Digital Evidence And Computer Crime Second Edition

国外IT精品丛书

数字证据与计算机犯罪

（第二版）

[美] Eoghan Casey 著

陈圣琳 汤代禄 韩建俊 等译

ELSEVIER
ACADEMIC
PRESS

電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
http://www.phei.com.cn

Digital Evidence And Computer Crime Second Edition

数字证据与计算机犯罪

(第二版)

[美] Eoghan Casey 著

陈圣琳 汤代禄 韩建俊 等译

電子工業出版社

Publishing House of Electronics Industry

北京 · BEIJING

内 容 简 介

本书所探讨的数字证据和计算机犯罪涉及到四个领域：法律、计算机科学、法学和行为证据分析。具体讲述了数字证据和计算机犯罪的基本概念、历史背景和相关术语、欧美相关法律的对比、调查推理、惯用手法和犯罪动机、计算机入侵调查、网络骚扰调查、因特网上的性犯罪和数字证据托辞等内容。

本书适合于计算机安全专业和涉及到计算机相关犯罪的法律专业人员和执法人员阅读。

版权贸易合同登记号　图字：01-2004-0337

图书在版编目(CIP)数据

数字证据与计算机犯罪(第二版)/(美)凯西(Casey,E.)著；陈圣琳等译. —北京：电子工业出版社，2004.9
书名原文：Digital Evidence and Computer Crime Second Edition
ISBN 7-121-00159-4

Ⅰ.数…　Ⅱ.①凯…②陈…　Ⅲ.①数字—证据—研究②计算机犯罪—研究　Ⅳ.①D915.13②D914

中国版本图书馆 CIP 数据核字(2004)第 074346 号

责任编辑：徐云鹏
特约编辑：卢国俊
印　　刷：北京天竺颖华印刷厂
出版发行：电子工业出版社
　　北京市海淀区万寿路 173 信箱　邮编：100036
　　北京市海淀区翠微东里甲 2 号　邮编：100036
经　　销：各地新华书店
开　　本：787×1092　1/16　印张：30.875　字数：790 千字
印　　次：2004 年 9 月第 1 次印刷
定　　价：48.00 元

凡购买电子工业出版社的图书，如有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系。联系电话：(010) 68279077。质量投诉请发邮件至 zlts@phei.com.cn，盗版侵权举报请发邮件至 dbqq@phei.com.cn。

作者简介

Eoghan Casey 是 Knowledge Solution LLC 的创立成员，也是一名开业法学自由职业者的合伙人，致力于提供高质量的培训、信息资源和案例咨询。他从事对网络入侵、知识产权盗窃以及其他计算机犯罪的调查，在数字证据分析方面具有丰富的经验。他曾经协助执法机构调查各种犯罪案件，包括凶杀案、虐待儿童案、网络骚扰、盗窃案等。Eoghan 还拥有广泛的信息安全经验。在耶鲁大学时，作为一名信息系统安全高级职员，在后来的咨询工作中，曾经实施过缺陷评估，部署并维护入侵检测系统、防火墙和公钥体系结构，制定安全策略、规程和教育课程。Eoghan 拥有加利福尼亚大学伯克利分校机械工程专业的学士学位，以及纽约大学的教育传播与科技专业的硕士学位，目前正在攻读都柏林大学计算机科学专业的博士学位。Eoghan 还曾汇集过多位法学专家编著了一本名为“Handbook of Computer Crime Investigation: Forensic Tools and Technology”的图书。他的联系方式是 eco@corpus-delicti. com。

Robert Dunne 是一名律师，也是耶鲁大学计算机科学系的教员，讲授“计算机和法律”、“计算技术的法律含义”、“数字时代的知识产权”等课程。他曾撰写过有关电脑空间行为控制选择范例、电脑空间对法律专业的影响以及因特网犯罪等方面的图书。Robert 是耶鲁因特网研究中心(Yale's Center for Internet Studies)的教学主任，耶鲁因特网研究中心是一个跨学科的企业，其目标是从技术、法律、政治、经济、文化、教育等视点来探索因特网对社会的影响，以及社会对因特网的影响。

Monique Mattei Ferraro 是康涅狄格州公共安全部(Connecticut Department of Public Safety)计算机犯罪和电子证据处(Computer Crimes and Electronic Evidence Unit)的律师，也是一名信息系统安全认证专家。她从 1987 年就在康涅狄格州公共安全部工作。她建议计算机犯罪处和针对儿童因特网犯罪的特派小组开发执法和起诉方面的培训课程，以及有关计算机犯罪调查和因特网安全方面的公共课程。Monique 还是《康涅狄格州关于计算机和电子证据搜索和查封的执法准则》的合作著者，现在还正在与 Eoghan 合著一本关于调查因特网儿童剥削的书。她取得了美国东北大学(Northeastern University)的学士学位，以及康涅狄格大学法律学院的学位。

Troy Larson 是 Digital Evidence Solution 公司的总裁，该公司位于华盛顿州的西雅图市。Larson 先生专门为律师提供全方位的有关诉讼、特别探查、专家证词等方面的数字证据服务。他还是华盛顿州律师界的会员。在加利福尼亚大学伯克利分校完成了大学学业，并取得了律师专业的学位。他的联系方式是 ntevidence@comcast. net。

Michael McGrath 博士从事临床、系统管理、教学和研究等方面的工作。他的专长包括法医精神病学和犯罪剖析。他曾出版过有关犯罪剖析、性侵犯和因特网、性侵犯的伪指控、性窒息等方面的文章和图书。

Gray Palmer 是 Security and Information Operations 集团在马萨诸塞州 Bedford 的 MITRE 公司的一位 INFOSEC 研究员。目前正支持美国空军研究实验室(Air Force Research Laboratory，简称 AFRL)驻罗马研究站(Rome Research Site)和驻纽约研究站的数字法学研究项目，着重研究法学身份验证、数据库系统的恢复和分析以及无线技术的法学问题等。

Gray 还是 AFRL 发起的数字法学研究工作组(Digital Forensic Research Workshop,简称 DFRW)的合作创始人和高层组织者,DFRW 为高校科研和实践领域之间的对话提供了一个论坛。他于 1979 年获得了弗吉尼亚理工学院(VATech)的学士学位。自从 1981 年以来,他一直活跃于计算机、网络和信息安全领域,在连接到 DEC PDP/11－44(运行 RSX11/M)的纸带上编写了他的第一个宏汇编程序。他住在佛罗里达 Sanford,骑着自己的摩托车,弹着吉他,目前参与了中佛罗里达大学计算机法学研究生认证课程。

Tessa Robinson B. L. 在都柏林三一学院(Trinity College)和爱尔兰 Kings Inns 做过研究。她是一位开业律师,在 1998 年进入爱尔兰律师业。她的业务领域包括犯罪、商业、管理和家庭法律。在进入爱尔兰律师界之前,她还曾在纽约人权律师委员会、布鲁塞尔伟凯律师事务所(White & Case)、旧金山美富律师事务所(Morrison Foerster)、华盛顿特区霍金·豪森律师事务所(Hogan & Hartson)工作过。

Brent Turvey 在康涅狄格州西汉文(West Haven)的纽黑文(New Haven)大学取得了法学硕士学位。他还拥有波特兰州立大学的心理学学士学位,主攻法学心理学,以及历史专业的学士学位。他从 1990 年就开始研究性暴力犯罪,曾在中国、美国、新西兰、加拿大、澳大利亚、韩国等国家作为一名法学家和犯罪心理分析家为执法部门、律师和私营机构提供有关强奸、杀人、分段犯罪现场和多宗死亡案的咨询服务。他的一部著作"Criminal Profiling: An Introduction to Behavioral Evidence Analysis, 2nd Ed"(犯罪剖析:行为证据分析介绍,第二版)被全世界各国的大学和学院广为使用。他目前是 Knowledge Solutions LLC 的全职合作伙伴、犯罪分析家和讲师。

致　谢

本书的内容和结构是经过多年透彻的案例分析、研究和教学而形成的。在这个过程中，很多同事、同学、家人和朋友帮助了我。对你们的支持和帮助，我表示由衷的谢意，其中我想特别感谢以下几位：

Robert Dunne、Monique Mattei Ferraro、Troy Larson、Mike McGrath、Gary Palmer、Tessa Robinson 和 Brent Turvey，因为你们的灵感和奉献，因为你们对这项艰巨计划的认同；Barbara Troyer，因为你对本书插图的帮助，也因为我们多年的友谊。

Colin Harris 和 Stephen Douglas，因为在艰难的修正过程中，你们带来了沉着和方向；Clare O'Conner，因为你给予了毕生的鼓舞和指引；Jim Casey，因为你明智的建议；Ita O'Connor，因为你清楚的思路，并使这一切成为可能；Genevieve Gessert，因为你无尽的爱、友谊和支持。

H. Morrow Long、Andrew Newman、Shawn Bayern 和耶鲁大学的所有朋友们，因为你们给予了全力的支持，以及提供的富于挑战性的工作学习环境。

Bruce Patterson、Andy Russell、Jim Smith、Joe Sudol、Ken Gray、John Blawie、Mike O'Connor、Mark Califano 和康涅狄格州犯罪实验室（Connecticut State Crime Laboratory）的所有朋友们，以及州和国家律师所的所有朋友们，因为你们的奉献和友情。

Fred Cotton、Todd Colvin、Jim Jolley、Keith Daniels、Glenn Lewis 和 SEARCH 的所有朋友们，因为你们不断地给予支持。

Tony Noble、Javier Torner、Larry Amos、Don Allison、Harlan Carvey、Paul Gillen、Harold Jones、Gray Gordon、Sarah Mocas、Warren Harrison、Mark Morrisey、Mark Bowser、Warren Kruse 和 Garrie Whitcomb，因为你们个人的鼓励和贡献。

Brian Carrier，感谢你对第 10 到第 12 章的技术检查；E. Larry Lidz，感谢你对第 16 到第 18 章的技术检查。

Brian Carrier、Joe Grand、Dan Mares、John Patzakis、Amber Schroader、Eric Thompson、Bob Weitershausen 和 Walker Whitehouse，感谢你们在数字证据检验工具上的帮助。

Mark Listewnik、Linda Beattie、Jennifer Rhuda 和 Academic 出版社的其他朋友，感谢你们多年来对这个计划的关注和开发。

译 者 序

非常荣幸能有机会为广大读者介绍国际上计算机安全前沿和最新交叉领域的现状和发展趋势。当计算机和网络已经成为我们生活中不可或缺的一员时，它们也深深地进入到我们生活中的各个方面，有正面的当然也有反面的影响。计算机相关犯罪在全球一直呈增长趋势，手段和类型也日趋多样化，很多国家都为此修正了相关法律条款来保护人们的合法电子权益。由于数字世界的特殊性，执法人员在行使法律特权的时候也遇到了前所未有的新问题，特别是数字证据方面。作为立案、审判、宣判的最基础依据，数字证据的重要意义是不言而喻的。

本书的著者 Eoghan Casey 等都是计算机安全、法律和法学、犯罪学等相关领域的专家，具有丰富的实践经验和坚实的理论素养，特别是本书的第一版曾在业界激起很大的反响，同时也推动了该领域的不断发展。本书是经过重新修正的第二版，增加了很多新的内容和实践指南，特别一些实际案例的介绍和推理，能给读者以极大的思维和想像空间，而不再仅仅是一些枯燥的理论描述。

数字法学是计算机科学和法学的交叉学科。对于两者的关系，可以这么认为，法学是目的，而计算机科学是手段，通过计算机技术和相关工具查找、收集、处理计算机和网络中存在的数字信息，形成潜在的数字证据，再利用法学知识进行分析和推理，最终得到的调查报告将提交给法院作为立案和审判的依据。

在本书的编译过程中得到了北京美迪亚电子信息有限公司和山东大众信息产业有限公司的大力支持和协助，在此表示衷心的感谢。本书所列举的法律相关内容都源自欧美国家，在此只作为参考，而不作为法律建议。另外，参与本书翻译和校对的同志还有袁然、吴东霞、法永洁、刘波、李丽、刘岩、侯凤成、向小平、理志强、李雪修、范荣鹏。由于时间仓促水平有限，如有不当之处，敬请批评指正。

前　言

自从本书的第一版问世以来，业界对数字证据的兴趣一下子爆发出来。这种爆发主要表现在对工具、术语、定义、标准、伦理和其他基础方面的激烈争论。因此这本书能反映出我在这些争论中所处的位置就不足为奇了。最引人注意的地方就是，本书反映了我的一个坚定信念：该领域在它的发展道路上一定会越来越科学。本书的主要目的就是帮助读者通过客观地和全面地分析数字证据来解决在寻求科学事实过程中遇到的各种难题。我们也衷心希望本书能够鼓励读者在法学执业领域不断得到提高。

专业领域

目前，该领域在有关“专业范围”以及“谁应该得到什么样的培训”等方面非常不明确。例如，在数字犯罪现场技术员（也称为“第一响应员（First Responder）”）和数字证据检验员之间就没有明确地进行区分，实际上，恢复数据要比基本的证据收集、保存、文档化需要更多的专业知识。本书第 4 章中详细讨论的调查过程就建议根据专业知识和培训的不同级别将相关人员分为三种类型：

- 数字犯罪现场技术员（Digital Crime Scene Technicians）：负责在犯罪现场收集数据的人员，除了具备证据处理和文档化的基本技能外，还应当了解基本的犯罪推理，以便帮助他们能够定位网络中的有效证据源
- 数字证据检验员（Digital Evidence Examiners）：负责处理特定类型数字证据的人员，需要进行专业培训并取得相应领域的认证证书
- 数字调查员（Digital Investigators）：负责整个调查过程的人员，需要接受综合培训，但不要求非常专业化，也不要求专业认证。调查员还负责利用第一响应员和法学检验员所提供的信息来推理与犯罪相关的行为，从而能为其他调查员和律师勾画出一幅完整的犯罪图像

提示：基于本书的用途，比较通用的术语“数字调查员”在本书中是指在数字调查中起到关键作用的人员，可能包括计算机安全专业人员、律师、执法警官或者法学检验员。

该领域的培训和认证课程应当考虑到这三种需要不同专业技能的角色。

数字证据的可靠性

目前，数字调查员还没有一个系统的方法来描述数字证据的确定性，而这些数字证据就是最后结论的基础。这种正式化描述的缺乏就导致了法庭和其他决策者难于确定数字证据的可靠性和数字证据调查员所得出结论的说服力。本书第 7 章中提出的确定性级别（Certainty Scale）就提供了一种表示不同类型数字证据的确定性的统一方法。确定性级别的直接目的就是提高我们判断数字证据可靠性的能力。

最终，我们希望这种确定性级别能应用于那些在数字证据研究中需要格外注意的领域。对一些特定案例中 C 值（Certainty-Value）的辩论可能会揭示出特定类型证据的可靠性比最初

设想的要低。对于某些类型的数字证据而言，也许能识别出其中错误和不确定性的主要根源在哪里，然后再制定出一套用于评估和减少这些负面影响的分析技术。对于另一些数字证据而言，也许能识别出其中错误和不确定性的所有根源，然后再制定出一套更正规化的模型，来计算此类证据的确定性级别。

标准化需求

数字证据是另一种"潜在"的证据形式，必须在科学的原理和法律的界限内进行处理。其中有电子犯罪的调查性构成，也有与该类犯罪相关的数字证据实验性构成(Carrie Whitcomb，2001 年，"A Forensic Science Perspective on Digital Evidence Training，Education，and Certification(关于数字证据培训、教育和认证的法学展望)"，National Center of Forensic Science(国家法学中心))。

1994 年，O. J. Simpson 案暴露了刑事调查和法学中的很多弱点。调查从一开始就因为在犯罪现场不完整的证据收集、文档化和保存而受到阻碍。因为这些初始失误，一些有经验的法学家就被那些被错误解释的重要证据所迷惑，进而也给陪审员带来了各种疑问。围绕该案件的争论使我们看清了一件事情：调查员和法学家不像以前那么可以信赖了，这不仅损害了他们的信誉，也毁掉了他们的职业。这种危机促使很多犯罪实验室和调查机构修正他们的规程、改进培训内容，并采取其他一些措施来避免以后发生相似的问题。最近，某些犯罪实验室所采用的指纹和 DNA 分析出现了更多的缺陷，致使很多判罚出现了问题，从而对分析技术本身产生了质疑。

在数字证据领域也是危机四伏。实践和培训标准的普遍缺乏导致本行业持续性上的弱点，不仅证据收集、文档化和保存不完善，而且数字证据分析和解释也存在错误。不适当的数字证据处理和解释会产生很多冤假错案，使无辜者蒙冤，而使犯罪分子逍遥法外。如果收集数字证据失败，那么就会毁掉整个调查工作，无法对犯罪分子进行逮捕和控诉，浪费了案件的有价值资源。如果这种形势得不到改观，该领域就不会进一步得到发展，如果失去了公正，那么该领域还有颜面立足于世吗？我们之所以还没有遇到这样的危机，是因为我们的错误被某种朦胧性所掩盖了。当更多的案件要依赖于数字证据的时候，也就应该更多地关注它，我们必须采取行动，建立相应的实践标准，使该领域的从业人员必须遵守这些规则。

该领域在标准化进程上有几个令人瞩目的发展。20 世纪 90 年代创立的"国际计算机证据组织(International Organization of Computer Evidence，www. ioce. org)"，就是要保证国家之间在计算机证据处理方法和实践上的一致，保证从一个国家收集来的数字证据能在另一个国家使用。1998 年，又成立了"数字证据科学工作组(Scientific Working Group on Digital Evidence，www. swgde. org)"，将各大学、军事机构和私营部门的相关专家召集在一起，讨论该领域所面临的挑战和研究需求。该工作组又赋予了在几年之前提出的一个观念以新的生命，就是"同行评审期刊(peer-reviewed journal)"，进而导致了"国际数字证据期刊(International Journal of Digital Evidence，www. ijde. org)"的创立。2003 年，"美国犯罪实验室主任协会/实验鉴定委员会(American Society of Crime Laboratory Directors/ Laboratory Accreditation Board，简称 ASCLD/LAB)"更新了他们的鉴定手册，包含了美国犯罪实验室中为数字证据检验员制定的标准和准则。2004 年，"英国法学服务(UK Forensic Science Service)"计划建立一个资格专家注册库，有些欧洲组织，包括"欧洲法学研究所(European Network of Forensic Science Institutes，简称 ENFSI)"，将为数字调查员出版撰写指南性的检验和报告。同样，

Elsevire 也开始出版“Digital Investigation: The International Journal of Digital Forensics and Incident Response”(http://www.compseconline.com/digitalinvestigation/)。

从历史上看,法学专业已经通过认证的方式来指导该领域实践和培训的标准。认证不仅提供了个人在职业上取得资格所需要达到的标准,而且还提供了一种激励措施使人们对专业知识的掌握能够到达某种特定程度。如果没有认证,所做工作的目标和报酬就不清楚。但这并不是说要求每个处理数字证据的人都要达到相同的技能和培训级别。一个强大的认证体系需要一种层次化的认证结构,有助于在认证过程中不断进步,比如犯罪现场技术员的基本认证需求、实验室专家和从事证据分析的调查员的高标准认证需求等。

虽然目前出现了很多关于数字调查员的认证课程,但是其中有不少只针对执法人员,而且不被国际所认可。2004 年,来自全世界的代表聚集在一起讨论数字调查员国际认证的可行性,但最终没有达成共识,因为要达到国际认证仍然存在一些障碍。有些人感到被提交的培训需求过高;而有些人则担心认证会使任何人都介入该领域获取专业知识,甚至那些从事刑事案件辩护工作的人;还有人担心对执业人员所设定的标准和所增加的额外需求会使取得法庭认可的数字证据更加困难。

自相矛盾的是,有些关心培训需求的人还想把“那些想把从事刑事案件辩护工作的人排斥在外的人”排斥在外。任何想限制刑事辩护律师的知识范围,以及想允许错误观念和拙劣实践继续存在以便抑止该领域的发展和进步的行为和观点都是缺乏道德的。如果我们不能开诚布公地发展该领域,那么最高兴的人就是那些犯罪分子。该领域的任何人都应该向最合理的标准和品质努力。长期来看,由经过认证的专业人员处理的数字证据被怀疑和引起不公正的可能性要小一些。

对 Starnet 网络赌博公司的调查就是一个良好培训和准备工作的成功案例。在 1999 年 8 月对在温哥华的 Starnet 办公室的突袭是经过了“加拿大皇家骑警(Royal Canadian Mounted Police)”一年多来有价值的调查和准备工作才取得成功的。来自加拿大各地的探员集中到一起搜查和查封 Starnet 系统。搜查小组经过了相关培训以便实施标准操作规程来保证整个过程的连贯性,另外还配备了充足的设备从而能将所需要的大量数据复制下来。因为经过了周密的计划,所以 Starnet 的办公大楼和所包含的网络被成功地冻结了几分钟的时间,但是从 80 多台计算机上保存数字证据则花费了几天的时间。2001 年,Starnet 承认自己违反了加拿大刑法的 Section 202 (1) b 条款,因为自己在加拿大拥有用于赌博的计算机。

虽然某些人不想在这方面职业化,但是对所有人来说这是一个必然趋势。如果没有通用的可接受标准,那么审判工作就没有基础。如果没有认证,就没有达到专业资格的基础。该领域有责任取得实践和培训标准的共识,也有责任使执业人员通过认证满足所需标准。

这种责任之所以存在是因为在法学中我们的观念和解释会对人们的自由甚至是生死造成重大影响(Turvey, B., 2000 年,“Criminal Profiling”中的“The Professionalization of Criminal Profiling”, Academic Press)。

本书导读

本书涉及到四个领域:法律(Law)、计算机科学(Computer Science)、法学(Forensic Science)和行为证据分析(Behavioral Evidence Analysis)。法律提供了本书中所有概念应当符合的总体框架。计算机科学提供了理解数字证据各方面内容的技术细节。法学提供分析任何形式数字证据的通用方法。行为证据分析提供了一个综合特定技术知识和常用科学方法的系统

化方法，以便对犯罪行为和动机进行深入理解。

本书分为五部分。第一部分(第 1 章到第 7 章)描述了相关法律问题和调查方法：第 1 章是概述；第 2 章提供了相关背景、历史和术语；第 3 章讨论了计算机相关调查中涉及到的法律问题，并对比了美国和欧洲的法律；第 4 章讨论了基于科学方法进行犯罪调查的系统方法，并提供了本书后面章节的整体结构；第 5 章描述了如何利用数字证据推理事件和剖析犯罪分子和受害者；第 6 章讨论了技术和利用技术实施犯罪的人之间的关系，理解犯罪动机和行为是评估风险(犯罪活动是否会逐步升级)、确定和寻找嫌疑犯(寻找和要会谈的人)、集中调查(在哪寻找和寻找什么)的关键；第 7 章提供了一个在法庭上会发生的与数字证据相关问题的纵览。

本书的第二部分(第 8 章到第 13 章)从介绍单台计算机环境下的基本法学概念开始，说明了即使涉及到网络，处理单台计算机也是非常关键的，收集存储在计算机上数字证据通常是必需的步骤。本书中提供的案例和指南也有助于知识的合理应用。第二部分后面几章详细介绍了几种特定类型的计算机，最后讨论了如何解决这些系统的口令保护和加密问题。

第三部分(第 14 章到第 18 章)主要介绍了计算机网络，特别关注了因特网。本书采用了一种自下而上的方法描述了计算机网络，开始是在网络中传输的原始数据，然后再建立可以在网络系统和因特网中发现的数据类型。计算机网络的“顶层”由用户使用的软件构成，比如电子邮件和 Web 等，这些顶层结构隐藏了计算机网络底层的复杂性，因此必须要检验和理解计算机网络的底层复杂性才能完整地理解在网络顶层找到的信息。另外，也必须理解在计算机之间传输数据的网络“底层”——物理介质(比如铜线或者光纤)，才能更好地收集和分析原始网络流量。

本书的第四部分(第 19 章到第 22 章)集中讨论了特定类型的调查：从第 19 章的计算机入侵调查开始，描述了一些该类调查所用到的特殊工具和技术，并用详细的案例演示了其中的关键点；第 20 章是网络骚扰调查；第 21 章详细介绍了因特网上的性侵犯；第 22 章讨论了将计算机作为不在犯罪现场的托辞。

第五部分比较简短，提供了处理数字证据的指南。这一部分没有涉及图像、视频和音频的法学分析。有关图像、视频和音频的详细信息以及此类信息的分析，可以参考 Gruber 的“Electronic Evidence”(Gruber，1995 年)。

对于前面描述的有关单台计算机的法学概念，又针对因特网的每一层进行了具体分析。从各种环境下来看法学概念的应用有助于读者将系统方法推广到数字证据处理和分析过程中去。一旦得到推广之后，这种系统方法就可以应用到本书中没有特别讨论过的环境中。本书没有采用第一版中使用的 CD-ROM 方式，而是提供了一个交互式网站(www. disclosedigital. com)，其中有基于真实案例的实践练习，演示了计算机相关调查的关键因素，帮助读者将从本书学到的知识应用到自己的调查实践中去。该网站概括了一个通用的教育模型，其他人可以复制或者从中借鉴，以便创建一个成本更低、更具教育意义的资源来辅助调查员的工作。

声明

本书中所提到的用于演示各种概念和技术的工具，并不是说这些特定工具在某种特定环境下是最合适的。数字证据调查员必须自己负责选择和评估自己的工具。

本书中所讨论的任何法律问题只是为了便于读者理解本书的内容，而不作为法律建议。在具体实践过程中，应该寻求有法定资格的法律建议，才能解决案件的特定问题，以确保能真正领悟到法律的微妙。

目　录

第一部分　数字调查

第二部分 计 算 机

第五部分　指　南

第一部分　数字调查