网络空间安全系列教材

Pearson

计算机取证与网络犯罪导论

（第三版）

Computer Forensics and Cyber Crime
An Introduction, Third Edition

[美] Marjie T. Britz 著
戴 鹏 周 雯 邓勇进 译

中国工信出版集团
電子工業出版社
http://www.phei.com.cn

计算机取证与网络犯罪导论

（第三版）

Computer Forensics and Cyber Crime

An Introduction

Third Edition

［美］ Marjie T. Britz 著

戴 鹏 周 雯 邓勇进 译

電子工業出版社

Publishing House of Electronics Industry

北京 · BEIJING

内 容 简 介

本书是计算机取证与网络犯罪方面的经典教材。全书首先概述理论，讨论计算机相关术语和传统计算机犯罪。然后讨论当前的计算机犯罪，身份窃取与身份欺诈，恐怖主义及有组织犯罪，起诉途径及政府行为。接着探讨所涉及的法律问题，计算机取证的术语与需求，如何搜索并获取证据，以及证据的处理及报告准备。

本书适合从事计算机取证和网络安全相关工作的技术人员参考，也适合作为相关院校本科计算机取证技术及网络犯罪预防等课程的教材。

版权贸易合同登记号　图字：01-2013-6967

图书在版编目(CIP)数据

计算机取证与网络犯罪导论：第 3 版 /（美）布里提（Britz, M.T.）著；戴鹏，周雯，邓勇进译.
北京：电子工业出版社，2016.9
书名原文：Computer Forensics and Cyber Crime: An Introduction, Third Edition
ISBN 978-7-121-27578-4

I. ①计… II. ①布… ②戴… ③周… ④邓… III. ①计算机犯罪－证据－调查 ②互联网络－计算机犯罪－研究 IV. ①D918②D914.04

中国版本图书馆 CIP 数据核字(2015)第 271336 号

策划编辑：马　岚
责任编辑：李秦华
印　　刷：北京京海印刷厂
装　　订：北京京海印刷厂
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
开　　本：787×1092　1/16　　印张：24.75　　字数：587 千字
版　　次：2016 年 9 月第 1 版(原著第 3 版)
印　　次：2016 年 9 月第 1 次印刷
定　　价：78.00 元

凡所购买电子工业出版社图书有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系，联系及邮购电话：(010)88254888，88258888。

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。

本书咨询联系方式：classic-series-info@phei.com.cn。

序

“向邻居看齐。”许多年轻读者可能从来没有听过这个说法。它通常指与邻居保持相同的社会和物质水平。但在这里，可能意味着计算机取证分析师和专家们不断试图跟上计算机和我们所有的电子产品技术的发展。在早先的出版物中，Britz 博士提出了计算机犯罪和计算机取证调查技术的基础教育，她再次将其涵盖到本书中。虽然，其中的一些技巧和准则现在看起来有些过时，但是，缺乏计算机及计算机相关的“智能”设备(手机、GPS，演变成“电脑”的智能手机等)如何工作的基本知识，研究者将会被拒之门外。Britz 博士的计算机取证技术和历史章节向新用户介绍所有相关信息，并向所有不同水平用户阐明标准化技术。这样的说明只是众多原因之一，本书中设置了标准。

文中包含有关网络和计算机调查适用法律的全面讨论。当我们“在云中”时，必须考虑法律和司法辖区，但是网络犯罪并不关心其中的任何一个。调查人员必须具备资料，以便进行适当的调查，本科生必须吸收基础知识，这样的学术研究可能会持续下去。本书以清晰、简洁的方式提供这样的信息，适当介绍了(美国)州和联邦立法、第一和第四修正案以及国际努力情况。

除了法律，本书给我们带来最新的信息技术和实践，这是调查人员必须了解和掌握的，以便开展高科技调查和分析。如果计算机专家不紧跟技术发展，他们将在数月之内、而不是几年后被甩下。试想这么短的时间内，所有的智能设备变得如此丰富。本书帮助分析师和调查人员达到与技术发展曲线保持同步的速度。此外，它提供了一个可供领域内新人理解的框架。

本书进一步探索了电子卡、电子现金、因特网或其他在线交易和购买行为，很少人没有经历过其中一个或另一个事物。随着身份诈骗和其他方式使用计算机、智能手机和其他电子设备非法获得资金的扩散，对资金窃取的调查一直在不断变化。本文中有关身份盗窃章节显示了这个领域中新兴的趋势，并提供加强个人安全和机构决策的建议。

最后，本书包括一个对调查人员和研究人员都至关重要的其他领域的全面讨论。这些讨论包括，网络，因特网，黑客，知识产权盗用，其他类型的计算机相关欺诈，最重要的是与科技社会相关的恐怖主义、有组织犯罪和性犯罪，以及如何进行涉及这些问题的计算机调查。

总之，Britz 博士再次概括了那些具有重大历史意义的计算机、法律和技术话题，这是当今计算机取证分析师、调查人员和专家必备的知识。与其他文章要么是太“技术化”，要么完全缺乏深度相比，本书是一本全面且具有可读性的书籍。简而言之，本书涵盖计算机研究人员和本科学生感兴趣的话题。总之，它对每个人都有用。

Dan Mare

目　录

第 1 章　计算机取证和网络犯罪的概述和简介

学习目标

学习完本章后，将能达到以下目标：

- 探究与科技进步和网络应用相关的社会变化
- 认识对计算机犯罪的起诉和执法带来的挑战
- 探索社会上计算机犯罪的范围
- 熟悉与计算机相关的犯罪分类

关键词和概念

- 计算机犯罪
- 计算机取证科学(计算机取证、数字取证)
- 计算机相关的犯罪
- 计算机犯罪
- 网络犯罪
- 数字贵金属
- 电子前沿基金会[Electronic Frontier Foundation(EFF)]
- 电子钱包
- 信息或数字革命
- 因特网
- 因特网支付服务
- 有限的或封闭系统卡
- 移动支付
- 多用途或开放系统卡
- 盗用电话线路
- 物理属性
- 预付卡
- 储值卡

1.1　简介

历史上，世界经历了几次启蒙运动和进步，例如，约两个世纪前的工业革命带来了空前的知识和机会，这次革命(一般工业自动化)提供了前所未闻的便利和进步。交通的发展增加了度假目的地的清单、使得相距遥远的亲人间能保持联系；偏远地区也因为可以方便获得产前照顾，得以降低婴儿死亡率。另外，通信上的巨大进步提高了警察效率、改变了情侣间示爱行为等。个人、家庭和机构更容易获得奢侈品(如空调系统)。通过高效的工具、庭院设备等，家务也变得容易了。通过增加可靠、可信的知识来源，印刷自动化、大量媒体的介入等也极大地增强了信息的分发和传播。遗憾的是，也提高了身体懒散、肥胖、自满、迟钝、子女缺少和犯罪行为的增加。作为信息革命的直接结果，今天的美国社会也正经历着类似的转变。

因特网的引入为商业、科研、教育、娱乐和公共讨论等创造了空前的机会。一个全球性市场开始出现，其中，新想法和对多元文化欣赏的增长日益兴旺。数字化的百科全书、国际公会、世界连通性和通信的引入极大地增强了个人的生活品质。实际上，因

特网作为世界的一个窗口，能满足个人的好奇心，并培养其全球意识。它允许个人体验以前只能在梦中出现的事物，有意者可以参观罗浮宫、在其闲暇时欣赏无价的史前古董或是进行一场非洲狩猎且没有炎热和蚊虫叮咬。他们可以找到最复杂法律或医疗问题的答案，或是搜寻与其性情相投的伴侣；可以下载喜爱餐馆的优惠券，或是搜索到喜爱的食物配方。另外，个人、公司、公众组织和机构能使用图像化的、高亮强调的信息并提供详细的信息或支持的链接，更有效地宣传他们的产品或服务。实际上，计算机化的海量信息访问跨越了传统通信的边界。

与其他机构一样，执法机构也从中受益。因特网成功地为社会成员间交换信息创建了一种不受威胁的平台。另外，速度和效率使得全球的机构之间可以相互通信、巩固关系和加强协作。确实，执法机构通过简单地扩大交流对象就能更好地促进任务的完成。对嫌疑犯或失踪人员的文字描述和图片可以被任何连接到因特网的人看到，有关市民可以用一种有效和高效的方式报告嫌疑犯的行踪。然而，对因特网、数字技术和通信的更多依赖，也有不利的一面——带来了看起来执法部门难以克服的障碍。确实，从马达加斯加岛获得所喜爱食物配方的技术，同样也可用于下载大规模杀伤性武器的蓝图；在网上冲浪的个人在享受此类搜索成果的同时，同样也能跟踪和骚扰特定目标的受害者。事实上，使得因特网、无线技术和智能手机如此吸引人的优势也正是带来巨大危险的因素。

因特网的不利方面还包括对网络信息的依赖不断增加。许多在读大学生只依赖来源于电子化的知识。遗憾的是，在网络空间中所找到的信息质量堪忧，对人工智能的依赖导致对人的取代。更重要的是，新技术在加强传统不良行为模式的同时，往往会培育出一些新的社会不良行为模式。就像印刷出版业的自动化和众多媒体的引入导致违禁品的分发和需求也成指数地增长，如色情和违法物品。因特网上产生了虚拟的儿童侵犯和色情的温床，并建立了武器和毒品等的地下交易市场。事实上，犯罪行为的流行、视频交换或情报的非法交易也达到前所未有的高度。不断增强的无线技术、社会网络和智能电话使得调查领域更加复杂，全球的执法机构都在努力建立和加强新兴技术条件下的法律和制度。

1.2 网络空间和犯罪行为

网络空间可以定义为一个虚拟的空间，在其中，个人可以交易和沟通。它是空间之间的空间[4]。尽管最初是在 1984 年由科幻小说作者 William Gibson 提出，但很难说这是一个新概念。实际上，普通的传统电子通信就属于这个空间，通过有线交换进行穿越时空的电话会谈。然而，熟知的因特网这种新媒体极大地增强了虚拟世界的真实感，相应地带来用户数量呈指数增长。例如，在 2009 年，大约有 78%的美国人使用这个媒体，而 1995 年还只有 10%。在英国，该媒体的用户增长更为明显，由 1995 年的 1.9%增加到 2009 年的 83.2%[5]。没有其他的媒体能如此有效地融合语音、视频和数据。与传统方法不同，因特网包括了邮件、电话和大众传媒。如先前所述，它展现给个人的是无数的新想法并可作为社会聚集区、图书馆或是独处的地方。个人用户可以在里面结婚、生活、

养育孩子。遗憾的是，这个虚拟世界也经常被当成逃避现实社会问题的避难所，在此，个人可以摆脱烦恼并自得其乐。

典型案例

第二生命：虚拟世界的实现

如前所述，在网络空间中存在很多虚拟社团，大多数表现出虚拟世界所具有的优柔寡断、寿命不长的特性。然而，在 21 世纪初由 Linden 实验室开发出来的第二生命(SL)，证明因特网虚拟世界可以吸引很多用户。一般所说的 SL——第二生命可以表示为一个社会网络地址，用户或居民由一个三维动画代理或化身代表，在里面可以参加各种与人类真实体验相同的虚拟活动。他们可以购买财物、购买衣服、接受手术、确定性关系、结婚、生子，甚至在 SIMetery 中拜访已故的爱人。他们通过轻点鼠标即可参加大学课程、赌场赌博或完成全球的远距传输。事实上，学术和商业团体也注意到并加入到这个虚拟世界中。然而，很多个人为这个虚拟存在投入了大量的时间和金钱，却没有回报[6]，以及规范和认识上的停滞不前都值得注意。

虚拟社区不仅跨越地理上的边界，还跨越了文化上的边界。关于种族、种族划分和国家民族血统的期望等被人工创造的自我(即化身)所取代，导致文化定义假设的悬而未决。换句话说，居民认可了肉体自我和虚拟代表之间的不一致，接受了能处理物理、社会和经济方面因素的虚拟物，而那些因素在现实中一度困扰着他们。于是，在虚拟世界中的异常行为也仅仅是局限在虚拟中，而非现实中，然而后果未必如此。

随着越来越多的用户混淆了他们的真实生活和第二生命的界线，关于虚拟化身行为的合法性问题就浮现出来。假设一个美国成年男子的虚拟化身与一个 12 岁泰国小孩的虚拟化身发生性关系，这如果算犯罪的话，算是什么样的犯罪行为呢？在一个网络聊天室里，一个恋童癖与儿童进行交谈，满足了有一个预先安排的会面地点这个条件，但这不够，法律界定仍需是有肉体侵犯或猥亵发生才能确认犯罪。在一个基于虚拟的世界中，关于犯罪意图或犯罪动机的法律要求能被满足吗？

隐私保护主义者经常忽视了这个全球媒体的消极影响，而狂热地讨论这个新兴技术在排除政府对个人监视方面的潜力。这种组织由诸如抒情诗人 John Barlow 和 John Gilmore 这样的知识渊博的人发起的“感恩而死”(The Grateful Dead)，John Barlow 和 John Gilmore 是 Cygnus Solution、Cyberpunks 和 DES Cracker 的合伙发起人/创建者。Barlow 和 Gilmore 强烈呼吁抵御美国的一些声名狼藉的计算机黑客并支持人权法案。他们认为警察最初目标为侵犯美国公民隐私的游手好闲者，而现在却将注意力集中在他们原来保护的个人身上。实际上，他们创建了 Electronic Frontier Foundation (EFF，电子前沿基金会)来提供“资金、指导和法律支持来证明美国特勤局限制出版物、限制自由言论、不恰当查封设备和数据、过度使用武力，且经常处于一种武断、强迫和违宪的状态[7]。”尽管美国特勤局早期的行为也证实了这种担心，但 EFF 的种种努力却忽视了全球范围内被快速发展的城市多元化重新构建的社会所带来的负面潜力。