

<<识数寻踪>>

图书基本信息

书名：<<识数寻踪>>

13位ISBN编号：9787115297211

10位ISBN编号：7115297215

出版时间：2013-1

出版时间：人民邮电出版社

作者：高志鹏，张志伟，孙云峰 编著

页数：314

字数：531000

版权说明：本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问：<http://www.tushu007.com>

前言

随着硬盘存储技术的发展，电脑硬盘的容量已达到TB级。对企业和个人而言，存储在硬盘上的数据，从普通的文档、电子相片到珍贵的视频、财务数据，包罗万象。

由于各种原因，如恶意程序入侵、用户误操作、硬盘物理损坏等，导致数据丢失的现象不断发生。为了尽可能把因数据丢失而带来的经济损失降到最低，数据恢复成为数据安全重要的避难所。

如今市面上常用的数据恢复软件有WinHex、R-Studio、EasyRecover、FinalData等。R-Studio、EasyRecover和FinalData等软件虽然操作简单易用，但同时也失去了数据恢复的灵活性。在常用的数据恢复软件中，WinHex以文件体积小、运行高效和操作灵活而著称，它既有十六进制文件编辑功能，也有磁盘编辑的功能，对手动恢复删除文件、手动修复硬盘损坏具有非常好的效果，得到了国外著名媒体ZDNetSoftwareLibrary五星的最高评价。在数据恢复和电子取证行业内，WinHex的角色有点类似操作系统中的Linux，用户可以利用其强大的脚本与API功能，灵活高效地完成许多数据恢复工作。

虽然现在市面上已经有一些数据恢复的书籍，但大多数图书都是讲解文件系统的原理与数据恢复的实践，对于初学者来说过于理论化、也过于深奥。

目前，数据恢复和电子取证行业针对WinHex的培训书籍非常匮乏，很多初学者无法自如地、充分地利用WinHex强大的数据恢复功能，而有志于数据恢复技术研究的人士也不知如何利用WinHex研究文件系统、研究文件结构。

本书的推出可谓正逢其时，不仅有助于读者对WinHex的深入理解和实际应用，而且有助于爱好者研究文件系统，从业者开发数据恢复软件，因此，本书的面世对整个数据恢复行业来说都具有不可忽视的、深远的意义。

.....

<<识数寻踪>>

内容概要

《识数寻踪：WinHex应用与数据恢复开发秘籍》根据WinHex菜单来划分章节，详细描述了WinHex的全部功能和使用方法，对于那些晦涩难懂的知识点，利用编写实验代码的方式直观地展示其原理。

《识数寻踪：WinHex应用与数据恢复开发秘籍》还揭示了WinHex脚本编程及WinHex API函数的秘密，这在相关图书中是很难得的。

最后，本书以SQL Server数据库页组合技术为案例回顾了部分所学内容。

《识数寻踪：WinHex应用与数据恢复开发秘籍》以WinHex的功能模块为线索，看似讲述操作技法，实则探讨数据恢复技术的研究思路，旨在拓宽读者视野，引发读者的兴趣，适合数据恢复工程师、数据恢复程序员、数据恢复研究人员、高校教师、电子取证工程师、技术支持工程师等读者阅读。

<<识数寻踪>>

作者简介

高志鹏，网名“困惑的浪漫”，著名数据恢复教程业余写手，数据恢复技术专家。

好文史，学计算机乃半路出家。

做过售后服务，也当过高校老师，现任高级研发工程师，从事信息安全相关领域的技术研发工作。

张志伟，计算机网络专业出身，高级研发工程师。

在嵌入式Linux开发领域打拼多年，遇到问题爱钻研，对项目管理和手机开发有独到见解。

与数据恢复有不解之缘，参与设计相关发明专利数个。

孙云峰，清华大学软件工程硕士，高级研发工程师。

山东汉子，憨厚耿直，所学颇丰。

擅长单片机和嵌入式Linux开发，喜欢为自己的iPhone设计应用程序，对数据恢复技术可谓一见如故。

<<识数寻踪>>

书籍目录

第1章 学海茫茫孤帆冷——数据恢复概述

- 1.1 给所有数据恢复工程师的话
 - 1.1.1 为什么选择数据恢复这个行业
 - 1.1.2 学习数据恢复需要什么基础
 - 1.1.3 数据恢复行业的现状
- 1.2 学习规划
 - 1.2.1 勤奋
 - 1.2.2 机遇
 - 1.2.3 自爱
- 1.3 数据恢复技术未来的发展方向
 - 1.3.1 FLASH数据提取技术
 - 1.3.2 数据恢复与残余数据分析并存
 - 1.3.3 数据恢复“云”
 - 1.3.4 数据恢复与人工智能
- 1.4 我们的“闺蜜”——数据恢复工具
 - 1.4.1 易学易用的R-Studio
 - 1.4.2 “闪电侠” Handy Recovery
- 1.5 数据恢复研究过程
 - 1.5.1 七个问题
 - 1.5.2 一个案例
 - 1.5.3 以Ext2为饵
 - 1.5.4 一个开源数据恢复软件项目

第2章 柳叶弯刀锋芒现——WinHex初探

- 2.1 面由心生——WinHex启动中心
 - 2.1.1 你是否对它一见钟情
 - 2.1.2 功能猜猜看
- 2.2 WinHex主界面
 - 2.2.1 叫谁谁回答的窗口标题栏
 - 2.2.2 一次疯狂的点菜——WinHex菜单栏和工具栏
 - 2.2.3 第一次编辑小心伤了自己——编辑窗口
 - 2.2.4 口若悬河的信息面板
 - 2.2.5 谁动了我的“地址”——地址跳转栏
 - 2.2.6 芝麻开门——分区快捷入口
 - 2.2.7 家有“贤妻”——快捷文件管理

第3章 开天辟地清浊辨——WinHex文件管理

- 3.1 新建文件
 - 3.1.1 我们需要多胖的“MM”
 - 3.1.2 眼前全是“0”
- 3.2 打开文件
 - 3.2.1 选择一个打开对象
 - 3.2.2 文件原来是这样的
 - 3.2.3 碎片分类初探
 - 3.2.4 从头到尾都别放过
- 3.3 保存和另存为
- 3.4 镜像功能

<<识数寻踪>>

- 3.4.1 孪生数据
- 3.4.2 一些镜像格式
- 3.4.3 克隆也可以有选择
- 3.4.4 要体积还是要速度
- 3.4.5 用镜像来恢复自己
- 3.4.6 备份管理器
- 3.5 文件属性功能
 - 3.5.1 文件也有属性
 - 3.5.2 文件属性调查
 - 3.5.3 文件属性修改
- 3.6 批量处理
- 3.7 不得不提的CreateFile
- 3.8 创建文件
- 3.9 读取大作战
- 第4章 移星换斗惊天颜——详解WinHex的编辑功能
 - 4.1 撤销
 - 4.2 剪切
 - 4.3 复制和粘贴
 - 4.3.1 数据复制方法也可以多种多样
 - 4.3.2 东拼西凑缝缝补补
 - 4.4 移除
 - 4.5 粘贴0字节
 - 4.6 转换
 - 4.7 修改数据
 - 4.7.1 给数据加上或减去某个数
 - 4.7.2 站队游戏
 - 4.7.3 简单的数学运算
 - 4.8 数据填充
 - 4.8.1 只想看见0
 - 4.8.2 不想让人知道数据被擦除过
- 第5章 金睛火眼识道缘——WinHex的搜索游戏
 - 5.1 搜索主菜单
 - 5.2 查找文本
 - 5.2.1 编码
 - 5.2.2 查找文本子项
 - 5.2.3 十六进制字节查找
 - 5.3 替换文本
 - 5.4 替换十六进制
 - 5.5 同步搜索
 - 5.6 组合搜索
 - 5.7 整型和浮点型查找
 - 5.7.1 整数和浮点数在计算机内部的表示
 - 5.7.2 整数和浮点数查找子项
 - 5.8 单词短语搜索
 - 5.9 搜索选项
 - 5.10 字符串查找代码示例
 - 5.10.1 简单匹配算法

<<识数寻踪>>

5.10.2 KMP算法

第6章 稳坐泰山傲天险——奇妙的地址管理功能

6.1 跳转

6.2 前进与后退

6.3 管理标记

6.3.1 自己设路标

6.3.2 位置管理

第7章 妙目流盼易妆容——WinHex不为人知的一面

7.1 改变编辑区

7.2 录制幻灯

7.3 模板管理器

7.3.1 惊喜

7.3.2 设计自己的模板

7.3.3 几个模板设计案例

7.4 同步比较

7.4.1 同步查看很重要

7.4.2 让差异显形

第8章 神功大展现本元——WinHex与数据恢复

8.1 打开磁盘

8.2 磁盘工具

8.2.1 磁盘克隆

8.2.2 展开目录

8.2.3 按类型恢复文件

8.2.4 初始化空余空间

8.2.5 初始化残余空间

8.2.6 初始化MFT表

8.2.7 寻找丢失的分区

8.2.8 分区恢复高级功能

8.2.9 设置磁盘参数

8.3 文件工具

8.3.1 文件合并

8.3.2 文件分割

8.3.3 整合数据

8.3.4 拆分数据

8.3.5 比较数据

8.3.6 安全擦除

8.4 内存编辑器

8.5 数据分析

8.6 计算哈希值

第9章 登峰造极乾坤改——我们渴望的高级功能

9.1 玩转文件系统扫描

9.1.1 数据恢复就是点鼠标的事

9.1.2 花团锦簇的附加功能

9.2 一份非常详尽的报告

9.3 视镜像文件为磁盘

9.4 RAID重组

9.5 荒野寻宝——收集空余空间

<<识数寻踪>>

- 9.6 探索被遗忘的角落——收集残余空间
- 9.7 取出夹缝中的明珠——收集分区间隙
- 9.8 找出人类文明——收集文本信息
- 9.9 文件也需要编号
- 第10章 曲径通幽窥法玄——通过“设置”驯服WinHex
 - 10.1 常规设置
 - 10.2 目录浏览器
 - 10.3 数据解释器
 - 10.3.1 解析文件的考勤记录
 - 10.3.2 勤俭持家的DOSDate
 - 10.3.3 生面孔OLEDate
 - 10.3.4 江湖前辈CDateTime
 - 10.3.5 简明扼要的IP地址
 - 10.3.6 数据库世界的ANSI SQL DATETIME
 - 10.3.7 满载荣宠的HFS+DATETIME
 - 10.3.8 再谈反汇编
 - 10.3.9 唯一标识GUID
 - 10.3.10 无处不在的安全标识符SID
- 第11章 运筹帷幄决千里——让WinHex更强大的脚本开发技术
 - 11.1 脚本特性一览
 - 11.2 WinHex脚本语法讲解及应用演示
 - 11.2.1 用Create命令创建文件
 - 11.2.2 用Open命令打开对象
 - 11.2.3 用CreateBackupEx命令创建备份
 - 11.2.4 用Goto命令进行地址跳转
 - 11.2.5 用Move命令移动光标
 - 11.2.6 用Write命令写入数据
 - 11.2.7 用Insert命令插入数据
 - 11.2.8 用Read命令读取数据
 - 11.2.9 用ReadLn命令读取一行数据
 - 11.2.10 用Close命令关闭访问对象
 - 11.2.11 用CloseAll命令关闭所有访问对象
 - 11.2.12 用Save命令保存
 - 11.2.13 用SaveAs命令另存为
 - 11.2.14 用SaveAll命令保存全部数据
 - 11.2.15 用Terminate命令中断脚本
 - 11.2.16 用Exit命令退出WinHex
 - 11.2.17 用ExitIfNoFilesOpen命令干一些心急的事情
 - 11.2.18 用Block命令选块
 - 11.2.19 用Copy命令复制
 - 11.2.20 用Cut命令剪切
 - 11.2.21 用Remove命令移除
 - 11.2.22 用CopyIntoNewFile命令将选块复制进新文件
 - 11.2.23 用Paste命令粘贴
 - 11.2.24 用WriteClipboard命令写入
 - 11.2.25 用Convert命令进行编码转换
 - 11.2.26 用AESEncrypt命令加密

<<识数寻踪>>

- 11.2.27 用Find命令搜索
 - 11.2.28 用ReplaceAll命令替换
 - 11.2.29 用IfEqual命令比较
 - 11.2.30 用Loop命令循环
 - 11.2.31 用Label命令标记脚本行
 - 11.2.32 用ForAllObjDo命令做并行
 - 11.2.33 用CopyFile命令复制文件
 - 11.2.34 用InitFreeSpace命令初始化自由空间
 - 11.2.35 用Assign命令声明变量
 - 11.2.36 用GetUserInput命令输入数据
 - 11.2.37 用Inc命令递增
 - 11.2.38 用Dec命令递减
 - 11.2.39 用IntToStr命令转换
 - 11.2.40 用GetClusterAllocEx命令获取簇分配状况
 - 11.2.41 用GetClusterSize命令获取簇大小
 - 11.2.42 用InterpretImageAsDisk命令变镜像文件为磁盘
 - 11.2.43 用CalcHashEx命令计算哈希值
 - 11.2.44 用Turbo命令节约资源
 - 11.2.45 用Debug命令调试
 - 11.2.46 用UseLogFile命令保存日志文件
 - 11.2.47 三个常量CurrentPos、GetSize、Unlimited
- 第12章 深山居士佛光潜——遮遮掩掩的WinHex API函数
- 12.1 佛光朦胧——初窥WinHex API
 - 12.2 WinHex API函数列表
 - 12.2.1 WHX_Init函数
 - 12.2.2 WHX_Done函数
 - 12.2.3 WHX_Open函数
 - 12.2.4 WHX_Create函数
 - 12.2.5 WHX_Close函数
 - 12.2.6 WHX_CloseAll函数
 - 12.2.7 WHX_NextObj函数
 - 12.2.8 WHX_Save函数
 - 12.2.9 WHX_SaveAs函数
 - 12.2.10 WHX_OpenEx函数
 - 12.2.11 WHX_Read函数
 - 12.2.12 WHX_Write函数
 - 12.2.13 WHX_GetSize函数
 - 12.2.14 WHX_Goto函数
 - 12.2.15 WHX_Move函数
 - 12.2.16 WHX_CurrentPos函数
 - 12.2.17 WHX_SetBlock函数
 - 12.2.18 WHX_Copy函数
 - 12.2.19 WHX_CopyIntoNewFile函数
 - 12.2.20 WHX_Cut函数
 - 12.2.21 WHX_Remove函数
 - 12.2.22 WHX_Paste函数
 - 12.2.23 WHX_WriteClipboard函数

<<识数寻踪>>

- 12.2.24 WHX_Find函数
 - 12.2.25 WHX_Replace函数
 - 12.2.26 WHX_WasFound函数
 - 12.2.27 WHX_WasFoundEx函数
 - 12.2.28 WHX_Convert函数
 - 12.2.29 WHX_Encrypt函数
 - 12.2.30 WHX_Decrypt函数
 - 12.2.31 WHX_GetCurObjName函数
 - 12.2.32 WHX_GetStatus函数
- 第13章 南柯梦醒暗香来——某个关于MDF文件的案例
- 13.1 郁闷
 - 13.2 页
 - 13.2.1 初探页头
 - 13.2.2 深入挖掘
 - 13.2.3 实验
 - 13.2.4 重点关注
 - 13.3 故事后记

章节摘录

版权页：插图：2.恢复/复制 单击“恢复/复制”（Recover / Copy）可以完成简单的数据恢复工作。

很多时候，我们只用这个功能就可以应付工作任务。

3.导出列表 单击“导出列表”可以为被选文件建立信息报告（见表2 - 1）。

现在，大型数据恢复公司都主动为客户提供数据恢复报告，该功能可以大大减少其工作量。

创建报告的方法也很简单，先选择要输出的字段，然后保存一个报告文件路径即可（见图2 - 46）。

表2 - 1提供了相当完整的文件基本信息，以后我们想关注该文件，无须重新启动WinHex查找，浏览该报告即可。

4.同步搜索 大家一定听说过正则表达式，它可以便捷地建立匹配模板，完成复杂数据环境下的搜索任务。

正则表达式已经广泛应用于跟数据处理有关的各个学科，WinHex对其更是重视。

可以先让大家有个准备，WinHex的“同步搜索”和“通过文件类型恢复”功能都和正则表达式息息相关，甚至可以划上等号。

这里我们可以看到，“同步搜索”已经出现在“快捷文件管理”菜单中。

5.隐藏“隐藏”有两个功能子项，第一个功能很好理解，就是将当前选择的文件从列表空间中隐藏。

有时候，我们用排除法定位需要的数据，就可以对无用数据进行隐藏，缩小筛选范围。

第二个功能可以排除完全相同的文件，这里的完全相同是指其哈希值相同，也就是每一个字节都相同。

对于相同的文件我们完全可以只关注其中一个，以求节约时间。

具体如图2 - 47所示。

6.Position Position（位置）功能（见图2 - 48）对学习数据恢复有很大的帮助。

为什么呢？

我们知道，在民间数据恢复机构中流行“手工数据恢复”一说，意指不通过数据恢复工具，而是完全凭借自身对文件系统或文件结构的理解，并利用WinHex的数据编辑功能，查找、填补、推算数据环境中的缺失点和关键点，从而实现数据恢复的技术。

从狭义上讲，手工数据恢复充分发挥了灵活优势。

我们知道，再精妙的程序也不能代替人脑的思考过程。

同样，数据恢复工具再强大，也不能面面俱到。

手工数据恢复就是在数据恢复工具丧失作用时的一种终极手段。

从广义上讲，手工数据恢复既是行业地位的象征，又是一种乐趣、一种艺术、每一名数据恢复工程师追求的较高境界。

手工数据恢复需要掌握大量的基础知识，并非一朝一夕可以练就。

“位置”功能可以帮助数据恢复工程师深刻理解手工数据恢复。

<<识数寻踪>>

媒体关注与评论

你想在企业服务器数据丢失的关键时刻亮剑吗？

你想让监控录像重现天日还人间一份正义吗？

你想闪电重组数据库碎片让时光倒流吗？

《识数寻踪：WinHex应用与数据恢复开发秘籍》一书为你保驾护航，让你如虎添翼。

——哈尔滨海云数据恢复中心创始人、SQLSave系列数据库恢复软件作者 江传力本书对WinHex工具讲解得非常透彻，涉及的知识非常全面，对WinHex工具的使用者来说是个福音，它可以让读者全面掌握WinHex脚本编程及WinHex API编程技术，是提升自我技术不可不读的一本好书。

——数据恢复业内高手郝槟楠（网名“windows hao”）志鹏被广大数据恢复从业者称为国内WinHex第一人，曾撰写WinHex网上教程十余篇，包括我在内的很多从业者、爱好者、网友都获益匪浅。

本书是志鹏的呕心沥血之作，相信这本书能为读者打开WinHex的神秘之门，让读者真正掌握WinHex这一神功利器。

——擅长碎片重组的数据恢复业内高手陈剑嵩（网名“12:00:00”）

<<识数寻踪>>

编辑推荐

《识数寻踪:WinHex应用与数据恢复开发秘籍》花费数年时间原创，国内唯一完整的WinHex使用教程和数据恢复开发资料！

揭示业内只有高手才掌握的秘密（WinHex脚本编程和API开发）！

<<识数寻踪>>

名人推荐

你想在企业服务器数据丢失的关键时刻亮剑吗？

你想让监控录像重现天日还人问一份正义吗？

你想闪电重组数据库碎片让时光倒流吗？

《识数寻踪：WinHex应用与数据恢复开发秘籍》一书为你保驾护航，让你如虎添翼。

——哈尔滨海云数据恢复中心创始人、SQLSave系列数据库恢复软件作者 江传力 本书对WinHex工具讲解得非常透彻，涉及的知识非常全面，对WinHex工具的使用者来说是个福音。

它可以让读者全面掌握WinHex脚本编程及WinHex API编程技术，是提升自我技术不可不读的一本好书。

——数据恢复业内高手郝槟楠（网名“windows hao”）志鹏被广大数据恢复从业者称为国内WinHex第一人，曾撰写WinHex网上教程十余篇，包括我在内的很多从业者、爱好者、网友都受益匪浅。

本书是志鹏的呕心沥血之作，相信这本书能为读者打开WinHex的神秘之门，让读者真正掌握WinHex这一种神功利器。

——擅长碎片重组的数据恢复业内高手陈剑嵩（网名“12:00:00”）

版权说明

本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问:<http://www.tushu007.com>