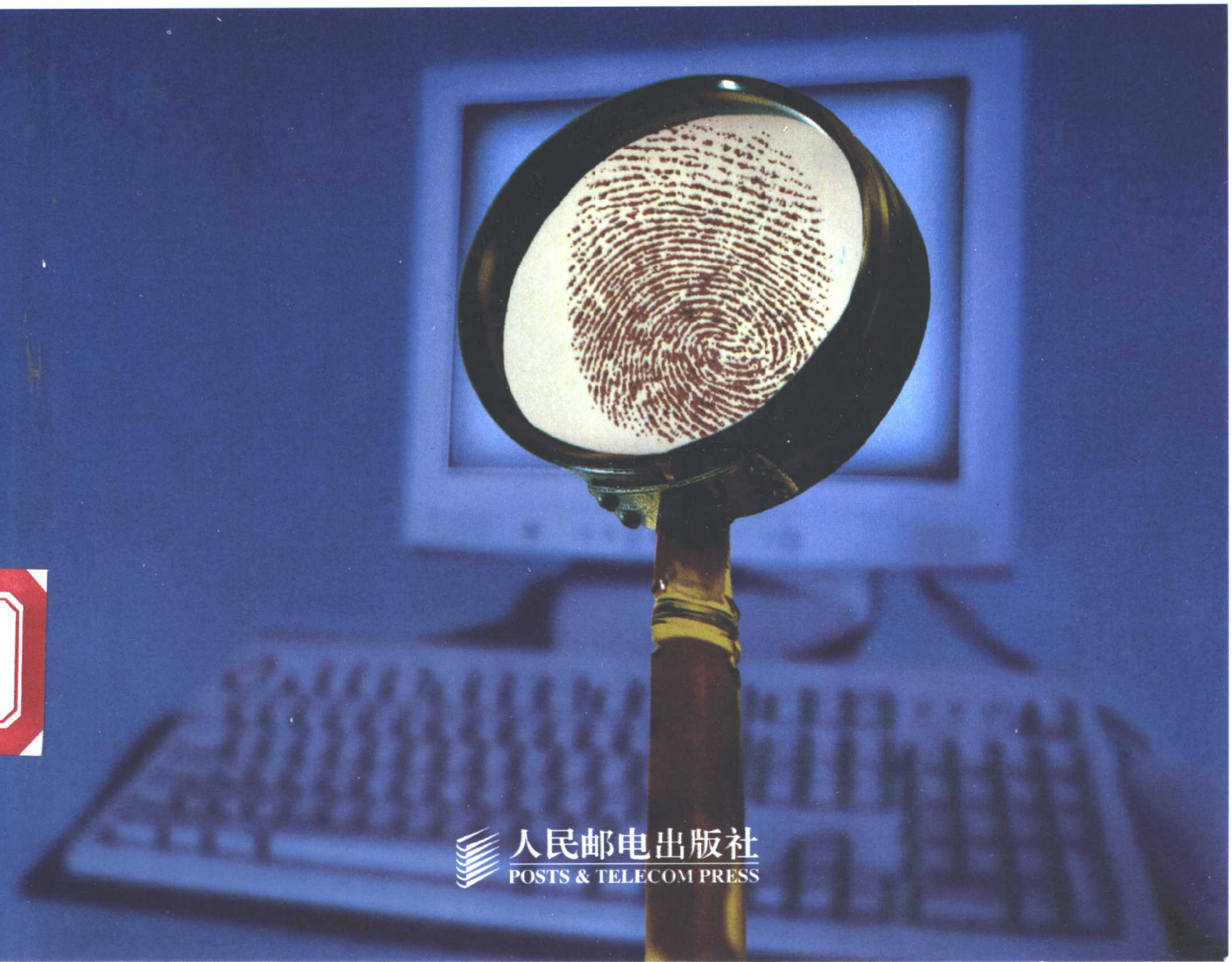
Addison Wesley

计算机取证：应急响应精要

Computer Forensics

[美] Warren G. Kruse II
Jay G. Heiser 著

中国教育和科研计算机网紧急响应组(CCERT) 段海新 刘武 赵乐南 译



人民邮电出版社
POSTS & TELECOM PRESS

计算机取证：应急响应精要

[美] Warren G. Kruse II
Jay G. Heiser 著

中国教育和科研计算机网紧急响应组（CCERT） 段海新 刘武 赵乐南 译

人 民 邮 电 出 版 社

图书在版编目（CIP）数据

计算机取证：应急响应精要 /（美）克鲁泽（Kruse,W.G.），（美）海泽（Heiser,J.G.），著；段海新，刘武译. —北京：人民邮电出版社，2003.8
ISBN 7-115-10875-7

Ⅰ. 计… Ⅱ. ①克…②海…③段…④刘… Ⅲ. 计算机犯罪—证据—调查 Ⅳ. D915.13

中国版本图书馆 CIP 数据核字（2003）第 040223 号

版权声明

Authorized translation from the English language edition, entitled
Computer Forensics: Incident Response Essentials, 1st Edition, ISBN: 0201707195, by Warren G. Kruse II and Jay G. Heiser, published by Pearson Education, Inc, publishing as Addison Wesley, Copyright © 2002 by Lucent Technologies.
All rights reserved. No part of the book may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording or by any information storage retrieval system, without permission from Pearson Education, Inc.
CHINESE SIMPLIFIED language edition published by Posts & Telecommunications Press.
本书英文版由 Addison Wesley 出版。人民邮电出版社取得授权翻译出版中文简体版。未经出版者许可，对本书任何部分不得以任何方式或任何手段复制和传播。
版权所有，侵权必究。

计算机取证：应急响应精要

◆ 著 [美] Warren G. Kruse II Jay G.Heiser
译 中国教育和科研计算机网紧急响应组 (CCERT) 段海新 刘 武 赵乐南
责任编辑 李 际

◆ 人民邮电出版社出版发行 北京市崇文区夕照寺街 14 号
邮编 100061 电子函件 315@ptpress.com.cn
网址 http://www. ptpress.com.cn
读者热线 010-67132705
北京汉魂图文设计有限公司制作
北京密云春雷印刷厂印刷
新华书店总店北京发行所经销

◆ 开本：787×1092 1/16
印张：17.75
字数：427 千字 2003 年 8 月第 1 版
印数：1-3 500 册 2003 年 8 月北京第 1 次印刷

著作权合同登记 图字：01 - 2002 - 1551 号
ISBN 7-115-10875-7/TP • 3194

定价：39.00 元

本书如有印装质量问题，请与本社联系 电话：(010)67129223

内容提要

计算机越来越多地被卷入到犯罪活动中，或者是受攻击的目标，或者是犯罪的工具。计算机取证是计算机安全领域中的一个全新的分支，涉及计算机犯罪事件证据的获取、保存、分析、证物呈堂等相关法律、程序、技术问题。本书的作者结合信息安全领域多年的经验和计算机取证培训班学员的需求，详细介绍了计算机取证相关的犯罪的追踪、密码技术、数据隐藏、恶意代码、主流操作系统取证技术，并详细介绍了计算机取证所需的各种有效的工具，还概要介绍了美国司法程序。

本书适合计算机网络和信息安全领域的工程技术人员阅读。对执法部门的计算机犯罪调查人员以及计算机安全事件调查处理人员，本书是目前非常难得的参考书。

致 谢

首先，要感谢在本书的创作过程中给予我们耐心帮助的人们(也许其中部分人可能没有意识到他们在此期间所做的工作)：Nate Miller、 Geoff Silver、 Felix Lindner、 Tom Shevock、Tim Lunsford、Dan Farmer、Wietse Venema、Aaron Higbee、Bill Brad、Aaron Kramer、Curt Bryson、Wil Harris、Dave Dittrich、James Holley、 Tim O'Neill、Fred Cohen、Lance Spitzner、Gene Spafford、Theresa Ho、Joe Ippolito、Abigail Abraham 和 Robert Weaver。

本书的技术审阅者对本书的内容进行了仔细的审查并提出了许多建议。他们是：Joe Balsama、Steve Rago、Ed Skoudis、Steve Romig、David Rhoades、Vernon Schryver、Peter Gutmann、John Sinteur、Will Morse、John Sebes、Howard Harkness、Chris Kostick、Bruce Schneier、Elizabeth Zinkann、David Weisman、Alain Mayer、John Stewart、Joshua Guttman 和 Harlan Carvey.

Mary Hart、 Emily Frey 和 Patrick Peterson 以及 Addison-Wesley 的其他工作人员也做了大量的工作，他们指导我们，将我们的经验在书中得到最好的体现。我们要特别感谢我们的编辑 Karen Gettman，是他最初提出了创作该书的建议，并在整个创作过程中一直给予我们支持。

我们将本书献给我们的孩子，Bobby、Caity、Cassidy Kruse 和 Kirk Heiser，以及我们的夫人 Maryann Kruse 和 Elizabeth Heiser，感谢他们在我们写书的这两年里给予我们的支持。

W.G.K 和 J.G.H

此为试读，需要完整PDF请访问：www.ertongbook.com

前 言

如今，每年由犯罪造成的损失多达数十亿美元，其中越来越多的犯罪牵扯到计算机。显然，执法机关需要对数字证据进行调查，但是鼓励一批计算机管理员去充当联邦调查员有意义吗？我们是否真的需要业余的数字侦探？简单地说，是的。当计算机本身发生了什么坏事儿或使用计算机干了什么坏事儿的时候，计算机的责任者往往需要知道在这些机器上到底发生了什么。你不可能在每次服务器出问题的时候都打电话找执法人员，希望他们派出取证专家来进行处理。即使你可以做到，你公司的主管也可能不希望你这样做。所有的大型公司都有自己的安全部门，他们整日忙于公司内部的安全事件调查。然而，所谓的安全专家通常只是处理盗窃和日常安全问题，而在处理计算机犯罪方面总是缺少准备。

本书的需求是由参加作者举办的计算机取证培训班的人们所提出的，从这些每次都爆满的培训班中我们可以得知，对数字调查的更专业知识存在着大量的需求。本书的读者对象是系统管理员和公司的安全人员。大部分学员都非常擅长使用和维护微软的操作环境，他们中的一些人同时也是 Unix 专家，但是还是有许多人迫切希望多了解一些 Unix 方面的知识。在实际情况中，一旦某个公司发现某人可以对 Windows 下的安全事件进行调查，他们就认为此人对计算机无所不知，除非此人有一天在 Unix 系统调查中陷入困境。

我们的学生有多种背景，有不同的调查需求和期望。我们尽量在本书中覆盖培训班上的所有内容，并将我们在调查和事件响应方面的经验介绍给读者。Warren Kruse 曾是一名警员，他现在负责朗讯科技公司内部和外部的计算机取证的检验。Jay Heiser 是一名信息安全顾问，曾经在一个应急响应组工作，参与了无数次 Internet 服务器攻击事件的响应。我们尽力使本书能够覆盖我们在调查过程中和培训时遇到的所有有用的信息。我们知道学员们会提出什么样的问题，本书就是为回答这些问题而写的。在进行计算机犯罪的调查取证过程中，本书可为读者提供实用的指导与帮助。

如何阅读本书

本书可以作为精读材料逐章阅读，此时它是一本计算机取证的入门教材。不过，本书

也可以作为一本手册，我们希望读者已经对本书包含的某些内容有所了解。为此，我们将每一个章节设计成完整、独立的单元，以便在必要时或方便时阅读其中的章节。你可能是本书介绍的某些领域的专家，然而我们相信本书涵盖了法律和计算机文化方面最起码的知识，我们还是希望读者能够对本书涵盖的各个领域（包括法律、程序和技术等方面）都有所了解。

下面是对每章内容的简要介绍。

计算机取证概述

第 1 章概要介绍了证据收集和分析的过程，这也是计算机取证的主要组成部分。即使是那些有法律背景的读者也将通过此章了解到计算机取证的特殊新技术。

跟踪罪犯

互联网现已非常普及，你的调查大部分都是涉及到出入网络的互联网流量。第 2 章的内容将会帮助你解析出包含在邮件和消息中的线索。这里也将是你成为一个网络侦探的起点，你可以通过此章了解如何使用标准的因特网服务进行远程调查。

硬盘驱动器和存储介质基础

对计算机侦探来说，硬盘是证据的重要集散地。第 3 章对硬盘的逻辑和物理配置进行了讲解。本章涵盖了分区、低级格式化、文件系统和硬件驱动接口等内容。

加密和取证

密码技术已在互联网的虚拟世界中非常普遍。一个高水平的调查人员必须对现代密码学的技术和目标有一定的了解。密码技术不仅有助于理解证据，还与证据的保存密切相关。许多调查人员都缺乏对密码技术的充分了解，所以在第 4 章中对加密技术进行了全面的介绍，并特别强调了它在计算机取证中的重要性和会用到的应用程序。在本章里我们同样也讨论了一些常用的编码和存档格式(例如 uuencode 和 PKZIP)，这些方法可以使得关键词搜索极为复杂。随着数字签名技术在法律上获得认可并被投入到新的用途中，取证调查人员必须掌握这些技术的限制，并且知道在什么情况下数字身份可能遭到窃取。证物的数字时间戳将会成为数字调查中的标准过程。如果你已经非常熟悉这些加密技术，就可以跳过本章。

数据隐藏

发现隐藏数据是一项至关重要的调查技术。即便你是高级的密码学专家，仍有可能不了解隐写术（将数据隐藏在其他信息之中的方法）和其他的数据隐藏技术。继续上一章加密技术，第5章描述了我们在实际调查取证过程中所使用过的一些实用的密码破解工具。本章对隐藏数据的方法（不只是通过加密进行隐藏的方法）进行了分类和描述，并为如何发现和读取隐藏数据提供实际性指导。

恶意代码

能够识别和理解犯罪隐含的犯罪工具是每个调查人员必备的技能之一。编写恶意代码的难度较大，很少有读者具有这方面的经验，第6章主要是对恶意代码做一介绍并对调查人员在实际中可能遇到的数字犯罪工具的种类和功能作了一个总体分析。其中包括了对近来越来越频繁出现的一些针对计算机群体的黑客工具的描述。

取证电子工具箱

虽然专用的取证工具犹如James Bond(电影007的男主角)一样具有无穷的魅力——我们将会介绍这些产品——但你在工作中用得最多的还是系统工具，尽管它们不是为取证调查而设计的。第7章将介绍大量的各种各样的工具类型和特殊品牌名称的工具，同时也描述了这些工具在数字调查中的用法。

调查 Windows 计算机

微软的Windows系列是目前家庭用户中使用最广泛的操作系统。在第8章中我们假设你已拥有一些Windows的工作背景，但也不是说你必须是一名微软认证系统工程师（MCSE）才能应用我们讨论的技术和技巧。本章重点讨论的是Windows NT 4.0和Windows 9x，此外还涉及到一些Windows 2000中出现的重要特性，例如加密文件系统。经验丰富的调查人员都知道调查对象必然具有多样性，所以本章还对Windows 3.1作了一些介绍。

取证员 Unix 入门

对于那些没有Unix经验的读者，第9章对Unix的特征加以重点介绍，这对取证调查人员相当重要。有Unix使用经验的读者可以跳过本章。

攻击 Unix 主机

希望第10章可以作为调查被攻击的Internet 主机的背景资料。本章描述了Unix 攻击者沿用的一般过程，并且对典型的系统攻击者的目的进行分析。

调查 Unix 主机

在介绍Unix 主机攻击的基础上，第 11 章给出了各种方式的Unix 调查技术。本章中包含使用Unix 系统提供的通用工具进行证据收集和评估的一组专门用于Unix 的技术和过程。此外本章还将教你在无法直接访问到可疑系统时，如何使用一个 Unix 引导光盘通过网络捕获信息。

美国司法系统简介

最后一章告诉你在开始收集证物后该做什么，并概要介绍了犯罪司法程序。本章涉及到许多法律上的概念，如书面陈述、传票和担保。如果你理解法律系统中每个机构做什么、调查和起诉的组织结构，那你就能更有效地在法律部门和你的单位之间工作。

附录

就像大部分的书一样，本书的附录包含的信息并非处处适用，而是针对某些具体问题。它主要是对特别的需求进行指导。

附录 A：网络数据中心响应准则。为处理网络数据中心的计算机安全事件定义了一个安全响应的过程。

附录 B：事件响应调查表。给出了在调查计算机犯罪事件时经常遇到的一些问题的列表。

附录 C：怎样成为 Unix 高手。为那些想提高调查 Unix 系统能力的取证人员提供自学方面的建议。

附录 D：导出 Windows 2000 的个人证书。形象地描述了从 Windows 2000 计算机中导出个人证书的过程。调查人员需要按照上面的过程准备自己的个人证书以备在调查涉及到加密文件系统的事件时使用。

附录 E：怎样“撬开”Unix 主机。描述了如何通过软盘或光盘启动系统来获得 Unix 系统管理员权限的过程。

附录 F：创建 Linux 启动光盘。提供了一些技巧和技术资料，这些资料可以帮助你创建启动光盘。使用这种光盘，你可以“撬开”Unix 或 NT 系统。通过启动 Linux 启动光盘

可以进入一个可信任的环境，在这里可以对证据进行测验和采集而不需要将硬盘从机器中取出。

附录G：取证光盘的内容。给出了一些实用工具列表和组成取证工具箱的最小配置。

目 录

此为试读，需要完整PDF请访问：www.ertongbook.com

第1章 计算机取证概述

每当我们告诉别人自己从事“计算机取证”工作时，人们无一例外的反应是“那很有意思”，然后问，“什么是计算机取证？”。尽管很少有人知道通过研究计算机可以获知操作者的行为，但大多数人都对传统的取证形式比较熟悉，并且对取证这一话题确实很感兴趣。这使得我们对计算机取证的介绍相对容易一些。

1.1 什么是取证

20世纪，人们在侦破案件的过程中越来越多地使用系统的调查方法，公众对侦探从事的工作也越发好奇。派翠西亚• 康威尔的小说不仅是很棒的读物，它们同时也给读者提供了对取证方法较为综合的理解，所以对于这些书籍在21世纪初如此畅销，我们丝毫不会感到意外。公众对案件侦破持续的兴趣直接导致有线电视中连续播放一系列相关的记录片，以此来吸引观众。2000年秋季播出的一部系列剧也是讲述警方的取证人员的冒险经历。后来，大众传媒开始把注意力从历险转移到案件的其他方面。很明显，取证以及计算机取证[1]正在成为热门的话题。为什么？不仅因为它的魅力，还在于它的必要性。人们都喜欢神秘的东西，但是对犯罪事件的调查更加能吸引人心。在调查犯罪、为公正而战斗的过程中，综合使用人类的智慧、高科技的工具以及严密的方法，对每一个人来说都是难以抗拒的。

1.2 计算机犯罪日趋严重

对计算机的不适当使用通常可分为两类：计算机被用作犯罪的工具，或是计算机成为犯罪侵害的目标。现在的机构中，计算机是无所不在的，它也不可避免地被牵涉到种种非法事件中。儿童色情、威胁信件、敲诈以及偷窃知识产权等都是常见的涉及数字技术的犯罪。对这类案件的调查通常包括对可疑计算机设备的搜索，这种分析工作可能涉及在数吉字节的数据中查找特定的关键字，分析日志文件查找某一时刻发生的事件，并希望借此证明某人曾经

[1] 计算机取证涉及到对计算机介质的保存、识别、提取、归档和解释，以作为证据或者作为动机分析的依据。请继续阅读，以获取更多详细的描述。

此为试读，需要完整PDF请访问：www.ertongbook.com