THOMSON

信息安全丛书

计算机取证调查指南

[美] BILL NELSON,AMELIA PHILLIPS,FRANK ENFINGER, AND CHRISTOPHER STEUART 著

杜江 白志 刘刚 主译

重庆大学出版社

http://www.cqup.com.cn

计算机取证调查指南

（原书第2版）

[美]BILL NELSON, AMELIA PHILLIPS, FRANK ENFINGER, AND CHRISTOPHER STEUART 著

杜 江 白 志 刘 刚 主译

重庆大学出版社

Bill Nelson, Amelia Phillips, Frank Enfinger, and Christopher Steuart
GUIDE TO COMPUTER FORENSICS AND INVESTIGATIONS(SECOND EDITION)
ISBN: 0-619-21706-5

版贸核渝字(2005)第12号

图书在版编目(CIP)数据

计算机取证调查指南:原书第2版/(美)尼尔森(Nelson, B.)等著;杜江,白志,刘刚译. —重庆:重庆大学出版社,2009.1
书名原文: Guide to Computer Forensics and Investigations, Second Edition
ISBN 978-7-5624-4648-4

Ⅰ.计… Ⅱ.①尼…②杜…③白…④刘… Ⅲ.计算机犯罪—证据—调查—指南 Ⅳ.D915.13-62

中国版本图书馆CIP数据核字(2008)第137898号

计算机取证调查指南(第2版)
Jisuanji Quzheng Diaocha Zhinan
[美] BILL NELSON, AMELIA PHILLIPS, FRANK ENFINGER, AND CHRISTOPHER STEUART 著
杜 江 白 志 刘 刚 主译

出 版 者:重庆大学出版社 **地 址**:重庆市沙坪坝正街174号重庆大学(A区)内
网 址:http://www.cqup.com.cn **邮 编**:400030
电 话:(023) 65102378 65105781 **传 真**:(023) 65103686 65105565
出 版 人:张鸽盛
责任编辑:王 斌 戴倩倩 余筱瑶 **版式设计**:王 斌
责任校对:谢 芳 **责任印制**:赵 晟
印 刷 者:自贡新华印刷厂
发 行 者:全国新华书店经销
开 本:787×1092 1/16 **印张**:34.75 **字数**:701千
版 次:2009年1月第1版 2009年1月第1次印刷
书 号:ISBN 978-7-5624-4648-4
定 价:79.00元

前　言

近年来世界范围内发生的重大事件，已经影响和改变了我们对于证据收集的思考方式。2001年9月11日美国纽约世贸中心遭到袭击后不久，许多青年男女都自发地以不同的方式为国家效力。没有参军的年轻人，则选择加入了执法和安全机构。随着诸如CSI、罪案取证和NCIS等主流电视节目越来越受欢迎，加上国土安全问题重新被重视，使得对计算机取证领域方面的专家需求大增。这种需求正通过在全美的大专院校甚至高中所开设的计算机取证专业课程来得以满足。

然而，计算机取证绝不是一门还处于探索阶段的新兴领域。早在20世纪90年代，当时我在海军犯罪调查机构里担任特别调查员，就已经意识到个人电脑，更专业地说是无安全保障的个人电脑，给国家安全带来了潜在的威胁。那时，我开始指导对白领犯罪、网络攻击，以及通信诈骗等案件的取证调查。今天，大多数新的计算机取证专家可能会参与更广泛和更多样化的取证调查，包括反恐间谍活动、反洗钱、知识产权窃取、电子监视等问题。

不同的取证专家所必须具备的技能是不一样的。最低限度来说，他们必须具备深厚的刑事司法体系知识、计算机硬软件系统知识、调查和证据收集规范方面的知识。下一代的“电子侦探”将必须具备相应的知识、技能和经验，才能完成涉及多种操作系统和文件类型的、复杂的、数据密集型的取证调查工作。

随着时间的推移，计算机取证正由“综合学科”逐渐演变为数字化取证的“综合科学”。美国及英国的一些大学正在设置综合课程，并提供数字取证专业的学士和硕士学位。《计算机取证调查指南》对于计算机与数字取证专业的人来说，是一本非常重要的教科书，现在已有了第2版。我相信，这本原本主要用于高等院校的书，在一位充满激情、博学的老师的讲授下，将会是一门生动有趣的课程。

如今，除了电脑，数不清的个人数字设备都采用1和0的二进制编码。如果其中有设备保留了犯罪证据，那么以一种可靠合理的取证方式来找出这些数字证据，就是新一代训练有素、受过高等教育的电子侦探接下来要完

成的任务。这本书将帮助学生和专业人士来实现这个目标。

致礼

John A. Sgromolo

John 作为一名资深的特别调查员，曾是 NCIS 计算机犯罪调查小组的创始成员之一。之后，他离开了政府机构并开设了自己的公司——Digital Forensics 公司，向全国成百上千的执法人员与公司职员讲授了计算机取证与调查的技术与科学。现在，John 是 Verizon 公司数字取证领域的首席调查员。

简　介

虽然计算机取证作为一个专业领域已经存在很多年了，但在这个领域里大多数被认可的专家都是自学成才。随着互联网和计算机在全世界的广泛应用，对规范实施计算机调查取证的需求也日益增长。计算机可以被用作犯罪工具，这样犯罪活动就可能被记录在计算机中，包括违背公司政策的行为、侵吞公款、电子邮件骚扰、谋杀、泄漏隐私信息，甚至可能是恐怖活动。司法部门、网络管理员，甚至私人侦探现在都依赖于专业计算机取证专家的技术来进行刑事或民事调查。

本书不打算提供对计算机取证的完整培训，但是，它将通过对计算机取证的介绍，帮助那些刚进入这个领域的人打下一个坚实的技术基础。其他关于计算机取证的书籍主要是面向专家的，而本书主要面向对计算机和网络有一定基础的新手。

新一代的计算机取证专家需要更多的基础培训，因为现在的操作系统、计算机硬件和计算机取证软件工具比以前变化更快。本书涵盖了以前的和现在主流的操作系统，比如 Windows 9x、Mac OS 和 Linux，以及一系列计算机硬件，从低端的 PC 工作站到高端的网络服务器。本书除了主要介绍几个计算机取证软件工具外，对当前适用的其他工具也进行了比较和讨论。

本书的主要目标是指导你逐步成为一个熟练的计算机取证调查员，并帮助你通过专门的认证考试，不过随着计算机取证与调查领域的日渐成熟，认证考试是会改变的。其中最为著名的是国际计算机调查专家协会（IACIS）考试，它主要面向司法部门。第三章介绍了当前公布的认证考试，附录 A 对它们进行了更详细的阐述。

本书面向的读者

本书可以为具有不同背景的人所使用，主要面向那些具有 A + 和 Network + 认证或同等水平的读者。读者具有网络背景知识是很必要的，这样才能够理解 PC 计算机如何在网络环境里运行，并且当需要时如何与网络管理员一起工作。另外，读者必须知道如何通过命令行来使用计算机，如何使用流行的操作系统，包括 Windows 9x、Windows 2000、Windows XP、Linux、Mac OS，以及相关的硬件。

本书可以被用于从技术专科学校、社区学院到研究生培养等各种教育层次，也适用于正在从事这个领域工作的公众或私人机构的专业人员。每个读者群以不同的观点和方法去解决问题，但都可以从本书中获益良多。

本书新增内容

和第一版相比，本版的章节顺序进行了调整，所以读者首先看到的是计算机取证实验室里发生的事情，和他们在进一步深入学习之前如何建立计算机取证实验室。本版还新涉及了几种 GUI 工具，以便学生们能够熟悉一些常用软件。另外，由于个人数字助理(PDA)对市场的影响，本版也包括了如何使用它们的内容，并新增了一章关于网络取证的内容，目的在于向网络安全方面的专业人士介绍如何在该领域进行计算机取证。基于读者的反馈，我们对第一版进行了修订，并且升级了所有软件包和网站，以便反映出它们的最新动态。

章节说明

下面对本书中的所有章节做简要说明。

第一章，“计算机取证和调查专业介绍”，介绍了计算机取证的历史和电子证据的价值是如何得到认可的，还对相关法律问题及公众和私立机构的情况做了比较。

第二章，“理解计算机调查”，展示了一个贯穿本书的实用案例，并向你演示如何将科学技术应用到一起调查案件中。

第三章，“调查人员的办公室与实验室”，描述了如何构建一个理想化的计算机取证实验室，包括从小型的私人调查员实验室到地区 FBI 实验室，还介绍了数字证据调查员资格认证。

第四章，“目前的计算机取证工具”，探讨了目前常见的计算机取证工具，包括一些不容易得到的工具，并评价了它们各自的优缺点。

第五章，“处理犯罪和事故现场”，讲述了证据搜索和一个典型的计算机取证案例的真实过程。本章讨论了什么时候聘用第三方专业人士，如何组建一支团队，以及如何评估一个事件。

第六章，“数字证据保全”，强调了数字证据是特别容易被破坏和篡改的。本章还介绍了如何控制一个犯罪现场，以及确保证据的真实性，以便能在法庭上使用。

第七章，“在 Windows 和 DOS 系统下工作”，讨论了目前通用的操作系统。读者将了解到在计算机启动过程中发生了什么事情和什么文件被修改过，以及每个系统是如何处理被删除和释放出来的空间的。

第八章，“Macintosh 和 Linux 引导过程和文件系统”，承接第七章继续讨论 Macintosh 和 Linux 操作系统。本章还介绍了 CD、DVD、SCSI 和 RAID 系统。

第九章，“数据提取”，讲解如何从一个嫌疑人的磁盘中提取数据，并介绍了可用于命令行和图形界面操作系统的工具。

第十章，“计算机取证分析”，介绍调查计划制订以及如何为特定调查搭建取证工

作站。本章还给出了一个可供采纳的循序渐进的提取潜在证据的步骤。

第十一章,"恢复图像文件",讲解如何恢复证据磁盘上的图像文件,评价图像恢复工具,并介绍了数据压缩、图像重建,以及掩密技术和版权问题。

第十二章,"网络取证",介绍了可用于指导有关网络取证调查的工具和方法,及如何使用网络日志来收集网络入侵或犯罪事件的证据。

第十三章,"电子邮件调查",介绍了电子邮件和互联网的基本原理,并对电子邮件形式的违法犯罪进行了分析。还介绍了目前常用的一些电子邮件取证工具。

第十四章,"成为一个专家型证人并书写调查结果报告",揭示专家证人所扮演的角色,包括编写履历和跟踪记录你所获得的资格证明。它也描述了专家型证人和技术型证人的不同之处,以及如何为计算机取证调查编写口头的或书面的报告。

附录 A,"证书考试介绍",分析目前已有的几种认证。

附录 B,"计算机取证参考",罗列了本书中所用到的命令,深入探讨了脚本和 FAT 目录结构,并列出计算机取证调查方面的其他参考书。

附录 C,"企业高科技调查规范",概述了企业取证调查的步骤和清单,涉及 Internet 和 E-mail 滥用调查、雇员辞退及商业间谍案件等。

本书的特点

为了帮助你全面地理解计算机和网络安全,本书具有以下特点,旨在丰富你的学习体验。

■ 章节目标。每一章的开始详细地列出了该章需掌握的概念列表。此列表有助于快速查找该章内容,是一个非常有用的学习帮手。

■ 图形和表格。以屏幕拷贝方式来指导讲解命令和取证工具。对于那些未随本书提供的或没有免费版的工具,就以图形的方式来描述工具的界面。全书中,使用表格旨在以一种系统的、易掌握的方式提供信息。

■ 本章小结。每一章末尾,对该章所介绍的概念进行小结。这些小结有助于读者复习该章中的概念。

■ 关键术语。在每章小结后,关键术语表列出了该章引入的所有以黑体字标出的新术语,并给出了每个术语的完整定义。此列表使读者能够更全面地理解该章中的关键概念,起到参考作用。

■ 复习题。每一章最后都有一套用于评估测验的复习题,旨在巩固每一章的主要概念。这些题目能够帮助读者评估和应用所学的知识。

■ 练习题。尽管掌握计算机技术的理论知识很重要,但是如果不在实践中得以应用就不会有进步。出于这点考虑,每章都配备一些练习题,这些练习题会涉及本书提供的软件工具或免费下载的计算机取证工具。读者可以研究获取证据甚至隐藏证据

的不同方式。对于概念性的章节，我们还给出了研究课题。

■ 案例题。每一章最后是若干案例题，其中包括两个贯穿全书始终的案例。要完成这些作业，就必须运用一些常识和本书中与该要点相关的技术课题。对于每一章，你的目的就是针对将来作为一名计算机取证调查员也会遇到的问题，提出解决办法。

■ 软件和学生数据文件。包括案例题所使用到的学生数据文件，还有用在各章练习题和案例题的免费软件演示包(练习题和案例题中也使用了其他软件演示包或免费软件，它们可以从网上下载)。有三家软件公司允许我们在本书中使用他们的产品：Digital Intelligence 公司的 DriveSpy 和 Image(这些软件需在线注册才能使用)；Access Data 公司的 Forensics Toolkit、Password Recovery Toolkit、RegistryViewer 和 FTK Imager；还有 X-Ways、X-Ways Forensics。如需最新版本或其他相关信息，请访问这些公司：Digital Intelligence 公司主页为 www. digitalintelligence. com，Access Data 公司网址为 www. accessdata. com，X-Ways Software Technology AG 网址为 www. x-ways. net。

■ Encase 软件的演示 DVD。该 DVD 包括 Encase 软件的演示版本，一道专门的案例题，该演示版使用的证据文件以及用户手册和其他文件。想要获得关于 Encase 更多的信息，或者购买该软件的完全版，请访问 www. Guidance Software. com。

(软件和学生数据文件，演示 DVD 及教师素材，请登录我社教育资源网该图书页面点击“电子教案”下载，我社教育资源网的网址为 Http://www. cqup. net/edusrc/index. aspx。)

文字和图形说明

本书中加入了适当的附加信息和练习，旨在帮助你更全面地掌握手边的课题。文中采用了图标的形式以提醒读者注意一些附加的信息。这些图标如下所示：

备注图标提示你注意相关主题的其他有用信息。

技巧图标是以作者的经验为基础，提供关于如何解决问题或在实际情况下应该做什么的信息。

注意图标提醒你注意潜在的错误或问题，并告诉你如何避免它们。

本书中的每一道练习题前面都有练习题图标，随后是练习题的详细描述。

标有案例图标的是案例题，是有场景为基础的作业题。要求你将所学的知识独立运用到这些涉及面较广的案例中。

教师素材

在课堂上使用本书时，可以采用以下这些附加材料。你也可以在 Course Technology 的网站 www. course. com 上，找到本书的网页，在“Download Instructor Files & Teaching Tools”下面检索这些辅助教材。

电子教学手册。本书附带的教师手册包括以下内容：备课的辅助教学材料，包括对授课主题的建议，推荐的实验室工作，关于建立练习题实验室的建议，所有各章末尾习题的答案。

ExamView 考试题库。使用这个功能强大的基于 Windows 的考试软件，教师可以有效创建并管理考试和测验。除了能够创建可打印的、便于管理的考试，这个功能完善的软件还具有在线考试组件，使学生可以通过他们的计算机参加考试，并自动评分。

PowerPoint 演示文稿。本书为每章都提供了 Microsoft PowerPoint 幻灯片。这些幻灯片可作为教学辅助工具供课堂演示使用，使学生可以通过网络查看章节内容，或打印出来在课堂上分发。教师还可以制作授课所需的其他主题的幻灯片。

图形文件。教师素材上包括了书中所有的图形。与 PowerPoint 演示文稿类似，这些图片也可作为教学辅助工具供课堂演示使用，使学生可以通过网络查看章节内容，或打印出来在课堂上分发。

实验室需求

书中的练习题有助于读者运用所学的计算机取证技术知识。下面列出了完成书中所有练习题所需的最低硬件要求。除了这些要求以外，学生还必须会下载和安装演示软件。

最低实验室要求

- 计算机能够启动到实命令行状态下，运行 Digital Intelligence 公司 DriveSpy 和 Image 软件。因为 Windows XP 不允许某些程序运行，取而代之的办法是使用 DOS 启动盘并将相应版本的 DOS 标准外部命令文件存储到取证驱动器的一个文件夹中。
- 能启动到 Windows XP 或 2000 的计算机。
- 双重启动到 Linux 或 UNIX 的计算机。
- 至少有一台 Macintosh 计算机。

请记住，书中的调查取证步骤与方案都是在满足下列硬件和软件要求的条件下设计而成的。因为大多数的工作都是在实验室完成，所以它应该是一个典型的网络培训实验室，具有很多不同的操作系统和计算机，其中包括一台 Windows XP、2000 或 9X 计算机和一台 Linux 计算机。

操作系统和硬件

Windows XP 和 2000

应采用标准安装的 Home、Professional 或 Sever 版。运行 Windows XP 或 2000 的计算机应至少满足下面的条件：

- 3.5 英寸磁盘驱动器
- CD-ROM 驱动器
- VGA 以上的显示器
- 10 G 以上硬盘分区
- 鼠标或其他指示器
- 键盘
- 128 MB RAM

Windows 9X

有些步骤和方案要求我们使用的计算机能够直接启动到 DOS 提示符下。你也可以在这些计算机上运行 GUI 程序，但是它们可能会比下列所示的最低配置更加消耗内存。运行 Windows 95 或 98 的计算机至少应满足下面的条件。

- Windows 95-8 MB RAM，推荐至少为 24 MB。
  Windows 98-16 MB RAM，推荐至少为 24 MB。
- 至少 1 GB 的硬盘。
- 其他硬件要求与运行 Windows XP 的计算机硬件要求相同。

备注：正如上面提到的实验室的最低需要，只要外部命令都存放在软盘的文件夹中，就可以直接从 DOS 启动盘启动。

LINUX

本书假定你正在使用的是 Red Hat Linux 9 或 Fedora 标准安装。一些可选步骤需要 GIMP 图形编辑器，在 Red Hat Linux 中，该图形编辑器必须单独安装。只要为 Linux OS 预留了一个以上的 2 GB 分区，我们就可以将 Linux 安装到双重引导的计算机上。

- 为 Linux 预留至少 2 GB 的硬盘分区。
- 其他硬件要求与 Windows XP 计算机的硬件要求相同。

计算机取证软件

本书提供了两种计算机取证软件：DriveSpy 和 Image，它们均为 Digital Intelligence

公司开发。DriveSpy 和 Image 都是从纯 DOS 提示符下而不是 DOS shell 下启动的 DOS 程序。它们只能在 Windows 98 上运行。如果你想要使用这些软件的话，就要对系统进行包括纯 DOS 和 Windows 98 在内的双重引导安装。

本书包括涉及以下软件的步骤和方案，这些软件大多可以从 Internet 上下载，有免费软件、共享软件或免费演示软件。因为网站地址经常变更，所以在以下网址无效的情况下，请上网使用搜索引擎进行搜索。

- Digital Intelligence 的 DriveSpy 和 Image：如果你是一名公认的学术机构的教职员工，就请与 Digital Intelligence 公司联系，打听一下用作培训的 DriveSpy 和 Image 软件的学术研究授权。网址是 www. digitalintelligence. com。
- FTK：你可以从 www. accessdata. com 上下载 FTK 的演示版。从我们开始写这本书起，AccessData 公司就已经有教育软件包和教师培训，不过要收取一部分费用。
- EnCase：Guidance Software 公司的产品，被执法部门广泛使用。
- Hex Workshop：你可以从 www. hexworkshop. com 上下载 Hex Workshop 的测试版。也可以使用 Norton DiskEdit 或 WinHex 代替 Hex Workshop。
- X-Ways Forensics 和 X-Ways Replica：两者都可以在 www. x-ways. net 上进行下载。
- IrfanView：从 www. irfanview. com 上下载。
- NTFSDOS：可从 www. sysinternals. com 上下载。
- SecureClean：可从 www. accessdata. com 上下载。
- 掩密技术工具（建议使用 S-Tools）：可从 www. stegoarchive. com 上下载。
- Tom's Root Boot Kit：可从 www. tux. org 上下载免费版本。
- WinZip：可从 www. winzip. com/download. htm 上下载评估版。
- JASC Paint Shop Pro：从 www. jasc. com 上下载测试版。

另外，你要使用 Microsoft Office Word（或其他文字处理软件）和 Excel（或其他制表软件）。你还需要在计算机上安装诸如 Microsoft Outlook Express 或 Eudora 之类的 E-mail软件。

关于作者

Bill Nelson 在一家《财富》杂志排名前 50 位的企业担任首席计算机取证探员已有 8 年多的时间，且为许多专业机构和大学开发了高科技调查程序。他曾开发 AFIS（自动指纹鉴定系统）软件项目并参加过预备警察工作。Bill 一直担任着 CTIN（美国西北部计算机技术调查协会）的主席和副主席，现在是 CRIME（计算机信息管理和教育组织）的成员。他经常在位于美国西北部的几所学院和大学做报告。

Amelia Phillips 毕业于麻省理工学院，取得航天工程与考古学学士学位，技术管理 MBA 学位。他曾在喷气推进实验室担任项目师，之后与几家电子商务网站合作开始了

他在计算机取证领域的培训工作，旨在防止信用卡号码从敏感的电子商务数据库中被盗。她曾为研究方向是电子商务、计算机取证和数据恢复的社区学院开发了软件。现在她任教于 Washington 州 Seattle 市的 Highline 社区学院。最近，Amelia 被授予 Fulbright奖学金，用作该地区的执教和在非洲撒哈拉沙漠以南地区的研究。

Frank Enfinger 现任 North Seattle 社区学院的教授，同时也是当地警察局的一名计算机取证专家。在进入计算机行业以前，Enfinger 教授曾在美国海军陆战队服兵役。过了几年，他就开始为企业和政府部门做计算机技术工作，其中包括医院、ISP 和环保公司。他拿到了计算机科学专业的学位，且获得该领域内的很多证书，现在仍继续从事不断发展的技术工作。

Christopher K. Steuart 曾为一家《财富》杂志排行前 50 名的公司和美国陆军部队做过信息系统安全工作，现任 CTIN 的总顾问。他一直活跃于谈论计算机取证领域的地方或全国性的论坛，这些论坛包括 ASIS（美国工业协会安全）、Agora、NCTCAS（西北计算机技术犯罪调查研讨会）和 CTIN。

致 谢

我们要感谢编辑部主任 Will Pitkin，感谢他给了我们许多精神上的支持。感谢整个编辑部和出版人员在出书过程中所表现出来的忘我精神和坚强毅力，包括产品经理 Amy Lyon 和制作编辑 Kristen Guevara。我们要特别感谢策划编辑 Lisa Lord，以及品质保证部的测试员 Shawn Day 和 Danielle Shaw。还要感谢技术编辑 Mike McNown 和 John Bosco 的认真阅读和宝贵建议。感谢 Washington Tacoma 的 Pierce County Prosecutor 探员 Franklin Clark 的参与，及 Mike Lacey 为我们提供图片。此外，我们还要感谢认真核查每一章并提供了有用建议和贡献的评审员们：

Larry Anderson	城市社区学院
Mark Davis	Tulsa 大学
Michael Sthultz	Southern Nevada 社区学院
Bill Nelson	

我要感谢我的妻子 Tricia 在我长时间的写作期间对我的支持。还要感谢其他作者 Amelia、Chris 和 Frank，以及我们的编辑，感谢他们为出版本书所作的努力。特别要感谢我计算机取证行业同事们的支持和努力，他们是：Washington Tacoma 的 Pierce County Prosecutor 办公室的 Frank Clark；Mike McNown 侦探和已经退休的 Wichita PD；Stoz Friedberg LLC 公司的 Don Allison；Washington Seattle 的 King County Sheriff 反欺诈办公室的 Brian Palmer 探员，Barry Walden 探员和 Melissa 探员；Verizon 的 John Sgromolo。

Amelia Phillps

首先我要感谢让人愉快的学生团体，他们编辑了贯穿本书的纵火案案例。他们之

所以创编此案，是为了对当时 Seattle 地区肆意猖獗的纵火案作出回应。我要感谢 Travis Scott Anderson，Cesar V. Noche，Jr.，Lucas Reber，Eric Apple，Mike Danseglio 和 Seth Diaz。感谢上我课的来自 Seattle 地区的学生和一些企业。他们提供了很多的案例，让我大长见识。我想感谢本书的其他作者和朋友，谢谢他们在我们学习的过程中表现出的坚强和幽默。还要谢谢 Lisa Lord，是他促成了这次有趣的经历。

Frank Enfinger

首先，我要感谢家人对我的关爱、理解和支持，使我能够从“ol'man”的其他活动中抽出时间来进行写作。感谢本书的其他作者所做的一切，能和你们一起完成这本书是我的骄傲和荣幸。特别要感谢 Lisa Lord，感谢你为顺利出版此书所做的一切，以及过去几个月中你所提供给我们的帮助。还有我所有的顾问们，你们知道你们是谁——感谢你们！我对本书的贡献都直接源于你们提供给我的培训、工作和机会。最后，我要感谢本书的读者。感谢你们使用计算机取证技术正在做的和将要做的一切。

Christopher K. Steuart

我要感谢我的妻子 Josephine，儿子 Alexander 和女儿 Isobel，感谢他们对我完成本书的大力支持，尽管因此夺去了很多本应属于他们的时间和精力。感谢我的父母 William和 Mary，因为编写本书需要接受一些教育和培养一些技能，感谢他们对我的支持。感谢其他作者，Bill，Amelia 和 Frank 邀请我参与本书的写作。感谢中将（后来是上将）Edward Soriano，在我还是一名青年士兵时，是他看出我的潜力并鼓励我学习管理、交流的技能和步骤，以及在法律体系、法规和个人义务中的指挥和组织能力。感谢 Drake 大学法学院的教职员工，尤其是 James A. Albert 教授，他们鼓励我在法律方面进行创造性写作。

图片鸣谢

图 1.2：IBM 公司档案中的 8088 计算机

目 录