

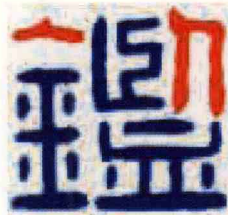
司法鉴定教育培训系列教材

司法部司法鉴定管理局 组织编写

# 电子数据司法鉴定实务

DIAN ZI SHU JU SI FA JIAN DING SHI WU

麦永浩 主编



法律出版社  
LAW PRESS · CHINA

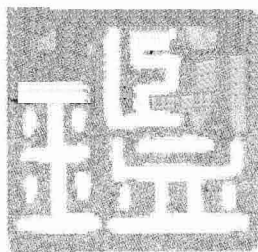
司法鉴定教育培训系列教材

司法部司法鉴定管理局 组织编写

# 电子数据司法鉴定实务

DIAN ZI SHU JU SI FA JIAN DING SHI WU

主 编 麦永浩  
副主编 赵 庸 金 波



法律出版社  
LAW PRESS · CHINA

## 图书在版编目(CIP)数据

电子数据司法鉴定实务 / 麦永浩主编. —北京:  
法律出版社, 2011. 8

司法鉴定教育培训系列教材

ISBN 978-7-5118-2421-9

I. ①电… II. ①麦… III. ①计算机犯罪—司法鉴定  
—技术培训—教材 IV. ①D918.9

中国版本图书馆 CIP 数据核字(2011)第 164996 号

© 法律出版社·中国

责任编辑/齐梓伊

装帧设计/乔智炜

出版/法律出版社

编辑统筹/综合出版分社

总发行/中国法律图书有限公司

经销/新华书店

印刷/北京北苑印刷有限责任公司

责任印制/张宇东

开本/787 毫米×960 毫米 1/16

印张/27.25 字数/484 千

版本/2011 年 12 月第 1 版

印次/2011 年 12 月第 1 次印刷

法律出版社/北京市丰台区莲花池西里 7 号(100073)

电子邮件/info@lawpress.com.cn

销售热线/010-63939792/9779

网址/www.lawpress.com.cn

咨询电话/010-63939796

中国法律图书有限公司/北京市丰台区莲花池西里 7 号(100073)

全国各地中法图分、子公司电话:

第一法律书店/010-63939781/9782

西安分公司/029-85388843

重庆公司/023-65382816/2908

上海公司/021-62071010/1636

北京分公司/010-62534456

深圳公司/0755-83072995

书号:ISBN 978-7-5118-2421-9

定价:58.00 元

(如有缺页或倒装,中国法律图书有限公司负责退换)

## 作者简介

**麦永浩** 湖北警官学院电子取证重点实验室主任,教授,计算机国家司法鉴定人,中国电子取证专家委员会委员,教育部高等学校计算机科学与技术专业教学指导分委员会专家组成员,武汉大学、中国人民大学兼职教授,武汉大学刑法学出站博士后,华东理工大学计算机科学与信息工程学院博士。邮箱:myh9999@163.com。

**赵庸** 中国电子学会高级会员、中国电子学会计算机取证专家委员会委员、国际 HTCIA 成员、福建警察学院客座教授、厦门市美亚柏科信息股份有限公司副总经理、福建中证司法鉴定中心主任、厦门市司法鉴定人协会理事。长期从事电子数据勘查、取证、鉴定技术研究和司法鉴定实践工作,参与了 GA/T 754—2008《电子数据存储介质复制工具要求及检测方法》和 GA/T 755—2008《电子数据存储介质写保护设备要求及检测方法》两个标准的编写。

**金波** 博士,研究员。公安部第三研究所信息网络安全首席科学家,信息网络安全公安部重点实验室主任,国家 863 反计算机入侵和防病毒研究中心总工程师,上海辰星电子数据司法鉴定中心主任,司法鉴定领域能力验证技术专家,上海法院知识产权技术咨询专家,上海市司法鉴定协会常务理事兼电子数据专业委员会主任。主持开发了我国第一套电子数据取证软件。上海交通大学、西安交通大学、重庆邮电大学兼职研究生导师。获国务院政府特殊津贴,获国家科学技术二等奖、公安部科学技术二等奖、全军科技进步二等奖等多项科技奖。

**戴士剑** 最高人民检察院技术中心高级工程师。

**刘品新** 法学博士,中国人民大学法学院副教授,证据学研究所副所长,电子证据国家司法鉴定人,中国人民大学刑事法律科学研究中心专职研究员,美国伊利诺伊大学访问学者,中国行为法学会理事,北京市侦查学研究会常务理事,中国电子学会计算机取证专家委员会委员。

**罗铂铀** 重庆市公安局公共信息网络安全监察总队政委, 硕士, 工程师, 公安部备案信息网络安全专家, 勘查取证技术手段建设的技术顾问, 承担着全国网安系统重要技术建设课题和重大疑难案件的攻关、咨询和指导等职责。作为最高管理者, 承担了重庆市公安局电子物证司法鉴定中心 CNAS 认证工作。

**陈 龙** 重庆邮电大学计算机科学与技术学院教授, 博士, 中国人工智能学会智能数字内容安全专业委员会委员, 中国计算机学会高级会员, 计算机司法鉴定人, 人民法院知识产权案件专家辅助人, 国际期刊《International Journal of Communication and Security》编委。主要研究领域为计算机取证、网络安全、智能信息处理。

**陈建民** 南开大学软件工程硕士, 北京工业大学计算机专业博士研究生, 中共党员, 高级工程师, 现任国家计算机病毒应急处理中心副主任, 公安部计算机病毒防治产品检验中心副主任, 亚洲反计算机病毒协会(AVAR)专家委员, 中国计算机安全专业委员会委员, 国家信息安全等级保护安全建设指导专家委员会专家, 国家信息安全产品认证专项工作组成员, 电子工业出版社《安全技术大系》专家委员会成员。主要研究方向为网络安全与计算机犯罪鉴定。

**杜振华** 南开大学软件工程硕士, 中共党员, 现任国家计算机病毒应急处理中心工程师, 主要研究方向为恶意代码分析与网站安全监测。

**沙 晶** 公安部第三研究所副研究员, 计算机国家司法鉴定人, 长期从事电子物证鉴定、信息网络安全、软件开发方面的研究和实践工作。中国合格评定国家认可委员会(CNAS)能力验证专家。2010 年荣获司法部“首届全国司法鉴定先进个人”称号。

**向大为** 湖北警官学院电子取证重点实验室、网络犯罪侦查教研室专职研究员, 计算机国家司法鉴定人, 湖北三真司法鉴定所优秀鉴定人。熊猫烧香病毒案、云南新东方网络赌博案、咸宁 500 亿赌球案等多起公安部督办案件第一鉴定人。研究领域: 计算机取证与司法鉴定、网络犯罪侦查。

**毛宪标** 福建中证司法鉴定中心副主任, MCE 认证调查员, CISP 注册信息安全专业人员。毕业于福州大学数学与计算机科学学院, 毕业即从事电子数据

司法鉴定相关工作,长期工作在计算机取证以及电子数据司法鉴定一线,积累了大量实战经验。

**隆波** 空军某部自动化站站长,主要从事电子取证鉴定研究。

**史经纬** 中国工商银行数据中心(北京)专职信息安全人员。

**孙国梓** 博士,副教授,南京邮电大学计算机技术研究所副所长,南京邮电大学计算机学院信息安全系副主任,中国计算机学会会员,中国人工智能学会智能数字内容安全专业委员会、江苏省计算机学会计算机安全专业委员会、计算机与通信专业委员会委员,全国计算机继续教育研究会江苏委员会理事,南京航空航天大学机械制造及自动化专业工学博士。清华大学博士后流动站出站后回南京邮电大学工作至今,多年来一直从事计算机取证、计算机网络及信息安全、嵌入式系统、企业信息化工程与电子政务工程的总体规划等相关理论和应用研究。

**王跃聪** 福建中证司法鉴定中心副所长,工程师,CNAS实验室认可内审员、评审员。长期从事电子数据司法鉴定工作以及实验室建设工作,负责指导实验室的设计、装备选型、系统集成、培训等工作,曾经指导建立各级电子数据司法鉴定数十个。

**田庆宜** 重庆市公安局公共信息网络安全监察总队,硕士,工程师,CISSP。重庆大学软件工程信息安全方向毕业。长期工作在电子取证分析工作领域,具有丰富的实验室建设经验。负责实验室技术路线设计和装备选型,所建设的重庆市公安局电子物证司法鉴定中心是公安部一级实验室。

**黄道丽** 信息安全公安部重点实验室(公安部第三研究所)助理研究员,上海辰星电子数据司法鉴定中心管理部负责人。主要研究信息安全、电子数据司法鉴定等。发表学术论文多篇。

**张鹏** 湖北警官学院电子取证重点实验室专职研究员,讲师,计算机国家司法鉴定人,华中科技大学硕士,主要研究方向为计算机犯罪侦查与取证,发表学术论文多篇。

**叶红** 国家信息中心电子数据司法鉴定中心常务副主任,北京市司法鉴

定协会理事,中国电子学会计算机取证专家委员会委员,高级工程师,国家科技进步一等奖获得者。长期从事信息安全、灾难恢复、网络应急救援,电子数据司法鉴定等方面的研究和服务工作,主持或参与完成了多部国家标准、行业规范的制定,具有丰富的理论知识和实践经验。

## 编写说明

“十二五”时期世情国情深刻变化,社会发展不断呈现新特征,随着信息技术与社会生产生活深度融合,一种社会需求广泛的崭新司法实践——电子数据司法鉴定迅速成为人们关注的热点。

电子数据司法鉴定是指在诉讼活动中,由具备相应资质的国家司法鉴定人运用计算机科学理论和技术,对诉讼中涉及的专门性问题进行鉴别判断,并提供鉴定意见的法律活动。通过电子数据司法鉴定可将电子数据证据转化为法定证据,实现法庭上的准确定案。目前电子数据司法鉴定已逐步成为赌博、诈骗、洗钱、贪污腐败、侵犯知识产权、黑客攻击、破坏国家安全等刑事案件,以及大量行政案件和民事案件量刑审判的关键依据,对于维护现实社会与虚拟社会的和谐发展发挥着不可替代的重要作用。同时,电子数据司法鉴定科学也是法学与计算机科学相结合的交叉学科、边缘学科和新兴学科,具有强烈的社会需求和鲜明的时代特征。

本书从电子数据司法鉴定的基本概念、司法制度、知识体系等基础内容入手,紧扣职业性、实用性和开放性三大原则,提炼出从案件委托受理、现场勘验、证据提取固定、分析判断,直到提交鉴定意见全过程的司法实践规范化流程与方法。按照常见委托事项分门别类,深入探讨了“用户行为、数据相似性、电子文档、数据电文、病毒及恶意代码、数据库、手机和网络数据”等多种司法活动中的实际问题,强调培养动手能力,着重解决现实难题。全书编写贴合司法教育培训系列教材大背景,对规范和指导司法鉴定实践活动具有较高参考价值,是深入贯彻落实科学发展观,做好当前社会矛盾化解、社会管理创新、公正廉洁执法三项重点工作,深化司法改革、扩大司法民主、推进司法公开的一项重要具体成果。

本书的作者来自该领域的各行各业,为全书高质量的完成付出了艰辛的劳动,在编撰过程中得到了各参编单位领导的大力支持,书中也参考引用了一些其他学者的研究成果,难免挂一漏万,敬请广大读者批评指正,以使本书臻于完善。

本书撰稿人的分工如下:

麦永浩 第一章、第十四章



|     |          |
|-----|----------|
| 戴士剑 | 第一章      |
| 刘品新 | 第二章      |
| 金 波 | 第三章      |
| 赵 庸 | 第四章      |
| 罗铂铀 | 第四章      |
| 陈 龙 | 第五章      |
| 陈建民 | 第六章      |
| 杜振华 | 第六章      |
| 沙 晶 | 第七章      |
| 向大为 | 第八章、第十四章 |
| 毛宪标 | 第九章      |
| 隆 波 | 第十章      |
| 史经纬 | 第十章      |
| 孙国梓 | 第十一章     |
| 王跃聪 | 第十二章     |
| 田庆宜 | 第十二章     |
| 黄道丽 | 第十三章     |
| 张 鹏 | 第十四章     |
| 叶 红 | 附 录      |

作 者

二〇一一年三月十六日

# 出版说明

## 一、编写目的

司法鉴定制度既是我国司法制度的组成部分,也是诉讼活动尤其是司法审判的重要保障。司法鉴定活动既不是行政行为,也不是司法行为,更不是一般的科学技术活动。司法鉴定具有法律性与科学性相统一的基本性质,有鉴于此,司法鉴定活动既是诉讼参与活动,又是科学技术实证活动,也可以说是科学技术与司法鉴定人的有机结合。因此,为了不断提高司法鉴定人的政治、业务素质和职业道德水平,统一规范司法鉴定人教育培训的要求和内容,促进司法鉴定队伍的可持续发展,保障鉴定质量,根据司法部颁布的《司法鉴定教育培训规定》,由司法部司法鉴定管理局自2007年起先后统一组织编写了司法鉴定教育培训系列教材。本系列教材第一批包括《司法鉴定通论》、《司法鉴定管理概论》、《司法鉴定工作手册》(已由中国政法大学出版社2008年出版)、《法医临床司法鉴定实务》、《法医病理司法鉴定实务》、《精神疾病司法鉴定实务》,已于2009年由法律出版社先后出版发行。第二批包括《法医物证司法鉴定实务》、《法医毒物司法鉴定实务》、《文书物证司法鉴定实务》、《痕迹物证司法鉴定实务》、《声像资料司法鉴定实务》和《电子数据司法鉴定实务》等六本教材,拟由法律出版社在2011年出版发行。

## 二、编写要求

为了保证系列教材编写质量,经司法部批准成立了“司法鉴定教育培训系列教材编委会”。编委会负责推荐各门教材主编及主审人选,审核确定主编推荐的编写人员及各部门教材的框架体系、编写内容和编写要求。本系列教材的编写工作汇集了全国法学界、法律界和鉴定业的同行专家、学者,参编人员不仅要具有较高的教材编写经验和教学经验,较好的文字表达和组织能力,专业知识深厚,了解学科前沿问题,熟悉本专业的新成就、新技术和新发展;同时还具有较丰富的司法鉴定执业经验,熟悉鉴定过程、技术、方法和仪器设备,充分了解各项鉴定实务职业岗位的任职要求。本系列教材编写要求主要有:一是职业性。本系列教材具有鲜明的职业性并以职业为导向。没有简单重复和系统介绍学科教育

阶段应该掌握的各专业的“三基”(基本原理、基本知识和基本制度规定),而是以培育和养成司法鉴定的职业素质、职业能力为主要目的。同时,还兼顾了新知识、新技能、新方法的补充完善与持续更新,实现了职业岗位培训与继续教育的有机结合和统一。二是实务性。根据司法鉴定职业岗位的要求,坚持以培育职业素质和提高鉴定能力为核心,充分满足从事鉴定实务的要求,具有较强的实践性和针对性。如在基本理论部分,贯彻“必需、够用”的原则;职业要求部分,根据“应知应会”的要求和本着“缺什么、补什么”的方针,包括实务知识、职业技能、鉴定方法、标准适用、案例评析和出庭应诉等内容;在能力方面,注重培养和提高专业能力、方法能力和应诉能力。三是开放性。教材在编写内容上充分体现开放性,不仅反映了当前司法鉴定执业活动中遇到的突出问题,而且在总结经验的基础上提出解决问题的办法和思路,推介了目前实践中常用的技术方法、技术标准和仪器设备,以及国内外研发推广的新仪器、新技术、新方法和发展趋势。不仅介绍了实践中常用的核心技术和常见的技术难点,而且还注重提高分析、解决问题的能力;不仅介绍了司法鉴定的管理制度和相关法律、法规,而且侧重介绍司法鉴定机构内部管理的规范要求和质量控制体系;不仅注重知识的传播和能力的训练,而且将职业道德的培育和养成贯穿于整个教育培训工作和执业活动的全过程;不仅介绍了司法鉴定行业通用的基础知识和技能,而且总结概括了各项鉴定实务特有的知识、技能和实践中的好经验、好方法。通过研究性学习和实践,实现教学相长、共同提高。

### 三、编写内容

本系列教材中各项鉴定实务主要由基本理论、实务知识、技术方法、执业规范、技能训练、评价要求和今后发展方向等内容组成。其要求:一是高度精练、概括准确,突出可操作性和实践性。二是结合司法鉴定实践中的常见问题,组织讨论和研究,注重训练和提高分析、解决问题的思路 and 办法。三是介绍本专业领域中的新问题、新要求和新成果,展望未来几年本专业可能的发展趋向,引导和促进学员深入思考,从整体上把握未来个人职业发展的目标定位,促其不断挖掘自身潜力,主动迎接新的职业挑战。

### 四、适用范围

司法鉴定的基本性质和基本要求决定了司法鉴定人不仅应当具有与所从事鉴定实务对口的专业知识,而且还必须具有相应的职业素养和执业技能;司法鉴定人执业的基本资质应当是专业知识、职业素养和执业技能的高度统一。有鉴于此:一是本系列教材的使用对象,不仅是已经接受过对口专业大学本科以上学历教育的司法鉴定人,而且也包括未接受过所从事鉴定业务对口专业本科以上

学历教育的(或未获得所从事鉴定业务高级技术职称,或未从事过十年以上该鉴定业务工作的)。当然,对于后者而言,首先应当按照司法部颁发的《关于开展法医临床司法鉴定人转岗培训工作的通知》(司发通〔2009〕95号)的要求接受转岗培训,然后再根据职业岗位的任职要求和发展需要,参加为提高职业素养和执业能力而进行的教育培训活动。二是本系列教材的适用范围,除已执业的司法鉴定人和拟申请执业的专业技术人员外,还包括高等院校中法学、法医等专业的在校学生,以及参与诉讼活动的法官、检察官、律师等相关专业人士。

司法鉴定教育培训系列教材编委会  
2011年3月

# 目 录

|                                 |        |
|---------------------------------|--------|
| 第一章 电子数据司法鉴定概论 .....            | ( 1 )  |
| 第一节 电子数据司法鉴定 .....              | ( 2 )  |
| 一、电子数据司法鉴定的基本概念 .....           | ( 2 )  |
| 二、电子数据司法鉴定的主要鉴定类别和适用范围 .....    | ( 4 )  |
| 三、电子数据司法鉴定各鉴定类别的鉴定事项和鉴定要求 ..... | ( 5 )  |
| 第二节 电子数据司法鉴定的基础和特点 .....        | ( 7 )  |
| 一、电子数据司法鉴定的法律基础 .....           | ( 8 )  |
| 二、电子数据司法鉴定的技术基础 .....           | ( 8 )  |
| 三、电子数据司法鉴定的特点 .....             | ( 9 )  |
| 第三节 电子数据司法鉴定的方案制定与体系结构 .....    | ( 10 ) |
| 一、电子数据司法鉴定的法律方案制定 .....         | ( 10 ) |
| 二、电子数据司法鉴定的技术方案制定 .....         | ( 12 ) |
| 三、电子数据司法鉴定计划的制定 .....           | ( 13 ) |
| 四、电子数据司法鉴定的工作环境和证据链监督 .....     | ( 13 ) |
| 五、电子数据司法鉴定的体系结构 .....           | ( 13 ) |
| 第四节 电子数据司法鉴定的要求 .....           | ( 14 ) |
| 一、电子数据司法鉴定的特殊执业规则和行业要求 .....    | ( 14 ) |
| 二、对电子数据司法鉴定意见的评价要求 .....        | ( 16 ) |
| 第五节 信息虚拟社会的法律责任制度 .....         | ( 17 ) |
| 一、刑事责任 .....                    | ( 17 ) |
| 二、行政责任 .....                    | ( 18 ) |
| 三、民事责任 .....                    | ( 19 ) |
| 第六节 电子数据司法鉴定的发展趋势及分析 .....      | ( 20 ) |
| 一、主机证据保全、恢复和分析技术 .....          | ( 20 ) |
| 二、网络数据取证与分析技术 .....             | ( 22 ) |
| 三、主动取证技术 .....                  | ( 23 ) |
| 四、电子数据证据法学研究 .....              | ( 24 ) |

|                                 |               |
|---------------------------------|---------------|
| 第七节 小结 .....                    | ( 24 )        |
| 思考题 .....                       | ( 25 )        |
| 参考文献 .....                      | ( 25 )        |
| <b>第二章 电子证据及相关鉴定的法律制度 .....</b> | <b>( 26 )</b> |
| 第一节 电子证据的法律地位 .....             | ( 26 )        |
| 一、对待电子证据的非歧视原则 .....            | ( 27 )        |
| 二、我国电子证据的混合定位法及其走向 .....        | ( 28 )        |
| 第二节 电子证据的可采性标准 .....            | ( 31 )        |
| 一、关联性标准 .....                   | ( 31 )        |
| 二、合法性标准 .....                   | ( 32 )        |
| 三、真实性标准 .....                   | ( 33 )        |
| 第三节 电子证据的证明力标准 .....            | ( 36 )        |
| 一、电子证据证明力的认定标准 .....            | ( 37 )        |
| 二、可靠性标准 .....                   | ( 38 )        |
| 三、完整性标准 .....                   | ( 39 )        |
| 四、电子证据的定案规则 .....               | ( 41 )        |
| 第四节 电子数据司法鉴定的法律制度 .....         | ( 42 )        |
| 一、电子数据司法鉴定的法律定位 .....           | ( 42 )        |
| 二、电子数据司法鉴定的法律原则 .....           | ( 43 )        |
| 第五节 小结 .....                    | ( 45 )        |
| 思考题 .....                       | ( 45 )        |
| 参考文献 .....                      | ( 45 )        |
| <b>第三章 电子数据司法鉴定基础 .....</b>     | <b>( 47 )</b> |
| 第一节 电子数据司法鉴定的基本原则 .....         | ( 47 )        |
| 一、电子证据的基本特征 .....               | ( 47 )        |
| 二、电子数据取证与鉴定的基本原则 .....          | ( 48 )        |
| 三、电子数据取证与鉴定的基本步骤 .....          | ( 48 )        |
| 第二节 电子数据司法鉴定技术知识体系 .....        | ( 50 )        |
| 一、知识体系的构成 .....                 | ( 50 )        |
| 二、数的机器表示 .....                  | ( 51 )        |
| 三、密码学基础 .....                   | ( 55 )        |
| 四、硬件技术 .....                    | ( 59 )        |
| 五、软件技术 .....                    | ( 61 )        |
| 六、计算机网络 .....                   | ( 64 )        |

|                             |         |
|-----------------------------|---------|
| 七、存储技术 .....                | ( 69 )  |
| 第三节 电子数据司法鉴定标准体系 .....      | ( 72 )  |
| 一、标准化的需求 .....              | ( 72 )  |
| 二、国内外标准化的情况 .....           | ( 73 )  |
| 三、标准体系的架构 .....             | ( 74 )  |
| 四、标准体系的构成 .....             | ( 76 )  |
| 第四节 小结 .....                | ( 76 )  |
| 思考题 .....                   | ( 76 )  |
| 参考文献 .....                  | ( 76 )  |
| 第四章 现场勘验与电子数据提取、固定 .....    | ( 78 )  |
| 第一节 电子数据现场勘验 .....          | ( 78 )  |
| 一、电子数据现场勘验的任务 .....         | ( 78 )  |
| 二、现场勘验规划与准备 .....           | ( 79 )  |
| 三、现场保护规划与准备 .....           | ( 83 )  |
| 四、现场电子数据处理 .....            | ( 83 )  |
| 第二节 电子数据提取、固定的方法 .....      | ( 92 )  |
| 一、使用硬盘复制机进行数据提取、固定 .....    | ( 93 )  |
| 二、使用只读锁 + 软件进行数据提取、固定 ..... | ( 95 )  |
| 三、现场数据固定应急方法 .....          | ( 98 )  |
| 四、电子数据提取、固定的后处理工作 .....     | ( 99 )  |
| 第三节 实验室中数据固定与检材管理 .....     | ( 99 )  |
| 一、检材接收 .....                | ( 100 ) |
| 二、检材预检 .....                | ( 102 ) |
| 三、检材备份 .....                | ( 104 ) |
| 四、检材存放 .....                | ( 105 ) |
| 五、检材流转 .....                | ( 106 ) |
| 六、检材清退 .....                | ( 106 ) |
| 七、备份检材清理 .....              | ( 107 ) |
| 第四节 小结 .....                | ( 107 ) |
| 思考题 .....                   | ( 107 ) |
| 参考文献 .....                  | ( 108 ) |
| 第五章 用户行为司法鉴定 .....          | ( 109 ) |
| 第一节 用户行为司法鉴定概述 .....        | ( 109 ) |
| 一、用户行为司法鉴定 .....            | ( 109 ) |

|                           |       |
|---------------------------|-------|
| 二、用户行为司法鉴定事项和鉴定要求 .....   | (110) |
| 第二节 用户行为司法鉴定技术 .....      | (120) |
| 一、用户身份确定技术 .....          | (120) |
| 二、文件系统分析 .....            | (120) |
| 三、日志分析 .....              | (122) |
| 四、注册表分析 .....             | (124) |
| 五、临时数据分析 .....            | (125) |
| 第三节 小结 .....              | (127) |
| 思考题 .....                 | (128) |
| 参考文献 .....                | (128) |
| 第六章 恶意程序司法鉴定 .....        | (129) |
| 第一节 恶意程序司法鉴定概述 .....      | (129) |
| 一、学习目的 .....              | (129) |
| 二、恶意程序的概念 .....           | (129) |
| 三、恶意程序的分类 .....           | (130) |
| 第二节 常用恶意程序司法鉴定工具介绍 .....  | (131) |
| 一、文件校验工具 .....            | (131) |
| 二、环境模拟工具 .....            | (132) |
| 三、行为分析工具 .....            | (134) |
| 四、动态代码分析工具 .....          | (138) |
| 五、静态代码分析工具 .....          | (140) |
| 第三节 恶意程序司法鉴定流程 .....      | (142) |
| 一、文件校验 .....              | (142) |
| 二、黑盒测试 .....              | (143) |
| 三、白盒测试 .....              | (143) |
| 第四节 恶意程序司法鉴定典型范例 .....    | (144) |
| 一、文件校验 .....              | (144) |
| 二、黑盒测试 .....              | (145) |
| 三、白盒测试 .....              | (152) |
| 第五节 小结 .....              | (153) |
| 思考题 .....                 | (154) |
| 参考文献 .....                | (154) |
| 第七章 电子文档与数据电文司法鉴定 .....   | (155) |
| 第一节 电子文档与数据电文司法鉴定综述 ..... | (155) |



|                             |       |
|-----------------------------|-------|
| 一、电子文档与数据电文的定义 .....        | (155) |
| 二、电子文档与数据电文的法律含义 .....      | (155) |
| 三、电子文档与数据电文司法鉴定的常见类型 .....  | (156) |
| 第二节 电子文档与数据电文司法鉴定技术 .....   | (156) |
| 一、基础知识 .....                | (156) |
| 二、证据获取 .....                | (163) |
| 三、证据分析 .....                | (173) |
| 四、常用工具介绍 .....              | (178) |
| 第三节 电子文档与数据电文司法鉴定展望 .....   | (180) |
| 一、国外现状 .....                | (180) |
| 二、技术展望及新类型案件 .....          | (180) |
| 第四节 电子文档与数据电文司法鉴定案例分析 ..... | (181) |
| 第五节 小结 .....                | (182) |
| 思考题 .....                   | (182) |
| 参考文献 .....                  | (182) |
| 第八章 数据库司法鉴定 .....           | (184) |
| 第一节 数据库司法鉴定的业务范围和主要任务 ..... | (184) |
| 一、数据库司法鉴定的业务范围 .....        | (184) |
| 二、数据库司法鉴定的主要任务和内容 .....     | (185) |
| 第二节 数据库司法鉴定关键技术 .....       | (193) |
| 一、常见关系型数据库系统基础操作 .....      | (193) |
| 二、数据库司法鉴定的主要技术 .....        | (200) |
| 第三节 小结 .....                | (208) |
| 思考题 .....                   | (208) |
| 参考文献 .....                  | (208) |
| 第九章 电子数据相似性司法鉴定 .....       | (209) |
| 第一节 电子数据相似性司法鉴定概述 .....     | (209) |
| 一、电子数据相似性司法鉴定的内容 .....      | (209) |
| 二、电子数据相似性司法鉴定方法与流程 .....    | (211) |
| 第二节 电子数据相似性司法鉴定技术 .....     | (212) |
| 一、电子数据相似性司法鉴定的基础知识 .....    | (212) |
| 二、电子数据相似性司法鉴定的关键技术 .....    | (215) |
| 第三节 电子数据相似性司法鉴定案例 .....     | (231) |
| 一、送检材料 .....                | (231) |