应急响应&计算机司法鉴定

（第2版）

Kevin Mandia　Chris Prosise　Matt Pepe　著
汪青青　付宇光　等　译

囊括所有司法鉴定内容和真实情景

Foundstone公司的计算机犯罪专家编写，FBI前专员Scott Larson为本书作序

“揭开计算机司法鉴定和分析的法律、规程与技术步骤的内幕。”

——*Information Security* 杂志

清华大学出版社

应急响应&计算机司法鉴定

(第2版)

Kevin Mandia

Chris Prosise 著

Matt Pepe

汪青青 付宇光 等 译

清华大学出版社

北京

Kevin Mandia, Chris Prosise, Matt Pepe
Incident Response 2nd
EISBN: 007222696X

Copyright © 2003 by The McGraw-Hill Companies, Inc.

Original language published by The McGraw-Hill Companies, Inc. All Rights reserved. No part of this publication may be reproduced or distributed by any means, or stored in a database or retrieval system, without the prior written permission of the publisher.
Simplified Chinese translation edition is published and distributed exclusively by Tsinghua University Press under the authorization by McGraw-Hill Education(Asia) Co., within the territory of the People's Republic of China only (excluding Hong Kong, Macao SAR and Taiwan). Unauthorized export of this edition is a violation of the Copyright Act. Violation of this Law is subject to Civil and Criminal Penalties.

本书中文简体字翻译版由美国麦格劳-希尔教育出版(亚洲)公司授权清华大学出版社在中华人民共和国境内(不包括中国香港、澳门特别行政区和中国台湾地区)独家出版发行。未经许可之出口视为违反著作权法,将受法律之制裁。未经出版者预先书面许可,不得以任何方式复制或抄袭本书的任何部分

北京市版权局著作权合同登记号 图字:01-2003-2188 号

版权所有,翻印必究。举报电话: 010-62782989 13901104297 13801310933
本书封面贴有 McGraw-Hill 防伪标签,无标签者不得销售。

图书在版编目(CIP)数据

应急响应 & 计算机司法鉴定(第 2 版). 曼迪尔(Mandia, K.), 普罗西斯(Prosise, C.), 皮皮(Pepe, M.)著; 汪青青, 付宇光等译. —北京: 清华大学出版社, 2004.11
ISBN 7-302-09727-5

Ⅰ. 应… Ⅱ. ①曼… ②普… ③皮… ④汪… ⑤付… Ⅲ. 电子计算机—安全技术 Ⅳ. TP309

中国版本图书馆 CIP 数据核字(2004)第 105390 号

出 版 者: 清华大学出版社
http://www.tup.com.cn
社总机: 010-62770175
地 址: 北京清华大学学研大厦
邮 编: 100084
客户服务: 010-62776969
责任编辑: 常晓波
封面设计: 立日新
印 刷 者: 世界知识印刷厂
装 订 者: 北京鑫海金澳胶印有限公司
发 行 者: 新华书店总店北京发行所
开 本: 185×230 印张: 26.75 字数: 594 千字
版 次: 2004 年 11 月第 1 版 2004 年 11 月第 1 次印刷
书 号: ISBN 7-302-09727-5/TP·6725
印 数: 1~3000
定 价: 49.90 元

本书如存在文字不清、漏印以及缺页、倒页、脱页等印装质量问题,请与清华大学出版社出版部联系调换 联系电话: (010)62770175-3103 或(010)62795704

前　言

我(Scott K.Larson)做了 13 年 FBI 特别调查员，现在是一家咨询和技术服务公司的执行副总裁，参与了高技术犯罪的预防、侦测、调查和取证工作。作为 FBI 调查员，我调查过计算机入侵、拒绝服务攻击、在线儿童色情文学、专用分组交换机/语音邮件欺骗、侵权、恶意代码/病毒/蠕虫和 Internet 欺骗。作为 FBI 实验室计算机分析和响应小组(Computer Analysis and Response Team，CART)司法鉴定领域的审查员，我收集了各种调查的计算机/电子证据，包括上面提到的内容，以及社会腐败、毒品交易、银行抢劫、团伙犯罪和白领犯罪。作为督察员，为 FBI 总部计算机调查部提供程序管理服务，监察计算机犯罪领域的 56 个办公室。作为美国国家基础设施保护中心培训和继续教育部(National Infrastructure Protection Center's Training and Continuing Education Unit，在这里看到了来自 Kevin Mandia 的第一手的知识、技巧和专业经验)的培训开发人员和程序管理员，我创建并合作开设了计算机犯罪调查、网络调查和基础设施保护课程。最后，作为现场调查的管理人，我不停地调查计算机入侵、拒绝拒绝攻击、恶意代码/病毒/蠕虫和非法数据截取(嗅探器)，包括反间谍行动、网络恐怖、犯罪、间谍和私人-公共合作程序，通过联合其他部门，如 InfraGard 和 ANSIR(美国国家安全突发事件和响应识别)，来防止计算机犯罪。

按照我的经验，即使在具有健全的安全基础设施的最好的政府和各行业系统，可以说外部和内部入侵仍然会持续存在。9·11 事件后的环境提醒我们，国家和网络安全的全球威胁受制于犯罪分子和恐怖分子集团的毁灭性想象力。在 FBI 工作期间，我看到 Robert Hanssen 有效地使用 FBI 的计算机系统对美国进行间谍活动。而恐怖集团想获得达到非法目的所需的攻击工具和技术。因为网络计算、犯罪动机、敌对情报服务和恐怖分子的普遍存在，所以应急响应和计算机司法鉴定的需求正在扩展。

好消息是，周边安全技术的有效性和分析能力正在提高。计算机司法鉴定技术也同样如此。但是，未知因素是管理和分析计算机数据的人。不管是执法官员、私人调查员、信息安全专家、顾问，或者是其他安全专家，成功防止和响应网络威胁的关键在于对计算机证据的合理鉴定、收集、保存和分析。本书提供了有效响应突发事件、收集计算机司法鉴定证据和分析合适的日志、文件所必需的知识、技巧和工具。这同时提高了各单位对突发事件的处理能力，或者事发前就汲取了教训。一盎司的预防效果等于一磅的治疗。

另外，本书还介绍了如何获取可能留下痕迹的位置和可能的对调查目标的警告，从而可以帮助公司或司法部门调查员主动执行在线调查。现在，公司的宝贵资料通常放在计算机中，这容易受到知识渊博的内部人员或机智的计算机黑客的攻击，他们可能敲诈你、贩卖信息，或将信息公布到 Internet。当然，如果需要处理敏感问题，那么在采取措施之前，

应该咨询安全部门、律师、知识丰富的计算机司法鉴定咨询公司(最好有执法或情报方面的经验)或执法机构。

总而言之，每个信息安全专家——不管是系统管理员、调查员、顾问或者执法官员——都应该遵循本书的建议。信息系统内忧外患，受过良好训练的协同保护、应急响应和司法鉴定分析团队对于所有要保护自身和财产免受网络威胁的组织而言，都是必需的。

Scott K. Larson
Stroz Friedberg, LLC 执行副总裁
www.strozllc.com

Scott Larson，前 FBI 特别调查员，是 Stroz Friedberg，LLC 公司明尼阿波利斯办事处执行副总裁和常务董事 Stroz Friedberg，LLC 公司是在网络犯罪响应、计算机司法鉴定和计算机安全领域领先的咨询和技术服务公司。

致谢

感谢下面所有人：Curtis Rose，他是我们所知的最有条不紊、最谨慎的计算机调查员。Keith Jones 坚韧不渝。Richard Bejtlich 编写了本书中的两章，他是我所知的学习知识最快的天才。Julie Darmstadt 完成了我们没有完成或无法完成的任务。1988 年拉斐特大学足球队教练组。Michele Dempsey 非常勤勉，而且颇具创造力，熠熠生辉。Dave Pahanish 谱写了伟大的歌曲。一起旅行的 Bruce Springsteen。Rick 拍摄了所有的精彩照片。Tim McNight 透露了 Kevin 经常去的地方。Eleanor Poplar 女士有一座很好的海滨别墅，并让 Kevin 使用。Matt Frazier 接受了顾问位置，最可信任。Jay Miller 的哲学讨论和疯狂的饮食习惯。Stephanie 是作者的知己，具有尚未发掘的文学天赋。Brain Hutchison 是敬业的榜样。Tom Mason 维护电源供给。Laine Fast 老把红笔放在破的后袋中。Mike Dietszch 再次败给了 Kevin。Dave Poplar 在注意到多起突发事件后，及时提供了简洁的法律建议。

还要感谢 FBI、AFOSI 和 AFIWC 的许多人，他们教会了我们很多知识，包括 Greg Dominguez、Chuck Coe 和最初的实验室工作人员：Jon、James、Cheri、Jason 和 Rob 等，真希望有机会报答你们。

如果没有 Osborne 小组(特别是 Jane Brownlow、Carolyn Welch 和 Marilyn Smith 无尽的耐心和持续的努力)本书无法完成，在此十分感谢。

此为试读，需要完整PDF请访问：www.ertongbook.com

作者简介

Kevin Mandia

Kevin Mandia 是 Foundstone 公司(一家 Internet 安全公司)计算机司法鉴定部(Computer Forensics)的主管。作为特别调查员、顾问和讲师，Kevin 在执行应急响应和计算机司法鉴定方面积累了大量的经验。

在加入 Foundstone 公司之前，Kevin 是美国空军特别调查办公室(Air Force Office of Special Investigations，AFOSI)的特别调查员，专门调查计算机入侵事件。离开 AFOSI 之后，Kevin 开设了为期两个星期的计算机入侵响应课程，特别制订了对 FBI 的要求。Kevin 在 FBI 学院教授了一年多的课程，在这里有超过 300 名专攻计算机入侵事件的 FBI 调查员参加了他的课程。课程的内容是根据法律实施、情报人员和某些特定个体(他们必须理解计算机网络的工作方式和黑客利用网络漏洞的方法)的特殊需要而量身定制的。Kevin 还为其他客户提供计算机入侵和司法鉴定培训课程，这些客户包括美国国会(State Department)、加拿大皇家骑警(Royal Canadian Mounted Police)、美国中央情报局(CIA)、美国国家航空航天局(NASA)、Prudential 公司以及一些国际银行和美国空军(United States Air Force)。

在 Foundstone 公司，Kevin 领导着一个计算机司法鉴定专家小组。在过去两年内，他们对 50 多起计算机安全突发事件作出了响应，这些事件涉及电子商务、金融服务和卫生保健组织。这些突发事件范围从有组织地偷盗数百万美元的商品，到对知识产权的盗窃，类型各异。

Kevin 从拉斐特学院(Lafayette College)获得计算机科学学士学位，从乔治·华盛顿大学(George Washington University)获得司法鉴定科学(Forensic Science)专业的硕士学位。他通过了信息系统安全专家认证(Certified Information Systems Security Professional，CISSP)，在卡内基·梅隆大学(Carnegie Mellon University)为研究生讲授应急响应课程。

Chris Prosise

Chris Prosise 是 Foundstone 公司专业服务部(Professional Services)的副总裁。他是该公司的合伙创建人，并启动了 Foundstone 公司的国际性专业服务业务。这种业务扩张使公司从早期的启动阶段发展到全球 500 强之一，为其独特的商业需要奠定了强大的、长期的安全基础。

Chris 在安全咨询和应急响应方面具有广泛的经验。作为卡内基·梅隆大学的助理教授，他向研究生讲授计算机安全方面的最新技术，并担任系顾问。Chris 在 Networld+Interop、

Infragard、LegalTech 和 FIRST(Forum of Incident Response and Security Teams，应急响应和安全小组论坛)等会议上成为受人瞩目的演讲者，不过，他更喜欢在弗吉尼亚州的农场种树和饲养野生动物。

Chris 的信息安全生涯是从他在美国空军信息战研究中心(Air Force Information Warfare Center)服役时开始的。在那里，他负责最高机密的政府网络应急响应和安全任务。他还开发了自动化的网络漏洞评估软件，并编写了实时入侵侦测和拒绝软件。Chris 在杜克大学(Duke University)获得电子工程专业的学士学位，并通过了信息系统安全专家认证(CISSP)。

其他撰稿人简介

Matt Pepe

Matt Pepe 是 Foundstone 公司的首席司法鉴定顾问。作为司法鉴定分析员和顾问，Matt 为美国空军特别调查办公室、FBI 和其他政府部门执行了 100 多起联邦调查的司法鉴定工作。

加入 Foundstone 公司之前，Matt 是美国空军特别调查办公室的计算机司法鉴定分析员。他是该组织的第一批非调查员的分析员，为美国国防部(Department of Defense，DoD)计算机司法鉴定实验室的成立做出了贡献。在这个位置上，他在媒体上对大量不同案例进行了评论，包括未经授权的入侵、欺骗和反间谍活动。

离开 AFOSI 后，Matt 为 FBI 国家基础设施保护中心(National Infrastructure Protection Center)提供技术调查支持。另外，Matt 领导着网络渗透测试小组，并参与开发了某个企业的入侵侦测系统。

在 Foundstone 公司，Matt 负责应急响应和司法鉴定工作，并指导应急响应和司法鉴定实践的研发工作。

Richard Bejtlich

Richard Bejtlich 是 Foundstone 公司的首席司法鉴定顾问。他从事应急响应、数字司法鉴定、安全培训工作，并提供网络安全监控方面的咨询。

加入 Foundstone 公司之前，Richard 是 Ball 航空技术公司(Ball Aerospace & Technologies Corporation)的高级工程师，负责管理网络安全操作。在此之前，Richard 是美国空军计算机应急响应小组(Air Force Computer Emergency Response Team，AFCERT)的组长，职责是保护全球范围内的美国信息资产。他领导 AFCERT 的实时入侵侦测任务，管理 60 多个民间和军方的分析员。

Rechard 受过正规的军事情报员培训，获得了哈佛大学(Harvard University)和美国空军

学院(United States Air Force Academy)的学位，并通过了信息系统安全专家认证(CISSP)。而且 Richard 还是《*Hacking Exposed* 第 4 版》和本书第 1 版的撰稿人。

技术编辑简介

Curtis Rose

Curtis W. Rose 是 Sytex 有限公司调查与司法鉴定部(Investigations & Forensics)的主管。Rose 先生以前是反间谍专员，是公认的司法鉴定和应急响应专家。他为美国司法部(U.S. Department of Justice)、FBI 的国家基础设施保护中心(National Infrastructure Protection Center)、空军特别调查办公室、美国陆军、公司实体和国家法律实施组织提供了调查支持和培训。

Rose 先生开发了专门的软件，用来识别、监控和跟踪计算机黑客。另外，他还写了(宣誓属实可用做法庭证据的)书面证词，并以专家身份在美国联邦法庭(U.S. Federal Court)上作证。

序　言

根据 Internet 调查公司 comScore 的资料，2002 年第 1 季度通过 Internet 售出的商品和服务价值超过了 170 亿美元。金钱来到哪里，犯罪就随之而来。最近几年，从我们对突发事件的响应看，计算机犯罪的首要目标是金钱。在我们响应工作中，几乎每次与计算机入侵伴随而来的都是信用卡欺骗、敲诈，或者是窃贼进行欺诈性买卖，犯罪分子在电子商务站点盗取了合法的客户证书。这些入侵很可能导致身份信息失窃。具有个人的足够信息后，犯罪分子可以制造假的证书并从那些不知情的用户的银行账户里支出现金。现在，攻击者在寻求经济利益方面比过去更加高效、更具侵略性。

新规则和新标准间接或直接影响着组织团体对计算机安全突发事件的响应能力。因此，本书说明了调查计算机安全事故的专业方法，以帮助组织团体遵循新标准和新规则要求，并减小损失。

在调查计算机安全事故过程中，未经训练的系统管理员、执法官员或者计算机安全专家可能意外破坏了有价值的证据，或者不能发现非法的或未授权的行为的关键线索。我们的经验证明：由于缺乏培训，大大降低了缉拿外部和内部攻击者的效率。

此外，计算机司法鉴定从只有内行才懂的技能发展为具有所有权的专业技能。几乎每家执行司法鉴定分析工作的公司都开发了许多专有的工具而并不对外共享。另外，只有执法人员可能得到较多司法鉴定培训，虽然对安全事故的最初响应多数是由每日劳累过度的系统管理员处理的。因此，本书提供了详细的技术实例，演示了进行计算机司法鉴定和分析的方法。许多在线出版物和书籍讲解了应急响应的结构和指导原则，不过这通常是分散的、过期的，不太适用于目前面临的挑战。

本书适用读者

如果曾经因为某人攻击了你的 Web 页面而在凌晨两点接到过电话，那么你应该阅读本书。如果管理人员请你查找是否有雇员向竞争对手发送私有的秘密信息，那么本书也适合你。如果惊惶失措的用户给你发送消息说计算机常常崩溃，那么你也应阅读本书。本书提供了你所需的详细的、法律上有效的技术响应。

- 调查源代码或私有信息失窃事件。
- 调查密码文件或信用卡信息被盗事件。
- 调查广告垃圾邮件带来的折磨和威胁。
- 调查对计算机系统的未授权入侵或非法入侵。

- ■ 调查拒绝服务攻击。
- ■ 对犯罪、欺诈、情报和安全调查提供司法鉴定支持。
- ■ 为公司的计算机事故和计算机司法鉴定事件担当关键角色。
- ■ 为计算机搜索和查询提供现场帮助。
- ▲ 遵守提高应急响应能力的新规则、标准和法令。

特别设计的辅助阅读元素

图标

下面的图标代表在本书中即将看到的标题：

可能发生的情况

简要描述会发生的情况。在每种突发情况发生之后，都将说明响应该突发情况的方法，或者查找证据的地方，这里使用特殊的图标。

查找证据的地方

如果需要，可去那里查找证据。

执法提示

该图标表示执法人员需要注意的内幕技巧，以维护美国公司的利益。

法律问题

该图标警告你在响应突发事故时应考虑的法律问题。
另外还提供了许多强化视觉效果的图标，以突出经常忽略的细节问题。

注意

警告

框符元素

除了图标外，本书还包括几种工具条。

目击者报告

描述调查过的真实事故，并提供解决事故的内部信息。

案发现场 请勿毁坏

通过详细的场景描述，就好像发生在你的身边一样，以此来建立犯罪现场。这与“可能发生的情况”不同，因为这里提供更多场景细节。

网络资源

代表本书中的一组参考信息的 Web URL。

本书的组织方式

本书的基本组织结构是根据最常面对的事故类型，向读者展示现实的场景，然后对最流行的操作系统中留下的痕迹做出鉴定。本书给出了非常特定而详细的例子，并鼓励提出解决司法鉴定问题的创造性方法。我们在维护证据完整性、记录和共享发现的信息方面也集中了大量精力。本书分成 4 部分，最后一部分是附录，下面分别进行说明。

第 1 部分：简介

本书第 1 部分建立了执行突发事故响应和计算机司法鉴定所需知识的基线。该部分提供了足够多的真实的例子，以深刻了解计算机安全事故。全面讨论了应急响应和计算机安全调查过程、组织团体提高应急响应能力以便成功保护财产的方法。深入研究了可接受的使用策略，并描述了它们对需要调查突发事故的人是否有所帮助。

第 2 部分：数据收集

对计算机安全事故的所有调查都要求收集信息。确切地说，要收集基于主机的证据、基于网络的证据和其他非技术证据，以便确定发生了什么、怎么解决问题。因此，该部分介绍了从现场计算机系统获取基于主机的信息、从 Unix 和 Windows 系统收集易失性数据

此为试读，需要完整PDF请访问：www.ertongbook.com

的方法。还深入讨论了获取司法鉴定副本的方法，以便收集计算机系统的完整内容。叙述了利用流行的网络包捕获程序执行网络监控的方法，以便收集基于网络的证据。还将讨论在调查计算机安全事故时，与系统管理员、管理人员和其他人员交流，以获得证据的方法。

在收集信息过程中，不要忽略下面的事实：必须以有利于鉴定的方式来获取和处理信息。因此，讨论了对所收集证据的归档和维护的细节。

第 3 部分：数据分析

学习了以司法鉴定方式收集信息后，必须分析或解释信息，以得到有效结论，最终帮助调查和解决问题。该部分介绍了在 Windows 和 Unix 系统中挖掘和解释数据的方法。将用一章的内容来分析网络数据流，并深入讨论了工具分析——确定程序功能。

第 4 部分：附录

在每章结尾(不包括第 1 章)，都有与本章内容相关的问题。这些问题用于强调关键概念，并帮助读者使用学过的知识。因此，第 1 个附录(附录 A)提供了这些问题的答案。其他附录(附录 B)包括用于执行应急响应的一些例子，如采样证据标记、采样“随身工具包”检查表和其他计算机应急响应小组经常使用的方法。

在线资源

希望本书对你有所帮助，无论准备保护网络或响应突发事故。因为应急响应经常与技术非常相关，并要求使用特殊工具，所以我们提供了一些在线资源的链接。我们当然不能控制这些站点，但是我们创建了一个配套 Web 站点 http://www.incidentresponsebook.com，以维护当前链接，并根据需要对方法进行更新。如果有什么建议、工具或要增加的技术，请发电子邮件到 authors@incidentresponsebook.com。

目　录

第1部分　简　介

第1章　现实生活中的突发事件 1
1.1　影响响应的因素 1
1.2　跨国犯罪 2
1.2.1　欢迎来到 Invita 2
1.2.2　PathStar 阴谋 3
1.3　传统的黑客行为 4
1.4　小结 6

第2章　应急响应过程简介 7
2.1　计算机安全事件的意义 7
2.2　应急响应的目标 8
2.3　应急响应小组参与人员 8
2.4　应急响应方法 9
2.4.1　事前准备 10
2.4.2　发现事件 11
2.4.3　初始响应 12
2.4.4　制定响应策略 13
2.4.5　调查事件 17
2.4.6　报告 20
2.4.7　解决方案 21
2.5　小结 22
2.6　问题 22

第3章　为应急响应做准备 24
3.1　突发事件预防准备概述 24
3.2　识别风险 25
3.3　单个主机的准备工作 26

3.3.1 记录关键文件的加密校验和 26
3.3.2 增加或者启用安全审核日志记录 29
3.3.3 增强主机防御 34
3.3.4 备份关键数据 35
3.3.5 对用户进行基于主机的安全教育 37
3.4 准备网络 37
3.4.1 安装防火墙和入侵侦测系统 38
3.4.2 在路由器上使用访问控制列表 38
3.4.3 创建有助于监视的网络拓扑结构 39
3.4.4 加密网络流量 40
3.4.5 要求身份验证 40
3.5 制订恰当的策略和规程 41
3.5.1 决定响应立场 42
3.5.2 理解策略如何辅助调查措施 44
3.5.3 制定可接受的使用策略 49
3.5.4 设计 AUP 51
3.5.5 制定应急响应规程 52
3.6 创建响应工具包 53
3.6.1 响应硬件 53
3.6.2 响应软件 54
3.6.3 网络监视平台 54
3.6.4 文档 55
3.7 建立应急响应小组 55
3.7.1 决定小组的任务 55
3.7.2 对小组进行培训 56
3.8 小结 58
3.9 问题 58

第 4 章 应急响应 59
4.1 初始响应阶段概述 59
4.1.1 获取初步资料 60
4.1.2 应对措施备案 60
4.2 建立突发事件通知程序 60
4.3 记录事发详情 61
4.3.1 初始响应检查表 61

4.3.2 案例记录 63
4.4 突发事件声明 63
4.5 组建 CSIRT 64
4.5.1 突发事件升级处理 64
4.5.2 执行突发事件通知 65
4.5.3 审视突发事件并配备合适的资源 66
4.6 执行例行调查步骤 68
4.7 约见 68
4.7.1 获得联系信息 69
4.7.2 约见系统管理员 70
4.7.3 约见管理人员 70
4.7.4 约见终端用户 71
4.8 制定响应策略 71
4.8.1 应对策略注意事项 72
4.8.2 策略验证 72
4.9 小结 73
4.10 问题 73

第 2 部分 数 据 收 集

第 5 章 Windows 系统下的现场数据收集 74
5.1 创建响应工具箱 74
5.1.1 常用响应工具 75
5.1.2 准备工具箱 76
5.2 保存初始响应信息 77
5.2.1 应用 netcat 传输数据 77
5.2.2 使用 cryptcat 加密数据 79
5.3 获取易失性数据 79
5.3.1 组织并备案调查过程 80
5.3.2 收集易失性数据 81
5.3.3 编写初始响应脚本 89
5.4 进行深入的现场响应 90
5.4.1 收集最易失的数据 90
5.4.2 创建深入的调查工具箱 91
5.4.3 收集现场响应数据 91

5.5 制作司法鉴定复件的必要性 97
5.6 小结 98
5.7 问题 98

第 6 章 Unix 系统下的现场数据收集 99
6.1 创建响应工具包 99
6.2 保存初始响应信息 100
6.3 在进行司法鉴定复制之前获得易失性数据 101
6.3.1 收集数据 101
6.3.2 编写初始响应脚本 110
6.4 进行深入的现场响应 110
6.4.1 侦测可装载内核模块 rootkit 110
6.4.2 获得现场系统日志 112
6.4.3 获得重要的配置文件 113
6.4.4 查找系统中的非法嗅探器 113
6.4.5 查看/proc 文件系统 116
6.4.6 转储系统内存 119
6.5 小结 120
6.6 问题 121

第 7 章 司法鉴定复件 122
7.1 可作为呈堂作证的司法鉴定复件 122
7.1.1 司法鉴定复件 123
7.1.2 合格的司法鉴定复件 123
7.1.3 被恢复的映像 123
7.1.4 镜像 124
7.2 司法鉴定复制工具的要求 125
7.3 制作硬盘的司法鉴定复件 126
7.3.1 用 dd 和 dcfldd 复制 127
7.3.2 用开放数据复制工具进行复制 128
7.4 制作合格的司法鉴定硬盘复件 132
7.4.1 制作引导盘 132
7.4.2 用 SafeBack 制作合格的司法鉴定复件 134
7.4.3 用 EnCase 制作合格的司法鉴定复件 136
7.5 小结 139

7.6 问题 140

第 8 章 收集网络证据 141
8.1 网络证据 141
8.2 网络监视的目的 141
8.3 网络监视的类型 142
8.3.1 事件监视 142
8.3.2 陷阱跟踪监视 142
8.3.3 全内容监视 143
8.4 安装网络监视系统 144
8.4.1 确定监视的目标 144
8.4.2 选择合适的硬件 145
8.4.3 选择合适的软件 147
8.4.4 部署网络监视器 150
8.4.5 评价网络监视器 151
8.5 执行陷阱跟踪 152
8.5.1 用 tcpdump 进行陷阱跟踪 153
8.5.2 用 WinDump 进行陷阱跟踪 155
8.5.3 创建陷阱跟踪输出文件 155
8.6 用 tcpdump 进行全内容监视 156
8.6.1 过滤全内容数据 157
8.6.2 保存全内容数据文件 157
8.7 收集网络日志文件 158
8.8 小结 159
8.9 问题 159

第 9 章 证据处理 161
9.1 证据 161
9.1.1 最优证据规则 162
9.1.2 原始证据 162
9.2 证据处理 162
9.2.1 证据鉴定 163
9.2.2 保管链 163
9.2.3 证据确认 164
9.3 证据处理程序概述 165

此为试读，需要完整PDF请访问：www.ertongbook.com