郭　果●主编

数据恢复技术基础实验指导

SHUJU HUIFU JISHU JICHU SHIYAN ZHIDAO

科学出版社

数据恢复技术基础实验指导

郭 果 主编

科学出版社
北 京

内 容 简 介

本书通过大量的实验项目——基础实验和磁盘存储结构及文件系统分析实验来引领读者学习数据恢复技术的基本内容，让读者在实验中学习理论知识，提高专业技能，并逐步培养安全使用计算机的良好习惯，从而有效地提高数据的安全性。

本书是根据作者多年从事数据恢复技术的实验教学经验编写而成的，详细地介绍了学习数据恢复技术必须要掌握的技能和知识。通过本书的学习，读者能在实际工作中解决大多数的数据安全和恢复问题。

本书可作为中高等院校（包括各类职业学校）的计算机及应用、软件工程或网络安全等相关专业的专业教材和参考书，也可作为社会培训机构的教学用书，以及计算机爱好者的自学用书。

图书在版编目（CIP）数据

数据恢复技术实验实训指导 / 郭果主编. -- 北京 : 科学出版社, 2014.10

ISBN 978-7-03-040997-0

Ⅰ.数… Ⅱ.①郭… Ⅲ.①数据管理－安全技术

Ⅳ.①TP309.3

中国版本图书馆 CIP 数据核字(2014)第 097441 号

责任编辑：杨 岭 朱小刚/ 封面设计：墨创文化

责任校对：邓丽娜 / 责任印刷：余少力

科学出版社 出版

北京东黄城根北街 16 号

邮政编码：100717

http://www.sciencep.com

成都创新包装印刷厂印刷

科学出版社发行 各地新华书店经销

*

2014 年 10 月第 一 版 开本：787×1092 1/16

2014 年 10 月第一次印刷 印张：18 1/2

字数：440 千字

定价：48.00 元

《数据恢复技术基础实验指导》

编委会

编 者 的 话

当今的数字化信息技术备受关注。人们通过各种方式、方法和途径来解决数字化信息的安全问题，比如“云”存储技术、网盘技术等。在实际工作和生活中，人们总是通过计算机来处理原始的数字化信息，所以安全问题在很大程度上是由个人因素（即个人使用计算机的方法及知识结构）直接决定的。

以下是一些常见的操作计算机的不良习惯，请读者改正。

（1）在电脑“桌面”上（或“我的文档”，或操作系统盘上等）放重要文件。这样做不仅会导致开机变慢，而且当操作系统出现问题时，有可能丢失重要文件等数据，且不易恢复。

（2）硬盘分区仍然使用 FAT 32 文件系统。FAT 32 文件系统会产生大量的文件磁盘碎片，数据一旦丢失，将不利于恢复，建议使用更先进的 NTFS 文件系统。

（3）把重要文件直接放在分区的根上而不是文件夹中。文件夹是存放文件十分安全的地方，其中的数据也较容易恢复。

（4）不习惯备份重要文件到移动盘或网盘上。

（5）利用“发送到”命令而不是使用“复制”的方法将文件移动到磁盘或 U 盘上，这样做可能会导致假发送。

（6）假如分区是 FAT 32 文件系统，若使用组合键“Shift+Del”来删除文件，则不利于数据恢复。

数据的保护，主要包括操作系统的保护和文件的保护两部分。操作系统的保护主要是指操作系统备份，它可以在很短时间内将操作系统还原到新安装时的状态。保护好操作系统也能很好地保证文件的安全。文件是最为重要的数据，也是构成数字化信息的主要组成部分。“云”存储技术是文件保护的主要方式之一。

在计算机的使用过程中，数据丢失是难免的。互联网上提供了大量的用于数据恢复的软件和工具，然而，这些数据恢复软件和工具都要求使用者要懂得设置参数，才能很好地恢复数据。

在进行数据恢复时，一定要懂得“准”“快”“好”三原则。“准”就是准确判断数据丢失的原因（越准确越好）。“快”就是合理设置参数，快速使用相应工具恢复数据。“好”就是指恢复数据的概率越高越好。

本书将通过大量的实验来说明数据丢失的原因（原理），一些实验要求读者亲自破坏数据，从而能很快学会恢复数据的各种方法，以提高“准”“快”“好”的综合技术能力。

在数据恢复技术领域中，对数据的恢复工作主要分为三个层面：一是软件级技术（也叫高层逻辑级）；二是固件级技术（也叫底层逻辑级）；三是硬件级技术。其中软件级技术是指在操作系统中利用数据恢复软件来进行恢复的技术层面，这是数据恢复技术中最为基础的层面，要求读者不仅要懂得软件工具如何使用，更要懂得数据存储的原理，从而能达到数据恢复的要求。后两个技术层面，要求读者必须具备软件级的能力，同时还要求具备更高的技术能力，这两个层面的技术最终都要回到软件级来进行。

本书的实验主要介绍的是软件级层面的应用，由浅入深，使读者最终能够自主解决实

际工作中的数据恢复问题。

本书的大多数实验都在虚拟机中完成，这样可避免直接面对实际计算机而导致其崩溃等不利因素。初学数据恢复技术的读者，跟随本书的顺序一步一步地做和学，即可达到学习目标，不会损坏读者的计算机系统和数据。

本书由郭果主编，编委成员有：四川师范大学的徐勇、杨春、冯山、郭荣佐、杨军、余毅，四川城市职业学院信息工程系的李力，成都大学信息科学与技术学院的刘莎，成都理工大学继续教育学院的谭素，昆明医科大学的刘永生、章可，云南中医学院的杨莉等。郭果负责统稿、校稿及技术验证。另外，本书由郭涛负责主审，由四川效率源信息安全技术有限责任公司的黄旭（技术总监）和张彬（高级工程师）作学术顾问。在此，对以上老师致以诚挚的谢意！

由于编者水平有限，书中难免存在不足和不妥之处，敬请广大读者不吝批评指正。

前　言

随着计算机用户数量的不断增长和互联网的迅猛发展，人类社会越来越依赖各种各样的数据网络和数量极为庞大的数字信息，因此数据安全变得越来越重要，其中设备意外损坏、病毒攻击、操作失误、人为破坏等是较为普遍的数据安全问题。

“电脑有价，数据无价”正是对信息时代电脑数据重要性的真实写照。具体到每个人的生活和工作中，从 PC 机、移动硬盘、U 盘、手机、数码相机到各种各样的银行卡、证照卡、交通卡等都有大量的数据贮存在介质上，这些数据汇成巨量数据流，且随时都存在丢失的可能。在庞大的数据损失的基数之上，数据修复业务迅速膨胀，是近年来越来越受重视的一个领域。数据恢复技术是保障数据存储安全的重要措施与手段之一，是计算机技术发展的必然产物，也是一门新兴技术。它主要研究如何修复硬盘上被破坏的数据，以及如何保护硬盘上的数据。相对国外较健全的数据恢复业市场，国内的数据恢复业发展虽慢了一些，但也显示出蓬勃旺盛的发展势头。

本书汇集了作者十余年教学实践经验，主要针对当前应用最普及的微软系列操作系统，循序渐进、全面系统地介绍了如何修复硬盘上被破坏的数据以及如何保护硬盘中的重要数据的方法，能逐步培养读者安全使用计算机的良好习惯，从而有效地提高数据的安全性。本书注重实用性与实效性，强调实践操作。

（1）实验工具说明。本书所用工具软件都来自于互联网。这些工具能使读者快速掌握数据恢复课程所必须具备的能力和知识，是有必要深入学习的工具软件。

本书中的每个实验项目，都列举了本实验项目中所用到的软件工具，建议读者根据所用软件工具的名称在互联网中进行搜索，并下载使用。

本书所介绍的实验工具软件可以从互联网搜索得到，从而可组成一个实验材料（如可以把这些工具软件都封装到一张光盘中），教师在教学过程中还能根据教学的要求或进度，对所选工具或章节进行适当的增减。

（2）实验环境要求。为了能很好地运行虚拟机及其相关软件工具，建议选用 Windows Server 2003、Windows XP、Windows7 和 Windows Sever 2008 等 32 位或 64 位的计算机操作系统之一。

计算机的硬件配置要求如下：CPU 为 P4 或性能更高的型号；内存 2GB 或以上；硬盘的空余空间建议 20GB 以上。

（3）教学建议。本书可用于相关实验教学，建议理论教学学时数为 32～48 学时，实验教学学时数为 32～40 学时。

本书创建了一个安全虚拟的学习环境，收集并提供了实用的系列工具软件，不仅是普通高校、职业技术学院计算机及其相关专业学生的首选实验教材，对广大计算机操作人员来说，也是一本重要的操作指南和技术手册。

由于计算机科学技术发展日新月异，加上作者学识有限，书中难免存在不足之处，敬请读者指正。

目　录

第一部分　基 础 实 验

实验项目 1 和实验项目 2 是本书所有实验项目的基础。要求读者能创建自己的可启动 ISO 工具光盘，并能运用到虚拟机上，能在 Win PE 或 DOS 操作系统中使用相应工具软件。

实验项目 3～6 能使读者对分区有直观理解，初步认识数据存储结构。实验要求读者能熟练地对硬盘进行分区操作，并能在分区间进行不同的应用，如 Ghost 应用、数据保护应用（即灾备）、Windows 操作系统的保护，以及 DOS 等操作系统的安装。

实验项目 1　创建 ISO 工具光盘

实验工具软件

（1）通用 PE 工具箱。

（2）UltraISO。

1.1　通过“通用 PE 工具箱”获得 ISO 光盘

1.1.1　基本概念

（1）本地操作系统：本地操作系统指读者计算机所用的操作系统，如 Windows 2003/XP/7/Sever 2008 等。

（2）物理光盘：指通过模具压制的，或用刻录机和软件刻录而成的类似塑料的圆片，如常见的 CD、DVD 等，它们分为只读和刻录等类型。物理光盘也可通过软件，如“UltraISO”制作为虚拟光盘。

（3）虚拟光盘：也叫软光盘或光盘映像，是一种文件形式，其类型为 ISO 文件，也有其他的后缀，如 BIN 等。ISO 虚拟光盘一般用在虚拟光驱中或虚拟机中，如同在实际的计算机中使用物理光盘一样。虚拟光盘可以通过刻录机和刻录软件将其刻录为物理光盘。在互联网中提供有大量的 ISO 光盘文件，如工具光盘、操作系统安装光盘等。虚拟光盘也可以通过“UltraISO”等软件工具来编辑得到。虚拟光盘只有在要刻录为物理光盘时，才需要注意容量是否能满足物理刻录光盘的规格。

（4）物理光驱：是指能放入物理光盘的盒子，就是平时说的光驱。一般分为只读及刻录等类型，又有 CD、DVD 等不同种类。物理光驱一般是向下兼容的。

（5）虚拟光驱：是由软件（如“UltraISO”）生成的模拟光驱工作的工具软件，它只能放入（或插入）虚拟光盘，如同将物理光盘放入物理光驱中一样来使用。虚拟光驱可以插入任意大小的虚拟光盘。在本地操作系统中，要区别物理光驱与虚拟光驱的图标和使用方法。

（6）MAXDOS：是迈思工作室利用 DOS V7.1（是 Windows 98操作系统自带的维护 DOS 操作系统）对微软的传统（或标准）DOS 操作系统进行扩展的一个软件工具。MAXDOS 以光盘或其他可携设备作为媒介，并提供了大量适用的工具和命令，是计算机维护和数据恢复等重要的工作平台。软件“通用 PE 工具箱”就提供有 MAXDOS 操作系统。

（7）WinPE：也叫 Windows 预先安装环境（Microsoft Windows Preinstallation Environment），是 Windows XP、Windows 2003、Vista 7 和 Vista 8 等操作系统的简化版。WinPE 以光盘或其他可携设备作为媒介。WinPE 的作用有：方便企业作出工作站和服务器的企划；给原始设备制造商（OEM）制造自定义的 Windows 操作系统；取代 MS-DOS 软盘等。WinPE 是计算机维护和数据恢复等工作的重要平台，软件“通用 PE 工具箱”就提供有 WinPE 操作系统。

1.1.2 工具简介

“通用 PE 工具箱”是一款可安装在硬盘、U 盘、光盘等上使用的 WinPE 或 MAXDOS 工具集合，是一款新手或高手都适用的维护工具。它可以快速实现一个独立于本地操作系统的临时 Windows 或 DOS 操作系统，并含有 Ghost、硬盘分区、密码破解、数据恢复和修复引导等工具。它完全在内存中运行的特性可以极高的权限访问硬盘，让用户在使用 PE 的时候也能够快速进入 DOS（即 MAXDOS，与 WinPE 相伴），能给用户带来完美的维护体验。

“通用 PE 工具箱”是很有代表性的工具，装机量也很大，其主要特点如下。

（1）简易的全能安装。“通用 PE 工具箱”采用 exe 压缩包安装方式，无需借助外部工具，安装时只需点击“下一步”即可。它可快速安装在计算机系统中，并具有制作可启动 U 盘、生成 ISO 镜像并刻录为物理光盘等功能。

（2）无可挑剔的兼容性。“通用 PE 工具箱”对硬盘识别率高达 99.99%，其中 MAXDOS 的兼容性也毋庸置疑，都是使用多年的产品。

（3）强大的功能序列。在“通用 PE 工具箱”中，WinPE 下含有 Ghost、硬盘分区、密码破解、数据恢复、修复引导等工具，DOS 下含有 Ghost，这些工具对维护系统而言完全够用。另外，它还有一键还原、DiskGen、MHDD、HDDReg、PQ 等常用磁盘工具和其他常用 DOS 工具。

（4）优良的性价比。在保证强大的功能序列同时，“通用 PE 工具箱”的大小控制在 100MB 左右。

（5）良好的用户界面。在安装“通用 PE 工具箱”时，会有许多个性化的选项，方便用户根据自己的使用习惯进行设置。

“通用 PE 工具箱”有不同的几个版本，如 V3.3、V4.0、V5.0、V6.0 等，而其内核主要有 Windows XP、Windows 2003、Windows 7 和 Windows 8 等。“通用 PE 工具箱”对计算机的兼容性越来越高（即能更好地利用计算机的硬件资源），但其对计算机的内存要求也越来越高，容量也越来越大。

本书以 Windows 7 内核的 V3.3 版本的“通用 PE 工具箱”为主要的实验工具软件。读者可以任意选择“通用 PE 工具箱”的版本来做实验，只要能生成出可启动的 ISO 虚拟光盘并能正常在虚拟机中使用即可；也可以选用其他的能启动的 ISO 虚拟光盘（网上提供有大量的这类虚拟光盘），只要能正常启动和使用 Win PE 和 DOS 操作系统即可。

Windows 8 内核的任何版本的“通用 PE 工具箱”中的 Win PE 操作系统在某些虚拟机中无法正常运行（其中的 MAXDOS 可以正常运行），原因是它对虚拟机软件的要求很高，必须能兼容 Windows 8 系统。不过，Windows 8 内核的任何版本的“通用 PE 工具箱”在实际的计算机上使用时没有限制。

1.1.3 实验目的

能获得适用的可启动 ISO 工具光盘，如“通用 PE 工具箱”等（“通用 PE 工具箱”是本书所有实验的基础工具之一）。能理解 ISO 软光盘的作用，能利用“通用 PE 工具箱”生成 ISO 软光盘。

1.1.4 实验指导

在本地操作系统中，双击下载好的“通用 PE 工具箱_V3.3”软件图标，如图1-1所示。

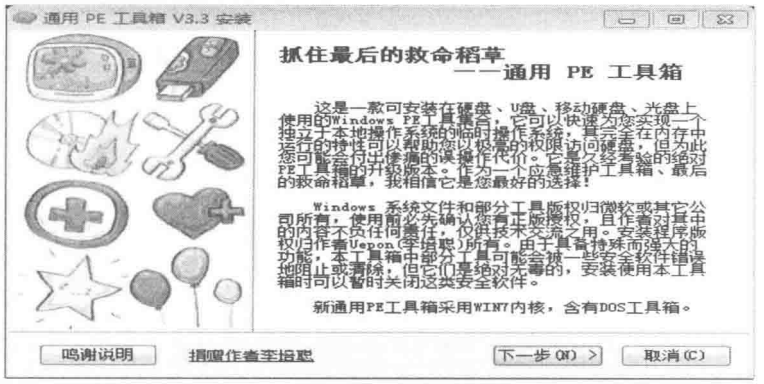

图 1-1 “通用 PE 工具箱_V3.3”欢迎界面

点击“下一步”按钮，如图 1-2 所示。

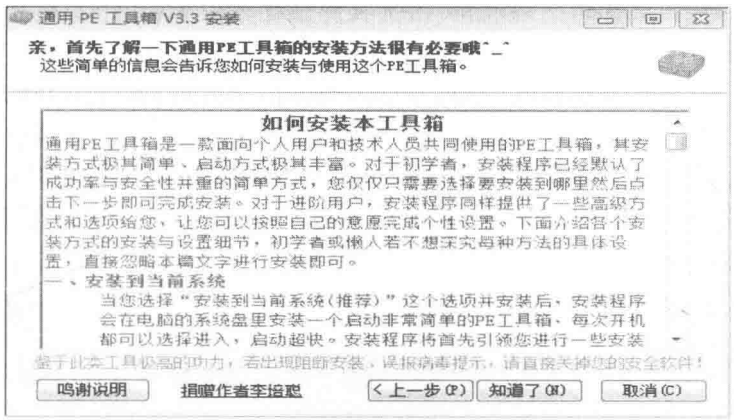

图 1-2 “通用 PE 工具箱_V3.3”介绍画面

点击“知道了”按钮，如图 1-3 所示。图 1-1 和图 1-2 是该软件的介绍和说明，这些内容对用户的使用十分有帮助。

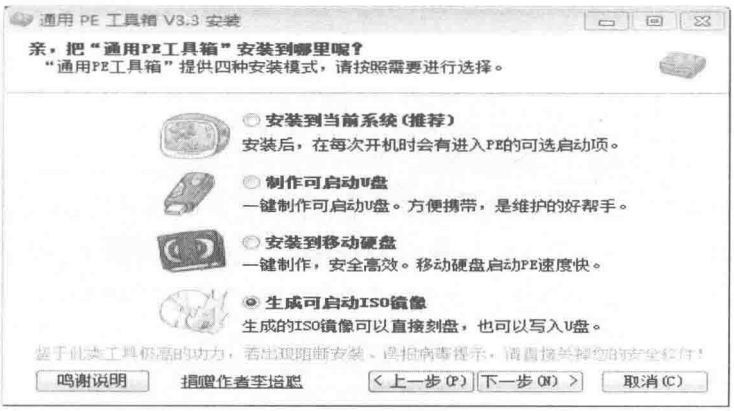

图 1-3 “通用 PE 工具箱_V3.3”的安装模式选择

在安装模式选择界面（图 1-3）上，请读者一定选择“生成可启动 ISO 镜像”选项，其他选项这里暂时不用考虑，也请不要莽撞尝试，以免给你的计算机系统或移动盘带来不必要的麻烦。点击“下一步”按钮，如图 1-4 所示。

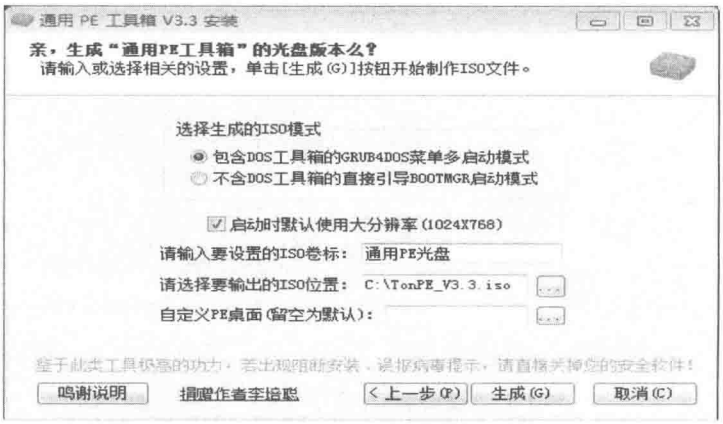

图 1-4 “通用 PE 工具箱_V3.3”生成 ISO 工具的选项

此时采用默认设置即可。需注意 ISO 文件输出的位置在 C 盘的根上，其文件名是“TonPE_V3.3.ISO”。

若选中“选择生成的 ISO 模式”选项中的第一项时，表示该 ISO 光盘在启动计算机后，将显示选择菜单，用户可以选择进入 DOS 操作系统，也可以选择进入 WinPE 操作系统；若选中第二项时，表示该 ISO 光盘在启动计算机后，直接进入 WinPE 操作系统而无法进入 DOS 操作系统。

这种默认设定的启动光盘，是一种通用方式，本书的所有实验项目都将使用这种启动光盘的模式。设置确定后，点击“生成”按钮，如图 1-5 所示。

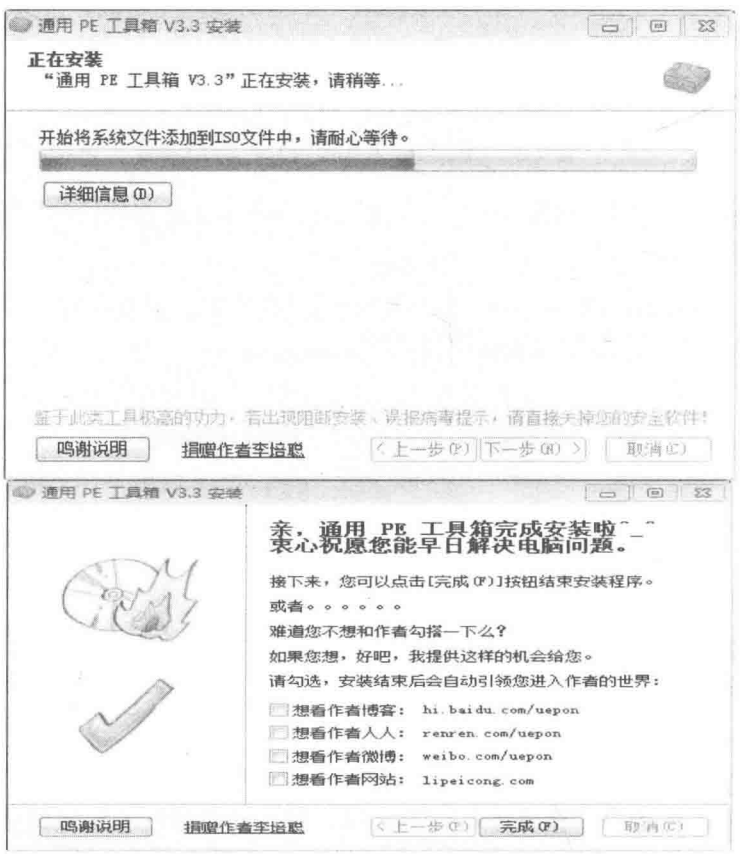

图 1-5 “通用 PE 工具箱_V3.3”生成 ISO 的过程和结束画面