信息安全系列教材

计算机取证技术

主　编　陈　龙　麦永浩　黄传河
副主编　董振兴　史文明　宋秀丽

WUHAN UNIVERSITY PRESS
武汉大学出版社

信息安全系列教材

计算机取证技术

主　编　陈　龙　麦永浩　黄传河
副主编　董振兴　史文明　宋秀丽
参　编　董　强

本教材的写作、出版得到了以下项目的资助：重庆邮电大学重点教材建设项目(编号：JC2006-05)、重庆市自然科学基金重点项目(编号：2005BA2003)、重庆市教委骨干教师资助计划、湖北省教育厅十五规划项目(编号：2004d349)、湖北省社会科学基金“十五”规划项目(编号：[2005]073)、公安部应用创新计划项目(编号：公科研[2005]246号)、公安部公安理论及软科学研究计划项目(编号：公科研[2005]245号)、2006年度湖北省博士后科技活动择优资助项目。在此一并致谢!

WUHAN UNIVERSITY PRESS
武汉大学出版社

图书在版编目(CIP)数据

计算机取证技术/陈龙，麦永浩，黄传河主编．—武汉：武汉大学出版社，2007.3

信息安全系列教材

ISBN 978-7-307-05429-5

Ⅰ.计… Ⅱ.①陈… ②麦… ③黄… Ⅲ.计算机犯罪—证据—调查—高等学校—教材 Ⅳ.D915.13

中国版本图书馆 CIP 数据核字(2007)第 023113 号

责任编辑：黄金文 夏炽元 责任校对：黄添生 版式设计：支 笛

出版发行：**武汉大学出版社** (430072 武昌 珞珈山)

(电子邮件：wdp4@whu.edu.cn 网址：www.wdp.com.cn)

印刷：华中科技大学印刷厂

开本：787×1092 1/16 印张：13.75 字数：339 千字

版次：2007 年 3 月第 1 版 2007 年 3 月第 1 次印刷

ISBN 978-7-307-05429-5/D・716 定价：22.00 元

信息安全系列教材

编 委 会

内容简介

本书介绍了计算机取证的原则和基本的法律、法规理念，全面阐述了计算机取证的基本原理与技术，编写了若干案例帮助读者全面理解计算机取证。全书分为计算机取证概论、计算机取证基础、计算机取证的法学问题、计算机取证技术、Windows 系统取证、LINUX 系统取证、网络环境下的计算机取证、计算机取证案例和计算机取证课程实验，共九章。

本书可作为各高等院校开设的信息安全相关专业的本科教材，也可供初学、准备从事相关研究的研究生参考，对从事公安网络监察、司法（计算机）、网络安全管理等领域的人员有参考价值。

序　言

21 世纪是信息的时代，信息成为一种重要的战略资源，信息的安全保障能力成为一个国家综合国力的重要组成部分。一方面，信息科学和技术正处于空前繁荣的阶段，信息产业成为世界第一大产业。另一方面，危害信息安全的事件不断发生，信息安全的形势是严峻的。

信息安全事关国家安全，事关社会稳定，必须采取措施确保我国的信息安全。

我国政府高度重视信息安全技术与产业的发展，先后在成都、上海和武汉建立了信息安全产业基地。

发展信息安全技术和产业，人才是关键。人才培养，教育是根本。2001 年经教育部批准，武汉大学创建了全国第一个信息安全本科专业。2003 年经国务院学位办批准，武汉大学又建立了信息安全的硕士点、博士点和企业博士后产业基地。自此以后，我国的信息安全专业得到迅速的发展。到目前为止，全国设立信息安全专业的高等院校已达 50 多所。我国的信息安全人才培养进入蓬勃发展阶段。

为了给信息安全专业的大学生提供一套适用的教材，武汉大学出版社组织全国 40 多所高校，联合编写出版了这套《信息安全系列教材》。该套教材涵盖了信息安全的主要专业领域，既有基础课教材，又有专业课教材，既有理论课教材，又有实验课教材。

这套书的特点是内容全面，技术新颖，理论联系实际。教材结构合理，内容翔实，通俗易懂，重点突出，便于讲解和学习。它的出版发行，一定会推动我国信息安全人才培养事业的发展。

诚恳希望读者对本系列教材的缺点和不足提出宝贵的意见。

编委会

2006 年 9 月 19 日

前 言

计算机取证是交叉学科，涉及计算机科学、法学、刑事侦查学等多个领域。作为一个新的领域，在我国研究与实践的时间都不长，但打击计算机犯罪等现实需求使得对此领域感兴趣的人越来越多，计算机取证将得到更加迅速的发展。

国内在计算机取证研究、实践、教学等方面都有不少突出的专家，但都十分繁忙，难以顾及教材编写工作。据了解，国内的警察类院校已开设过相关的课程，现在信息安全专业也已有几届毕业生，但国内尚无自编教材可供使用，只有一些翻译书籍。2005 年武汉大学出版社组织出版信息安全系统教材，将《计算机取证技术》列入了规划，必然会对计算机取证人才的培养起到积极的推动作用。

本教材注重系统性，将计算机取证原理与实践相结合。

全书共分九章。第一章计算机取证概论，介绍了有关计算机取证的基本概念，计算机取证的发展、取证目标、取证原则和技术，最后分析了计算机取证面临的困难和发展趋势。第二章计算机取证基础，介绍了数据存储介质、文件系统、数据加密和数据隐藏以及入侵与入侵检测的信息源等背景知识。第三章计算机取证的法学问题，阐述了计算机取证的法律依据，电子签名法的主要精神，电子证据的法律认定、电子数据鉴定规范与政策，给出了一个电子数据鉴定报告实例。第四章计算机取证技术，以计算机取证的法律执行过程模型为主线分别介绍了计算机取证准备，计算机证据收集与保存、计算机证据提取、计算机证据的检验与分析等相关技术知识和磁盘映像工具。第五章 Windows 系统取证，介绍了计算机系统运行现场数据收集方法，Windows 系统证据收集与推理，Windows 反取证技术和集成取证工具 Encase、FTK。第六章 LINUX 系统取证，介绍了系统现场数据收集，LINUX 系统证据收集与推理和取证工具 TCT、ForensicX。第七章网络环境下的计算机取证，主要讨论 Web 浏览、电子邮件、即时通信、P2P 应用等几种典型网络应用的取证问题和以网络监视为手段的网络数据流实时取证及其分析。第八章计算机取证案例，收集、整理、撰写了五个案例，案例类型丰富，有故事性的，探讨性的，实践性的案例。第九章计算机取证课程实验，设计了一些可供开设的配套实验，也有建议读者自行锻炼而可以选做的实验，将来可考虑在网络上提供模拟案例和真实案例的数据。可用于计算机取证的各种小工具众多，如果单独把这些工具整理归纳到一起会使本教材成为工具手册，所以各章在涉及到相关内容时会单独介绍或使用各自的工具，同类工具的原理是相通的，所以读者不必担心。

目前国内翻译国外的计算机取证书籍已有一些，但还没有计算机取证的教材，教学和新进入该领域的人员都急需计算机取证方面的教材。本书内容全面，针对性强，作为国内该领域的第一本教材，想必对读者会有很大的帮助。

在武汉大学出版社的组织下，重庆邮电大学计算机科学与技术学院陈龙副教授与湖北警官学院麦永浩教授、武汉大学计算机学院黄传河教授担任本书主编。参加编写工作的具体分工是：陈龙副教授主持编写第一章、第七章、第八章，麦永浩教授主持编写第三章，黄传河

教授主持编写第四章，中国地质大学计算机学院史文明高级工程师主持编写第五章，重庆邮电大学计算机科学与技术学院的讲师董振兴主持编写第二章和第六章，宋秀丽主持编写第九章。全书由陈龙负责统稿。

本书可作为各高等院校开设的信息安全相关专业的本科教材，也可供初学、准备从事相关研究的研究生参考，对从事公安网络监察、司法实践、网络安全管理等领域的人员有参考价值。

在本书的编写过程中，有重庆邮电大学计算机科学与技术研究所的王应、方敏、方新蕾、武汉大学计算机学院黄传河实验室的韩长霖、王庆刚等四位硕士研究生参与了部分资料收集与整理，方新蕾为本书排版作了部分工作。在此对所有参与本书编写工作的老师和同学表示衷心感谢。在此要特别感谢武汉大学张焕国教授、武汉大学出版社黄金文副编审对编写本教材所给予的建议与帮助。在此也感谢我的导师王国胤教授多年来给我的指导、关心和鼓励。

因从教材体系结构设计到教材内容选取等都是全新的，加之作者水平有限，书中一定存在不恰当甚至错误的地方，恳请老师、同学、专家等各类读者提出意见与建议，作者将十分感谢！

作者

2006 年 10 月

目 录

第1章 计算机取证概论

1.1 计算机取证基本概念

计算机和网络越来越多地参与到人们的工作与生活中，可以说已成为社会、政治、经济、文化生活的重要组成部分，与此相关的各种争议以及与计算机有关的犯罪现象越来越多。打击并遏制犯罪，维护社会公正、公平依赖于法律，法庭依照法律进行判决时需要证据。计算机取证（computer forensics）为解决民事纠纷和打击计算机犯罪将提供科学的方法和手段，可以提供法庭需要的合适证据。

人们对于传统的取证并不陌生，但很少有人知道通过分析计算机和网络的有关状态、运行过程等可以获知有关人员的行为。计算机在相关的犯罪案例中可以扮演黑客入侵的目标、作案的工具和犯罪信息的存储器这三种角色。无论作为哪种角色，通常计算机（连同它的外设）中都会留下大量与犯罪有关的数据，进而可以依据有关科学与技术的原理和方法找到证明某个事实的证据。

1.1.1 计算机取证的定义

目前，计算机取证还没有统一、准确的定义。

Lee Garber 在 IEEE Security 发表的文章中认为，计算机取证是分析硬盘、光盘、软盘、Zip 和 Jazz 磁盘、内存缓冲以及其他形式的存储介质以发现犯罪证据的过程。

计算机取证资深专家 Judd Robbins 给出了如下的定义：计算机取证是将计算机调查和分析技术应用于对潜在的、有法律效力的证据的确定与获取。

计算机紧急事件响应组 CERT 和取证咨询公司 NTI（New Technologies Incorporated）进一步扩展了该定义：计算机取证包括了对以磁介质编码信息方式存储的计算机证据的保护、确认、提取和归档。

SANS 公司则归结为：计算机取证是使用软件和工具，按照一些预先定义的程序，全面地检查计算机系统，以提取和保护有关计算机犯罪的证据。

参考一般取证的含义，关注计算机取证本质层面的意义，综合起来，我们认为计算机取证是运用计算机及其相关科学和技术的原理与方法获取与计算机相关的证据以证明某个客观事实的过程。它包括对计算机证据的确定、收集、保护、分析、归档以及法庭出示。

有人将计算机取证看成是计算机司法鉴定，有必要解释相关概念：

何谓司法鉴定？一种解释认为，“司法鉴定是鉴定人运用科学技术或者专门知识对涉及诉讼的专门性问题进行检验、鉴别和判断并提供鉴定结论的活动”，强调的是鉴定人向委托人提供鉴定结论的一种服务；另一种解释将司法鉴定界定为，“在诉讼过程中，为查明案件事实，人民法院依据职权，或者应当事人及其他诉讼参与人的申请，指派或委托具有专门知识的人，

对专门性问题进行检验、鉴别和评定的活动”，强调这种鉴定是由审判法庭启动实施的，具有司法的中立性，显然是比较狭义的解释。

总体而言，计算机取证的内涵要丰富得多。计算机司法鉴定的检验、鉴别和判断等活动则属于计算机取证的一部分。

1.1.2 计算机证据

证据在司法证明中的作用是毋庸置疑的，它是法官判定罪与非罪的标准。在人类的司法证明发展过程中，证明方法和手段经历了两次重大转变。第一次是从以“神证”为主的证明向以“人证”为主的证明的转变。第二次是从以“人证”为主的证明向以“物证”或“科学证据”为主的证明的转变。

在很长的历史时期内，物证在司法活动中的运用一直处于随机和分散发展的状态。直到18世纪以后，与物证有关的科学技术才逐渐形成体系和规模，物证在司法证明中的作用也才越来越重要起来。随着科学技术的突飞猛进，各种以人身识别为核心的物证技术层出不穷。例如，继笔迹鉴定法、人体测量法和指纹鉴定法之后，足迹鉴定、牙痕鉴定、声纹鉴定、唇纹鉴定等技术不断地扩充着司法证明的“武器库”。特别是20世纪80年代出现的DNA遗传基因鉴定技术，更带来了司法证明方法的一次新的飞跃。计算机证据的出现将为司法证明方法带来新的进步。由于计算机证据的特殊性，对传统证据规则也带来新挑战。

计算机证据是指以计算机形式存在的、用作证据使用的一切材料及其派生物，或者说借助计算机生成的一切证据。

与计算机取证有关的证据的术语比较多（新领域都会出现此问题），如：计算机证据、电子证据、网络证据、数字证据等。

我们对计算机证据与电子证据进行一下对比。计算机证据与电子证据有着千丝万缕的联系但却不同于电子证据。很多时候，计算机证据在外延上要大于电子证据，因为以机械式计算机、光学计算机、生物计算机为基础的证据只能从“功能上等同”的角度临时当作电子证据处理，显然不是典型的计算机证据。电子证据在外延上也可能大于计算机证据，例如固定电话机是基于属于模拟电子技术的半导体技术而制成的现代通信工具，它所录制的电话资料就属于电子证据而不属于计算机证据。

以计算机科学为背景或从事技术工作的人多使用计算机证据，而我国司法实践领域、特别是法律界人事多使用电子证据一词。尽管计算机证据、电子证据在概念内涵和外延上是有差别的，但一般情况下使用时可以不严格区分，将来可以用标准化的方法指定某一术语来涵盖全部或特定的证据类型。本书后面不具体区分，一般使用“计算机取证”、“计算机证据”，讨论涉及具体实践等相关的其他场合使用“电子证据”。国外在计算机取证的基础上提出了数字取证（Digital Forensics），相应地有数字证据（Digital Evidence），这些术语在国外已得到比较普遍的承认。

任何材料要成为证据，均需具备三性：客观性、关联性、合法性。

计算机证据与传统证据一样，计算机证据必须是：

- 可信的。
- 准确的。
- 完整的，使法官信服的。
- 符合法律法规的，即可为法庭所接受的。

计算机证据与传统的证据相比较,新特性多,其中突出的有:

(1)计算机证据同时具有较高的精密性和脆弱易逝性。一方面,计算机证据以技术为依托,很少受主观因素的影响,能够避免其他证据的一些弊端,如证言的误传、书证的误记等;另一方面,由于计算机信息是用二进制数据表示的,以数字信号的方式存在,而数字信号是非连续性的,故意或因为差错对计算机证据进行的变更、删除、删节、剪接、截收和监听等,从技术上讲很难查清。

(2)计算机证据具有较强的隐蔽性。计算机证据在计算机系统中可存在的范围很广,使得证据容易被隐藏。另外,由于计算机证据在存储、处理的过程中,其信息的表示形式为二进制编码,无法直接阅读。一切信息都由编码来表示并传递,使得计算机证据与特定主体之间的关系按照常规手段难以确定。计算机数据不是肉眼直接可见的,必须借助适当的工具。

(3)计算机证据具有多媒性。计算机证据的表现形式是多样的,尤其是多媒体技术的出现,更使计算机证据综合了文本、图形、图像、动画、音频及视频等多种媒体信息,这种以多媒体形式存在的计算机证据几乎涵盖了所有传统证据类型。

(4)计算机证据还具有收集迅速、易于保存、占用空间少、容量大、传送和运输方便、可以反复重现、易于使用、便于操作等特点。

(5)相关数据的"挥发性"。数据挥发特性主要从时间上体现,内容见表1-1。

表1-1 数据存留时间

数据	硬件或位置	存活时间
CPU数据	高速缓冲存储器、管道	数个时钟周期
系统	RAM	直至系统关闭
内核表	进程中	直至系统关闭
固定介质	Swap/tmp	直至被覆盖或被抹掉
可移动的介质	Cdrom,Floppy,HDD	直至被覆盖或被抹掉
打印输出	硬拷贝打印输出	直至被毁坏

计算机证据的这些特点表明计算机取证面临不少难题,有完全不同于传统取证的问题需要研究。

1.1.3 计算机取证与计算机犯罪

1. 有关计算机犯罪的法律规定

我国对计算机犯罪进行规定的法律条文主要有:

(1) 非法侵入计算机信息系统罪。

《刑法》第二百八十五条规定,"违反国家规定,侵入国有事务、国防建设、尖端科学技术领域的计算机信息系统的,处3年以下有期徒刑或者拘役。"

(2) 破坏计算机信息系统罪。

这一行为《刑法》第二百八十六条概括为破坏计算机信息系统罪,主要表现为:

"违反国家规定,对计算机信息系统功能进行删除、修改、增加、干扰,造成计算机信息系统不能正常运行,后果严重的"行为。