信息安全与犯罪取证系列丛书

数字取证

SHUZI QUZHENG

蒋平 黄淑华 杨莉莉 编著

清华大学出版社
中国人民公安大学出版社

信息安全与犯罪取证系列丛书

数字取证

蒋　平　黄淑华　杨莉莉　编著

清华大学出版社
中国人民公安大学出版社
·北　京·

图书在版编目（CIP）数据

数字取证/蒋平，黄淑华，杨莉莉编著．—北京：清华大学出版社，中国人民公安大学出版社，2007.1

（信息安全与犯罪取证系列丛书）

ISBN 978-7-81109-558-6

Ⅰ.数… Ⅱ.①蒋…②黄…③杨… Ⅲ.数字技术—应用—刑事侦查—证据—收集 Ⅳ.D918.2-39

中国版本图书馆 CIP 数据核字（2006）第 145505 号

信息安全与犯罪取证系列丛书

数字取证

SHUZI QUZHENG

蒋 平 黄淑华 杨莉莉 编著

出版发行：清华大学出版社
中国人民公安大学出版社

地　　址：北京市西城区木樨地南里

邮政编码：100038

经　　销：新华书店

印　　刷：北京市泰锐印刷厂

版　　次：2007 年 1 月第 1 版

印　　次：2007 年 1 月第 1 次

印　　张：19.75

开　　本：787 毫米×1092 毫米　1/16

字　　数：342 千字

印　　数：0001～5000 册

ISBN 978-7-81109-558-6/D·528

定　　价：40.00 元

E-mail：cpep@public.bta.net.cn

www.phcppsu.com.cn　　www.jgclub.com.cn

信息安全与犯罪取证系列丛书

主　编　杨永川　蒋　平

副主编　顾　坚　刘　舒　赵明生

丛书序

互联网的迅猛发展使得人类各种活动对信息网络的依赖程度越来越大。人们在得益于网络技术带来便利的同时，也面对网络安全所带来的严峻考验。当前，计算机犯罪案件屡屡发生，信息安全问题日益突出，人们逐渐认识到对信息安全、信息对抗、计算机犯罪侦查、数字取证及电子证据等进行研究的必要性和紧迫性。鉴于此，作者精心组织编著了这套“信息安全与犯罪取证系列丛书”。

在《信息安全》一书中，作者从信息安全的现状和研究内容入手，对信息安全的关键技术作了详细的介绍，研究了信息安全的标准、策略、立法等内容，探讨了信息安全管理中存在的问题和解决办法，分析了信息安全产品的现状，并指出了今后信息安全产品的研发趋势。在《信息对抗》一书中，作者分析了信息对抗的两个方面，即网络攻击和网络防御，重点阐述了其理论和主要技术。在《计算机犯罪侦查》一书中，作者深入探讨了计算机犯罪案件的管辖以及计算机犯罪侦查的要求、措施、方法和技术，给出了一些典型对象的调查技巧，分析了数十例具有代表性的典型案例，为侦查人员科学、规范地侦办计算机犯罪案件提供了很好的参考和借鉴。在《数字取证》一书中，作者分析了各国数字取证研究的状况，阐述了数字取证的概念，介绍了当前流行的取证技术，对数字取证程序、数字取证相关法律等进行了深入的分析和研究，同时还对数字取证工具作了详细的介绍，并对数字取证工作规范进行了探讨。在《电子证据》一书中，作者借鉴了证据学的理论和方法，阐述了电子证据的概念、立法和来源，对电子证据的收集作了详细的探讨，并在总结电子证据特征的基础上，分析了电子证据的形式、保全、效力、认定和出示等问题，为电

子证据的学习者提供了参考。

该丛书内容丰富，不仅涵盖各自领域的理论和技术，而且涉及其他领域的多个学科。各书之间内容紧凑、衔接合理，构成了从信息安全到计算机犯罪侦查取证较为完整的研究体系。该丛书的研究具有一定的深度和广度，作者参考研究了大量国内外书籍及互联网上的最新资料。在技术介绍方面，作者力求紧跟国内外技术前沿，全面、系统地反映出各领域研究的最新动态，分析预测了各学科的前沿趋势和未来的发展方向。在立法和法规方面，作者对现有的法律状况进行了研究和思考，并提出了一些立法方面的建议。此外，该丛书引用了大量典型案例，通过对案例的深入剖析，使读者能更好地理解并掌握基础理论知识与技术的实际应用。

该丛书在理论和技术方面均有突破和创新，适合政法系统高等院校、其他高等院校和科研院所相关专业的研究生、高年级本科生，信息安全、法学等领域的研究人员、技术人员和管理人员以及政法系统相关执法人员在学习、研究和执法中参考和借鉴。

中国工程院院士 刘锦先

2006 年 8 月

丛书导论

计算机网络起源于20世纪60年代，在短短的几十年中几乎遍及全世界，目前已经渗透到社会的各个方面，并成为信息收集、分析、传输以及交换等各种处理过程中必不可少的途径。计算机网络进一步走向开放是大势所趋，只有采用开放式体系结构，才能提供良好的系统可移植性、兼容性、互操作性、可靠性和可扩展性。但开放的网络势必带来各种各样的复杂问题，信息安全日益突出，网络攻击事件层出不穷。2002年10月21日，美国9台互联网服务器遭到不寻常的网络攻击，黑客按照传统方法，通过控制某大学、公司甚至家庭用户的第三方计算机，向目标服务器发送大量数据流。经追踪调查后发现，攻击来源于美国及韩国。被攻击的9台服务器中有7台不能响应正常的网络流量，2台暂时中断。2003年8月11日，一种名为“冲击波”的新型“蠕虫”病毒开始在国内互联网和部分专用信息网络上传播，该病毒传播速度快、波及范围广，对计算机的正常使用和网络运行造成了严重影响。

在信息时代，以计算机网络为核心的信息系统已成为国家的信息基础和战略命脉，一旦这些重要的网络信息系统陷入瘫痪，整个国家安全就面临着危险。1988年11月2日，美国国防部战略C4I系统的计算机主控中心和各级指挥中心相继遭到计算机“蠕虫”病毒的攻击，共约8500台军用计算机感染病毒，美军的通信和指挥一时陷入混乱状态。更加令人始料不及的是，“蠕虫”病毒以闪电般的速度迅速自行复制，大量繁殖，不到10小时就从美国东海岸蔓延到西海岸，使众多的美国军用计算机网络深受其害，直接经济损失上亿美元。后来查明，这场第一次渗透到军事网络

的“恶作剧”，是当时年仅23岁的美国康奈尔大学计算机系研究生莫里斯制造的。这就是著名的“莫里斯”事件。1995年9月18日，一名年轻的美国空军上尉，利用一台普通计算机在众目睽睽之下拨号进入互联网，几分钟内便进入美国海军在大西洋舰队的指挥系统，轻而易举地控制了该舰队的指挥权，顷刻间成为这个舰队的“秘密司令”。1999年3月29日，南联盟及俄罗斯计算机高手成功地侵入美国白宫网站，使该网站当天无法工作。1999年4月4日，贝尔格莱德黑客使用“宏”病毒对北约进行攻击，使其通信一度陷入瘫痪。从军事角度审视这些事件，或许可以认为，对一个国家进行战略打击，点击鼠标比抠动扳机更有效。1999年4月，美国《新闻周刊》透露，克林顿批准了由美中情局实施的绝密计划：利用电脑黑客，通过入侵南联盟总统米洛舍维奇及其他领导人的外国银行账号来颠覆这个政府。2000年2月，美国著名的几大网站雅虎、亚马逊、CNN等相继遭到不明身份的黑客分布式拒绝服务攻击，导致网络瘫痪、服务中断，引起了各国政府和企业界的极大关注。仅就雅虎网站被袭击的情况来看，攻击者共调用了约3500台计算机同时向雅虎发送信息，发送量达每秒10亿兆位，远远超出了其信息处理能力，完全阻塞了网络系统，致使雅虎被迫中断服务达数小时。

从上述安全事件不难看出，网络攻击危害极大，并带来巨大的经济损失和不良的社会影响。随着信息技术的进一步发展、互联网普及程度的提高以及电子政务、电子商务的不断发展，传统领域的违法犯罪活动逐渐向计算机、互联网渗透，计算机犯罪案件将逐年上升。人们逐渐认识到在发展信息网络技术的同时，对信息安全、计算机犯罪及其取证方面的研究同等重要，网络技术与安全技术的研究应相辅相成、共同发展。在我国，对信息安全的研究起步相对较晚，信息安全技术还有待整体地提高和发展。面对日益严峻的信息安全问题，我们应该如何去认识、分析和防范，是当前所面临的一个迫切的问题。为此，作者组织编写了“信息安全与犯罪取证系列丛书”。这套丛书准备分期出版，第一

期出版《信息安全》、《信息对抗》、《计算机犯罪侦查》、《数字取证》、《电子证据》五部著作。

在《信息安全》一书中，作者从信息安全现状和信息安全的研究内容入手，对信息安全的关键技术作了深入介绍，研究了信息安全标准、信息安全策略、信息安全立法等方面的内容，探讨了信息安全管理中存在的问题和解决办法，最后分析了现有信息安全产品，指出了今后信息安全产品的研发趋势。

了解了信息安全面临的问题，就要采取防御措施预防或阻止网络攻击，网络攻击与网络防御构成了信息对抗的两个方面。《信息对抗》一书共分三部分。第一部分为基础理论部分，介绍了信息对抗的基础知识，包括信息对抗的基本概念、信息对抗的产生原因以及信息对抗的表现形式（即电子战）。第二部分为网络攻击部分，在介绍网络攻击理论的基础上，重点分析了黑客攻击技术和计算机病毒技术。第三部分为网络防御部分，首先介绍了网络防御理论，然后根据所提出的网络防御模型分章分别研究了网络防御中的网络防护、入侵检测、攻击源追踪、应急响应、入侵容忍和灾难恢复等方面的问题。

由网络攻击引发的安全问题直接导致了计算机犯罪案件的发生。要从根本上遏制计算机犯罪案件的发生及蔓延，不仅要具备基本的信息安全知识，而且需要善于利用法律武器打击计算机犯罪，惩罚和威慑计算机犯罪分子。计算机犯罪有别于一般刑事犯罪，这种犯罪行为往往具有隐蔽性、智能性和严重的社会危害性。因此，为了使计算机犯罪侦查具有科学性、规范性，在《计算机犯罪侦查》一书中，作者借鉴了一般刑事犯罪案件的侦查理论、原则和方法，根据计算机犯罪案件自身的特点，界定了计算机犯罪侦查的概念，明确了计算机犯罪案件的管辖，从计算机犯罪侦查现状及存在的问题、计算机犯罪侦查基本程序、计算机犯罪侦查的主要原则等方面阐述了计算机犯罪侦查的要求，研究总结了计算机犯罪侦查的措施及计算机犯罪的侦查方法。同时，给出了典型对象的调查技巧，并介绍了几种常用的计算机犯罪侦查技术

和相关工具。该书还精选了数十例具有代表性的典型案例，通过分析基本案情、侦查过程、处理情况，以及对案件侦查进行评论，使读者对计算机犯罪侦查有更深的理解。

计算机犯罪侦查与数字取证密切相关。数字取证不仅包括对计算机犯罪的取证，而且包括对其他刑事犯罪案件、民事案件、行政案件以及工作失误和设备故障等的取证。在《数字取证》一书中，作者首先介绍了国内外的数字取证研究状况，在此基础上对数字取证的概念进行了阐述，并对数字取证研究趋势进行了预测。在对数字取证技术的研究中，主要阐述了数字取证技术的范围，并介绍了当前几种流行的取证技术。对于数字取证程序的研究，主要探讨了数字取证程序的要求和研究方法，并从实体法、程序法和证据法三种角度对国内外数字取证相关法律进行了分析。此外，还对数字取证工具功能和规范分别进行了详细的研究。

对于数字取证，重点在于如何收集及分析电子证据，而电子证据目前在国内还没有被采纳作为一种独立的证据形式。为了使立法工作者、计算机犯罪侦查取证人员及相关读者更加深入地了解电子证据，在《电子证据》一书中，作者借鉴了证据学的理论和方法，探讨了电子证据的概念、立法情况，从不同方面考查了电子证据的来源，依据证据学中对证据的收集原则及方法，并根据电子证据自身的特点，对电子证据的收集作了详细的探讨。该书在总结电子证据特征的基础上，阐明了电子证据的形式，并从证据学的角度对电子证据和一般证据的保全、效力、认定和出示进行了比较，同时探讨了电子证据保全措施、电子证据效力的概念、电子证据认定的方法和电子证据出示的相关问题。

该丛书各书的附录部分收录了与该书相关的国内外法律、法规，给出了相关中英文名词对照表及主要参考文献，以供读者学习时参考。

近年来，有关计算机安全以及网络安全方面的书籍逐渐增多，这些著作大多从各自的研究角度出发，各有侧重，为不同层次的读者提供了宝贵的资料。但是，这些著作多数缺乏系统性，不能

构成完整的研究体系。因此，作者在该丛书的编写过程中，从不同的角度看待问题，力求各著作的完整性以及它们之间的统一性，试图形成较为完整的研究体系。该丛书具有如下几方面的特点：

第一，内容全面。该丛书对信息安全、信息对抗、计算机犯罪侦查、数字取证以及电子证据所涉及的问题都作了详细的研究，以全新、全面、深刻的视角分析了各领域的研究内容。五本书的研究内容紧密相关、环环相扣，构成了从信息安全到计算机犯罪侦查取证较为完整的体系。前者可作为后续书籍研究的基础，是后续书籍编著的主要起因，对后续书籍的编著和研究起到了铺垫作用；后续书籍是前者继续研究与发展的结果。该丛书围绕技术和法律两条主线研究和探索信息安全问题，其中《信息安全》和《信息对抗》主要是从技术角度来认识信息安全问题并研究防御措施，《计算机犯罪侦查》、《数字取证》和《电子证据》主要从法律角度来研究和探讨计算机犯罪侦查、数字取证及电子证据的相关问题。

第二，内容易懂。作者以简洁的语言和清晰的叙述方法，向读者介绍了各研究领域的基本理论、基本知识和常用技术。作者在阐述较为专业的知识和技术时，力求做到准确、科学，并尽量使用较为通俗的语言。在介绍最新的理论和技术时，通过对相关知识背景的介绍，方便了读者理解和掌握。

第三，材料新颖。该丛书较以往相关方面的著作有明显的突破和创新，作者对目前的研究现状进行跟踪，补充了最新的研究成果。信息技术的发展非常迅速，为了使这五本书能反映出最新的理论和技术，尽量靠近新知识、新技术前沿，作者参考、研究了大量国内外书籍以及互联网上最新的资料。

第四，实用性较强。在该丛书的编写过程中，作者突出了技术的实用性，如在讲述信息安全理论的同时，还介绍了有关信息安全产品及其应用技术，以便读者理解和掌握，有利于自学。

第五，展望趋势。作者通过对信息安全及计算机犯罪侦查取证方面的多年研究，对各领域的研究背景和现状都进行了深入的

分析，同时展望了各领域未来的发展趋势。这五本书都具有比较重要的研究和参考价值。

在该丛书的编写过程中，得到了公安部有关司局、中国人民公安大学及南京市公安局有关领导的大力支持和精心指导，得到了中国人民公安大学王大中教授、王靖亚副教授、曹金璇副教授和南京师范大学宋如顺教授的帮助与配合，从事本专业研究的硕士研究生王亮、张羽、赵洁、刘志高、李素娟、李学宝等也为该丛书的出版做了大量工作。此外，该丛书还参考了许多国内外学者及实务工作者的论著及研究成果。在此，一并表示衷心的感谢。

该丛书可作为政法系统高等院校信息安全、法学等专业以及其他高等院校和科研院所相关专业的研究生、高年级本科生的教学用书或教学参考书，也可作为信息安全、法学等领域的研究人员、技术人员和管理人员的学习资料，还可作为政法系统相关执法人员的工作参考书。我们相信，这套丛书的出版，将对我国信息安全、计算机犯罪侦查取证等方面的理论研究和实践应用起到重要的推动与促进作用。

编　者

2006 年 8 月

前　言

目前，很多人认为数字取证（Digital Forensics）是针对计算机犯罪进行的取证活动，实则不然。数字取证具有广义的范畴，它不但包括对计算机犯罪进行取证，还包括对其他刑事犯罪、民事案件、行政案件、工作疏忽或设备故障中涉及的计算机或其他数字产品进行取证。

数字取证涉及法学、刑事侦查学和计算机科学等学科，因而要从这些不同学科的角度及其相互关系等方面进行研究。美国等发达国家于20世纪80年代开始研究数字取证，在取证思想、理论、技术、方法等方面取得了不少成果。现在美国至少有70%的法律部门拥有自己的计算机取证实验室，经过资格认定的取证专家使用专门技术，通过网络或从犯罪现场获取的计算机和外设进行证据的提取和分析，目的在于提供非法活动的证据，并将这些证据提交给法庭，作为裁决的依据。近年来，我国研究机构和有关部门已经意识到数字取证的重要性，开始进行理论探讨和技术开发。但到目前为止，我国对于数字取证仍缺乏系统的研究。

本书首先分析了国内外数字取证的研究状况，在此基础上归纳提出了数字取证的概念，并对数字取证研究趋势进行了预测。对于数字取证技术的研究，主要界定了数字取证技术的范围，并介绍了当前几种流行的取证技术。对于数字取证程序的研究，主要从国内外两方面进行分析，给出了数字取证程序的要求和研究方法。对于数字取证法律的研究，主要从实体法、程序法和证据法三种角度对国内外数字取证相关法律进行了分析与探讨。此外，本书还对数字取证工具和规范分别进行了详细的阐述。本书附录部分收录了国内外数字取证方面的法律、法规，给出了相关专有

名词中英文对照表及主要参考文献，以供读者学习时参考。

由于数字取证是一个新领域，加之作者水平有限，书中难免有疏漏和不妥之处，敬请读者批评指正。

作　者

2006 年 8 月

目　录