21世纪高等学校规划教材 | 计算机应用

计算机取证与司法鉴定（第2版）

麦永浩 邹锦沛 许榕生 戴士剑 主编

清华大学出版社

21世纪高等学校规划教材

计算机取证与司法鉴定

（第2版）

麦永浩 邹锦沛 许榕生 戴士剑 主编

清华大学出版社
北京

内容简介

计算机取证与司法鉴定是法学和计算机科学的交叉学科，本书介绍了计算机取证与司法鉴定的国内外研究概况和发展趋势，分析了计算机取证与司法鉴定的证据效力和法律地位，指出了计算机取证与司法鉴定的特点和业务类型，阐述了计算机取证与司法鉴定的原则和过程模型，论述了计算机取证与司法鉴定的实施过程，介绍了常用的几种计算机取证与司法鉴定设备和分析工具，讨论了 Windows XP、Windows Vista 和 UNIX/Linux 系统的取证理论与方法，探讨了网络取证、QQ 取证、木马取证、手机取证和专业电子设备取证等特定取证类型的分析方法，最后给出了笔者所带领的团队完成的 7 个典型案例。

本书在学术理论上具有交叉性、前沿性和创新性，在实践应用中注重可操作性和实用性。本书可作为计算机学院和法学院的本科生和研究生教材，对于法学理论研究者、司法和执法工作者、律师、司法鉴定人和 IT 行业人士，也具有良好的参考价值。

图书在版编目(CIP)数据

计算机取证与司法鉴定/麦永浩等主编. --2 版. --北京：清华大学出版社，2014
21 世纪高等学校规划教材 · 计算机应用
ISBN 978-7-302-34542-8

Ⅰ. ①计… Ⅱ. ①麦… Ⅲ. ①计算机犯罪－证据－调查 ②计算机犯罪－司法鉴定 Ⅳ. ①D918

中国版本图书馆 CIP 数据核字(2013)第 277006 号

责任编辑：黄　芝　王冰飞
封面设计：傅瑞学
责任校对：时翠兰
责任印制：杨　艳

出版发行：清华大学出版社
网　　址：http://www.tup.com.cn，http://www.wqbook.com
地　　址：北京清华大学学研大厦 A 座　　邮　　编：100084
社 总 机：010-62770175　　邮　　购：010-62786544
投稿与读者服务：010-62776969，c-service@tup.tsinghua.edu.cn
质 量 反 馈：010-62772015，zhiliang@tup.tsinghua.edu.cn
课 件 下 载：http://www.tup.com.cn，010-62795954
印 刷 者：北京富博印刷有限公司
装 订 者：北京市密云县京文制本装订厂
经　　销：全国新华书店
开　　本：185mm×260mm　　**印　　张**：18.25　　**字　　数**：443 千字
版　　次：2009 年 3 月第 1 版　2014 年 3 月第 2 版　　**印　　次**：2014 年 3 月第1 次印刷
印　　数：1～2000
定　　价：34.50 元

产品编号：054478-01

编　委　会

主　编：麦永浩　邹锦沛　许榕生　戴士剑

副主编：孙国梓　张国栋　徐云峰　李俊娥　傅建明　张　俊

参　编：鲁　翱　向大为　张　鹏　隆　波　史　靓　魏　连

郝万里　危　蓉　吴燕波

出版说明

随着我国改革开放的进一步深化，高等教育也得到了快速发展，各地高校紧密结合地方经济建设发展需要，科学运用市场调节机制，加大了使用信息科学等现代科学技术提升、改造传统学科专业的投入力度，通过教育改革合理调整和配置了教育资源，优化了传统学科专业，积极为地方经济建设输送人才，为我国经济社会的快速、健康和可持续发展以及高等教育自身的改革发展作出了巨大贡献。但是，高等教育质量还需要进一步提高以适应经济社会发展的需要，不少高校的专业设置和结构不尽合理，教师队伍整体素质亟待提高，人才培养模式、教学内容和方法需要进一步转变，学生的实践能力和创新精神亟待加强。

教育部一直十分重视高等教育质量工作。2007 年 1 月，教育部下发了《关于实施高等学校本科教学质量与教学改革工程的意见》，计划实施“高等学校本科教学质量与教学改革工程（简称‘质量工程’）”，通过专业结构调整、课程教材建设、实践教学改革、教学团队建设等多项内容，进一步深化高等学校教学改革，提高人才培养的能力和水平，更好地满足经济社会发展对高素质人才的需要。在贯彻和落实教育部“质量工程”的过程中，各地高校发挥师资力量强、办学经验丰富、教学资源充裕等优势，对其特色专业及特色课程（群）加以规划、整理和总结，更新教学内容、改革课程体系，建设了一大批内容新、体系新、方法新、手段新的特色课程。在此基础上，经教育部相关教学指导委员会专家的指导和建议，清华大学出版社在多个领域精选各高校的特色课程，分别规划出版系列教材，以配合“质量工程”的实施，满足各高校教学质量和教学改革的需要。

为了深入贯彻落实教育部《关于加强高等学校本科教学工作，提高教学质量的若干意见》精神，紧密配合教育部已经启动的“高等学校教学质量与教学改革工程精品课程建设工作”，在有关专家、教授的倡议和有关部门的大力支持下，我们组织并成立了“清华大学出版社教材编审委员会”（以下简称“编委会”），旨在配合教育部制定精品课程教材的出版规划，讨论并实施精品课程教材的编写与出版工作。“编委会”成员皆来自全国各类高等学校教学与科研第一线的骨干教师，其中许多教师为各校相关院、系主管教学的院长或系主任。

按照教育部的要求，“编委会”一致认为，精品课程的建设工作从开始就要坚持高标准、严要求，处于一个比较高的起点上；精品课程教材应该能够反映各高校教学改革与课程建设的需要，要有特色风格、有创新性（新体系、新内容、新手段、新思路，教材的内容体系有较高的科学创新、技术创新和理念创新的含量）、先进性（对原有的学科体系有实质性的改革和发展，顺应并符合 21 世纪教学发展的规律，代表并引领课程发展的趋势和方向）、示范性（教材所体现的课程体系具有较广泛的辐射性和示范性）和一定的前瞻性。教材由个人申报或各校推荐（通过所在高校的“编委会”成员推荐），经“编委会”认真评审，最后由清华大学出版

社审定出版。

目前,针对计算机类和电子信息类相关专业成立了两个“编委会”,即“清华大学出版社计算机教材编审委员会”和“清华大学出版社电子信息教材编审委员会”。推出的特色精品教材包括:

(1) 21世纪高等学校规划教材·计算机应用——高等学校各类专业,特别是非计算机专业的计算机应用类教材。

(2) 21世纪高等学校规划教材·计算机科学与技术——高等学校计算机相关专业的教材。

(3) 21世纪高等学校规划教材·电子信息——高等学校电子信息相关专业的教材。

(4) 21世纪高等学校规划教材·软件工程——高等学校软件工程相关专业的教材。

(5) 21世纪高等学校规划教材·信息管理与信息系统。

(6) 21世纪高等学校规划教材·财经管理与应用。

(7) 21世纪高等学校规划教材·电子商务。

(8) 21世纪高等学校规划教材·物联网。

清华大学出版社经过三十多年的努力,在教材尤其是计算机和电子信息类专业教材出版方面树立了权威品牌,为我国的高等教育事业作出了重要贡献。清华版教材形成了技术准确、内容严谨的独特风格,这种风格将延续并反映在特色精品教材的建设中。

清华大学出版社教材编审委员会

联系人:魏江江

E-mail:weijj@tup.tsinghua.edu.cn

前言

计算机取证与司法鉴定是研究如何对计算机证据进行获取、保存、分析和出示的法律规范和科学技术。计算机取证与司法鉴定既是一个法学问题，又是一个计算机科学与技术问题；既是一个法学理论问题，又是一个司法实务问题。

计算机证据是一种十分重要的证据，已经被誉为信息社会的“证据之王”，可以通过计算机取证与司法鉴定寻找案件线索，也可以通过计算机取证与司法鉴定将计算机证据转化为法定证据，从而在法庭上胜诉定案。

计算机取证与司法鉴定是计算机案件审判和量刑的关键依据，由于计算机证据具有易修改性、实时性、设备依赖性，又具有可以精确重复性等高科技特性，因此必须将计算机取证与司法鉴定的特殊性和一般性相结合，研究计算机证据现场勘查、获取、保全、运用、审查和确认的各环节，以保证计算机证据的客观性、合法性和关联性。

本书从法学的角度分析了计算机证据的法律性质、类型、效力及取证规则，从计算机科学与技术角度研究了计算机证据的收集分析技术。

计算机犯罪是21世纪破坏性最大的一类犯罪，要打击和遏制这种犯罪，计算机取证与司法鉴定承担着不可取代的作用，这是法学与计算机科学紧密结合的边缘学科、交叉学科和新兴学科，是当前或不久的将来，我国信息网络安全亟须解决的重要问题，具有强烈的社会需求，具有鲜明的时代性和创新特点。

本书介绍了计算机取证与司法鉴定的国内外研究概况和发展趋势，分析了计算机取证与司法鉴定的证据效力和法律地位，指出了计算机取证与司法鉴定的特点和业务类型，阐述了计算机取证与司法鉴定的原则和过程模型，论述了计算机取证与司法鉴定的实施过程，介绍了常用的几种计算机取证与司法鉴定设备和分析工具，讨论了 Windows XP、Windows Vista 和 UNIX/Linux 系统的取证理论与方法，探讨了网络取证、QQ 取证、木马取证、手机取证和专业电子设备取证等特定取证类型的分析方法，最后给出了笔者所带领的团队完成的7个典型案例。

由于计算机取证与司法鉴定、电子取证、电子数据取证和司法鉴定有很多的共同点，因此本书在不引起歧义的情况下，有时并不区分它们。

本书从各种论文、书刊、期刊和互联网中引用了大量资料，有的在参考文献中列出，有的无法查证，在此对这些资料的作者表示感谢。由于时间和水平有限，书中难免存在疏漏与不妥之处，恳请各位专家批评、指正，使本研究成果得以改进和完善。

本书为国家科学基金项目(07BFX062)：计算机取证研究成果，电子数据取证湖北省协同创新中心成果。

编　者

2013年10月

目 录

第1章 计算机取证与司法鉴定概论

计算机犯罪是21世纪破坏性最大的一类犯罪，要打击和遏制这种犯罪，计算机取证与司法鉴定承担着不可取代的作用，这是法学与计算机科学紧密结合的边缘学科、交叉学科和新兴学科，是当前或不久的将来我国信息网络安全亟须解决的重要问题，具有鲜明的时代性和创新特点。由于计算机取证与司法鉴定、电子取证、电子数据取证和司法鉴定有很多的共同点，因此本书在不引起歧义的情况下，有时并不区分它们。

1.1 概述

1.1.1 计算机取证与司法鉴定

关于计算机取证与司法鉴定(Computer Forensics and Judicial Identification)，目前还没有权威组织给出一个统一的定义，很多的专业人士和机构从不同的角度给出了计算机取证与司法鉴定的定义。Judd Robbins是计算机取证与司法鉴定方面的一位著名的专家和资深人士，他对计算机取证与司法鉴定的定义如下："计算机取证与司法鉴定不过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和取证咨询公司New Technologies进一步扩展了该定义："计算机取证与司法鉴定是对计算机证据的保护、确认、提取和归档的过程"。取证专家Reith Clint Mark认为计算机取证与司法鉴定可以认为是"从计算机中收集和发现证据的技术和工具"。

此外，还有电子数字取证(Electronic Digital Forensics)和电子取证(Electronic Forensics)等，这与计算机取证与司法鉴定是有所区别的：计算机取证与司法鉴定的主体对象是计算机系统内与案件有关的数据信息，电子数字取证的主体对象是存在于各种电子设备和计算机系统中与案件有关的数字化数据信息，而电子取证的主体对象是指电子化存储的、能反映有关案件真实情况的数据信息。

本书受客观和主观所限，论述和举例时往往针对刑事案件，但是，计算机取证与司法鉴定对于民事案件、行政案件和非诉讼活动也具有重要的意义，对于一些基本的技术环节，区别并不大。因此，本书对计算机取证与司法鉴定进行了分层，提出了计算机取证与司法鉴定的层次功能表，如表1-1所示。

表 1-1 计算机取证与司法鉴定的层次功能表

<table>
<tr><td rowspan="9">计算机取证与司法鉴定</td><td rowspan="2">证据层</td><td colspan="2">溯源取证</td><td colspan="2">同一取证</td><td colspan="2">内容取证</td><td colspan="2">刑事责任</td></tr>
<tr><td colspan="2"></td><td colspan="2"></td><td colspan="2"></td><td colspan="2">行政责任</td></tr>
<tr><td colspan="3">功能取证</td><td colspan="3">复合取证</td><td colspan="2">民事责任</td></tr>
<tr><td colspan="3"></td><td colspan="3"></td><td colspan="2">非诉讼活动</td></tr>
<tr><td rowspan="2">应用层</td><td colspan="3">用户行为取证</td><td colspan="3">手机数据取证</td><td colspan="2">数据库取证</td></tr>
<tr><td colspan="2">计算机病毒与恶意代码取证</td><td colspan="2">电子数据相似性取证</td><td>网络数据取证</td><td colspan="2">电子文档与数据电文取证</td></tr>
<tr><td rowspan="3">技术层</td><td colspan="4">基础技术</td><td colspan="4" rowspan="3">主机证据保全、恢复和分析技术；网络数据捕获与分析、网络追踪技术；主动取证技术；密码分析与破解技术等</td></tr>
<tr><td colspan="4">网络技术</td></tr>
<tr><td colspan="4">工具集成运用</td></tr>
<tr><td>基础层</td><td colspan="2">法律基础</td><td colspan="2">规范标准</td><td colspan="2">技术基础</td><td>案例研究</td></tr>
</table>

1.1.2 计算机取证与司法鉴定的研究现状

1. 国外的研究概况

1984 年美国 FBI 成立了计算机分析响应组(Computer Analysis and Response Team, CART),20 世纪 90 年代创立的“国际计算机证据组织(www. ioce. org)”就是要保护国家之间在计算机证据处理方法和实践上的一致性,保证从一个国家收集的数字证据能在另外一个国家使用。1998 年成立了“数字证据工作组(www. swgde. org)”,该工作组在几年前提出了“同行评审期刊”,进而推出“国际数字证据期刊(www. ijde. org)”。2000 年业内许多专家逐渐意识到由于取证理论的匮乏所带来的种种问题,因此又开始对取证程序及取证标准等基本问题进行研究,并提出了几种典型的取证过程模型,即基本过程模型(Basic Process Model)、事件响应过程模型(Incident Response Process Model)、法律执行过程模型(Law Enforcement Process Model)、过程抽象模型(Abstract Process Model)和其他过程模型。2003 年,“美国犯罪实验室主任协会/实验鉴定委员会(ASCLD/LAB)”制定了新的鉴定手册,包含了美国犯罪实验室中为数字证据取证人员制定的标准和准则。2004 年,“英国法学服务”计划建立一个资格专家注册库。2008—2011 年,有些欧洲组织,包括“欧洲法学研究所(ENFSI)”为计算机取证与司法鉴定人员出版、撰写了系列指南性的检验和报告。在国外,这个领域日新月异。

2. 国内的研究概况

2005 年 11 月,我国在北京成立了电子取证专家委员会,并举办了首届计算机取证与司法鉴定技术研讨会,2007 年 8 月,在新疆乌鲁木齐举办了第二届计算机取证与司法鉴定技术研讨会。2005 年以来,CCFC 计算机取证与司法鉴定技术峰会和高峰论坛也非常活跃,举办了三次大型活动。2007—2011 年,在国际反恐警用装备展中,电子取证的软硬件等设备,开始成为亮点。目前,中科院在网络入侵取证、武汉大学和复旦大学在密码技术、吉林大学在网络逆向追踪、电子科技大学在网络诱骗、北京航空航天大学在入侵诱骗模型等方面都展开了研究工作。湖北警官学院在计算机取证与司法鉴定方面的研究工作走在公安院校的前列。在国内,这个领域已经开始非常活跃。