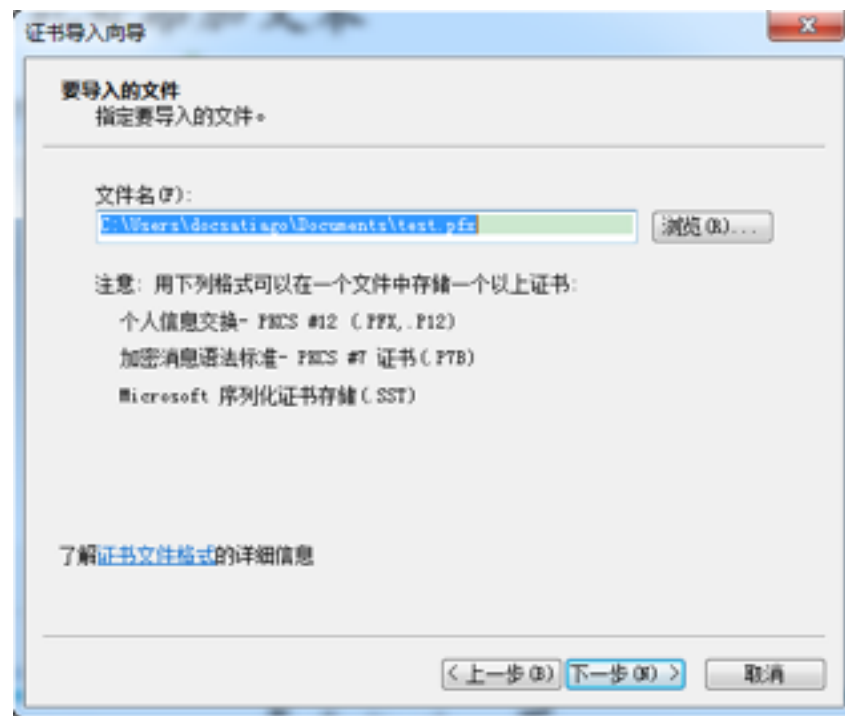
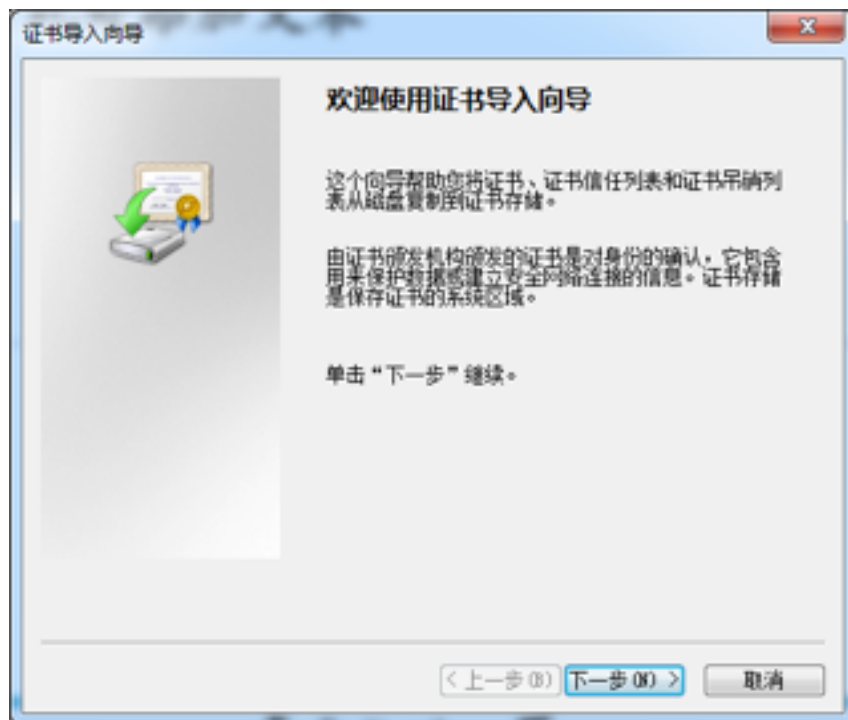
- 实验三 导入备份的加密密钥





课后实验

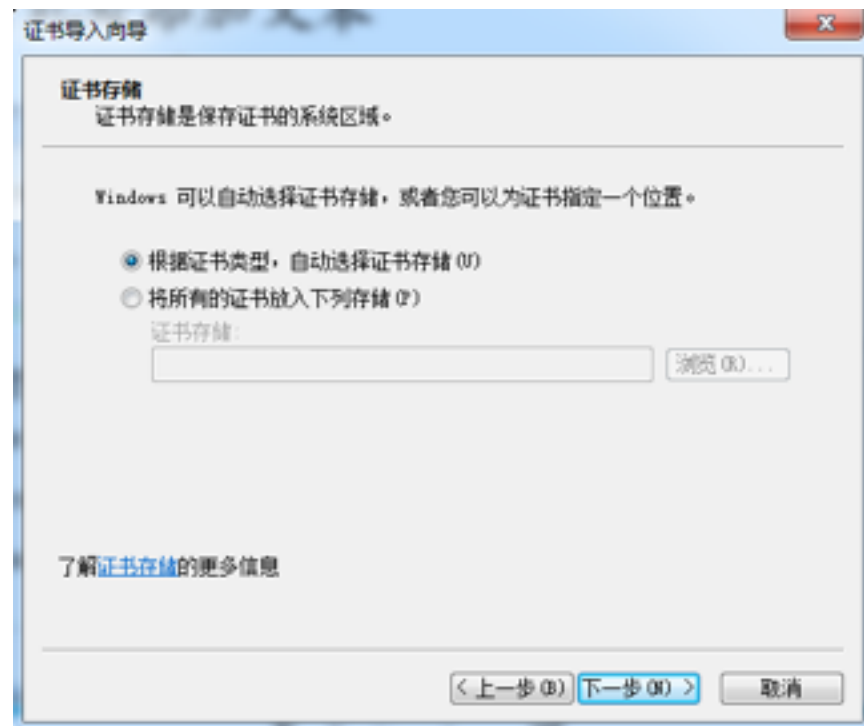
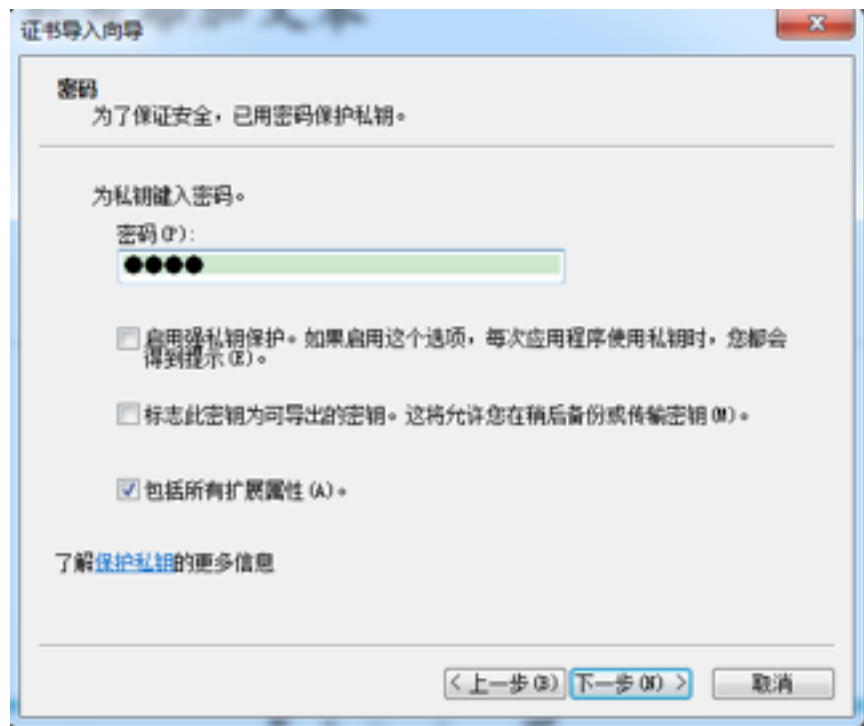
- 导入选择的证书文件





课后实验

- 输入导出时输入的密码，选择证书导入的位置





课后实验

- 确定设置无误后，点击“完成”

