



华东政法学校庆六十周年纪念文丛

计算机司法 鉴定：理论探索

廖根为◎著

EAST CHINA UNIVERSITY OF POLITICAL SCIENCE AND LAW



法律出版社
LAW PRESS · CHINA

上海市教委重点学科建设项目 (J51102) 资助。

EAST CHINA UNIVERSITY OF POLITICAL SCIENCE AND LAW



华东政法大学校庆六十周年纪念文丛

计算机司法 鉴定：理论探索

廖根为◎著



法律出版社
LAW PRESS · CHINA

图书在版编目(CIP)数据

计算机司法鉴定:理论探索 / 廖根为著. —北京:
法律出版社, 2012. 7
(华东政法大学校庆六十周年纪念文丛)
ISBN 978 - 7 - 5118 - 3719 - 6

I. ①计… II. ①廖… III. ①计算机应用—司法鉴定
IV. ①D918.9 - 39

中国版本图书馆 CIP 数据核字(2012)第 152805 号

华东政法大学校庆
六十周年纪念文丛

计算机司法鉴定:理论探索

廖根为 著

责任编辑 黄琳佳

装帧设计  ilovee

© 法律出版社·中国

开本 A5

印张 11 字数 247 千

版本 2012 年 7 月第 1 版

印次 2012 年 7 月第 1 次印刷

出版 法律出版社

编辑统筹 学术·对外出版分社

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 陶松

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

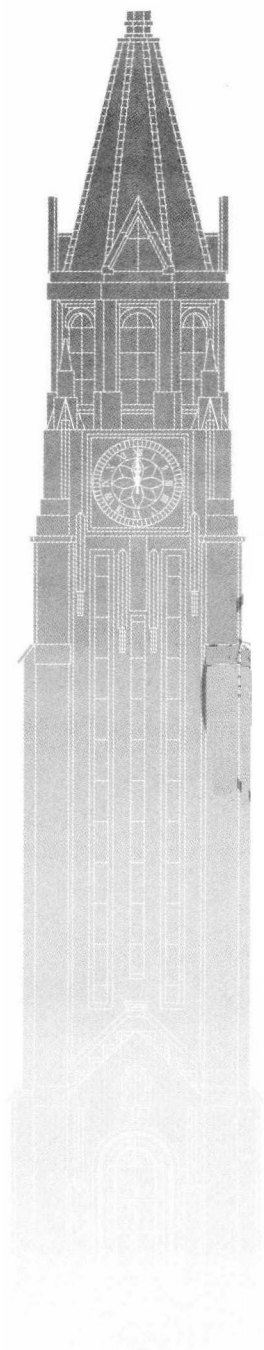
北京分公司/010-62534456

深圳公司/0755-83072995

书号:ISBN 978 - 7 - 5118 - 3719 - 6

定价:33.00 元

(如有缺页或倒装,中国法律图书有限公司负责退换)



编委会主任： 杜志淳 何勤华

编委会委员： 张智强 顾功耘 刘晓红

林燕萍 应培礼 马长山

王 迁 王立民 朱榄叶

刘宁元 刘宪权 牟道媛

杨正鸣 吴 弘 肖国兴

何 敏 何明升 邱格屏

沈贵明 沈济时 沈福俊

张明军 范玉吉 罗培新

金可可 唐 波 高富平

傅鼎生 童之伟



沉舟侧畔千帆过

——华东政法大学校庆六十周年纪念文丛总序

沧海桑田,情怀依旧。六十年来,在逆境中崛起,在忧患中奋进,在辉煌中卓越,一代又一代华政人,将华政精神传承。从长宁旧居赏月苏州河畔,到松江新校读书玉泊湖旁,今天,华东政法大学迎来了六十周年华诞!六十年,华政为国家、为社会培养了大量优秀的人才,而他们,已经成长为国家的栋梁和母校的骄傲。

忆往昔,桃李不言,自有风雨话沧桑。1952年6月,经华东军政委员会批准,华东政法学院(现华东政法大学)由原圣约翰大学、复旦大学、南京大学、东吴大学、厦门大学、沪江大学、安徽大学等9所院校的法律系(法律学院)、政治系和社会系等合并组建成立。其后由于历史原因,学校曾于1958年和1972年两度停办,1979年3月经国务院批准复校。2007年3月,经教育部批准,华东政法学院正式更名为华东政法大学,2012年系华东政法大学建校六十华诞。

自1952年从苏州河畔的这一片红墙绿瓦中走出

新中国第一批政法干部开始,六十年来,华政经历了三起两落的命运。昨日的历练成就了今日的辉煌,近十万毕业生勤勉工作,开拓进取,奋发向上,成为共和国法治建设及各项事业的骨干力量。复校以来,尤其是2003年于松江进行“二次创业”以后,华政在办学条件、办学规模、办学层次、队伍建设、学科建设、科学研究、服务社会等方面均取得了飞速发展。目前,学校设有长宁、松江两个校区,占地面积1300余亩,是“教育部依法治校示范校”、“国家语言文字规范化示范校”、“上海市文明单位”、“上海市市级建筑保护单位”、“上海市花园单位”。学校现设有16个学院(部),现拥有法学一级学科博士学位、硕士学位授予权,以及政治学、马克思主义理论、公共管理、应用经济学一级学科硕士学位授予权,建有10个博士点、25个硕士点、23个本科专业及法学博士后流动站。2002年、2008年两次教育部本科教学工作水平评估均被评为优秀。目前,学校法律史学科为国家级重点学科,法律史学、经济法学本科教学团队为国家级教学团队,外国法制史、中国法制史、经济法学、司法鉴定概论为国家级精品课程,法学综合实验教学中心为国家级实验教学示范中心,法学、侦查学为教育部高等学校特色专业建设点,“开放型国际法律人才培养模式创新实验区”为教育部建设项目。学校已被社会各界广泛赞誉为“法学教育的东方明珠”。

建校六十年来,华政披星戴月,风雨兼程,赢得桃李满天下,更在中国的法制现代化进程中,留下了浓墨重彩的一笔。华政的莘莘学子,肩负着建设法治社会的重任,同时也见证着母校各方面的长足发展。硬件方面,从“帐篷办学”到长宁校区的精致典雅,再到松江校区的恢宏大气且美仑美奂;软件方面,从实现华东地区法学博士点零的突破,到一举拿下法学一级学科博士点、获得非法学专业硕士学位授予权,再到填补上海市法学国家重点学科零的空白。2009年至2011年,学校国家社科基金法学类课题立项数连续三年名列全国第一,2011年又实现了国

家社科基金重大项目的历史性突破。2007年3月,华政更名大学的成功,标志着学校从此踏上了建设多科性大学的新的征程。

岁月悠悠,薪火相传,六十岁的华政犹如惊鸿一瞥。此番出版校庆六十周年纪念文丛,华政并未走“遍寻成功校友、为其寻章摘句并编撰成册”之路径,而想虚中求实,为青年教师提供出版著作、展示才华之契机。故而,入选本文丛的,绝大多数是尚未获得教授职称的青年学者。华政奖掖才俊、提携后学之美意,尽在其中矣!

值此华政建校六十周年之际,谨祝这颗法学教育的东方明珠更加光彩夺目!

华东政法大学校庆六十周年纪念文丛编委会

2012年6月

目 录

第一篇 计算机司法鉴定基本理论问题

第一章 计算机司法鉴定概述 003

第一节 计算机司法鉴定研究的基本范畴 003

一、计算机司法鉴定概念 003

二、计算机司法鉴定基本特点 010

三、计算机司法鉴定研究的基本范畴 013

第二节 计算机司法鉴定相关概念比较分析 017

一、计算机司法鉴定与计算机取证 017

二、计算机司法鉴定与电子数据司法鉴定 023

三、计算机司法鉴定与声像资料司法鉴定 025

四、计算机司法鉴定与司法会计鉴定 025

五、计算机司法鉴定与知识产权鉴定 026

第二章 计算机司法鉴定原则、程序和技术理论 027

第一节 计算机司法鉴定的基本原则 027

一、合法性原则 027

二、科学性原则	029
三、可重复可验证原则	032
四、及时性原则	032
五、公正性原则	032
六、独立性原则	033
七、规范性原则	033
第二节 计算机司法鉴定程序	034
一、计算机司法鉴定相关模型	034
二、计算机司法鉴定基本框架	037
三、计算机司法鉴定主要程序分析	039
第三节 计算机司法鉴定主要技术理论	052
一、软件相关技术理论	053
二、计算机网络技术理论	055
三、信息安全技术理论	056
四、数据存储相关技术理论	060

第三章 两种不同类别计算机司法鉴定分析 064

第一节 计算机司法鉴定分类	064
一、计算机司法鉴定分类现状	064
二、计算机司法鉴定学理分类	066
第二节 基于“证据发现”的计算机司法鉴定	070
一、基于“证据发现”计算机司法鉴定的特点	070
二、基于“证据发现”的计算机司法鉴定内容	075
三、基于“证据发现”的计算机司法鉴定思路	079
第三节 基于“证据评估”的计算机司法鉴定	081

一、基于“证据评估”的计算机司法鉴定的特点	081
二、基于“证据评估”的计算机司法鉴定的内容	083
三、基于“证据评估”的计算机司法鉴定的思路	089

第四章 计算机司法鉴定中所涉证据审查判断 093

第一节 计算机司法鉴定中所涉证据及其定位 093

一、计算机司法鉴定意见证据及其定位 094

二、数字证据及其定位 095

第二节 计算机司法鉴定意见证据的审查判断 109

一、鉴定意见证据关联性判断 109

二、鉴定意见证据合法性判断 112

三、鉴定意见证据客观性审查 117

第二节 计算机司法鉴定所涉数字证据的审查判断 120

一、数字证据关联性审查 120

二、数字证据合法性审查 123

三、数字证据真实性审查 127

第二篇 基于“证据发现”的计算机司法鉴定

第五章 数据内容分析 137

第一节 数据内容分析概述 137

一、数据内容分析简介 137

二、数据内容分析基本思路 140

三、数据内容分析常见工具 141

第二节 密码破解技术 146

一、密码破解常见方法 147

二、密码破解主要内容 148

第六章 数据恢复 152

第一节 数据恢复理论基础 152

一、数据恢复概述 152

二、数据恢复的基本思路 153

三、数据恢复的可靠性分析 166

第二节 常见文件系统的数据恢复 171

一、FAT 文件系统数据恢复方法 171

二、NTFS 文件系统数据恢复方法 175

第七章 数据检索与固定 180

第一节 数据检索技术 180

一、数据检索技术概述 180

二、数据检索的主要方法 181

第二节 数据提取与固定方法 190

一、数据提取和固定的常见方法 190

二、数据提取与固定的基本要求 191

第八章 数据来源分析 195

第一节 数据来源分析概述 195

一、数据来源分析概述 195

二、数据来源分析的主要方法 197

第二节 常见数据来源分析技术 199

- 一、IP 地址追踪 199
- 二、其他数据来源分析技术 207

第三篇 基于“证据评估”的计算机司法鉴定

第九章 真伪鉴定 211

第一节 电子邮件真伪鉴定 211

- 一、电子邮件原理 212
- 二、电子邮件的可靠性分析 215
- 三、电子邮件常见伪造手法 219
- 四、电子邮件真伪鉴定的基本思路 224

第二节 聊天记录真伪鉴定 234

- 一、聊天记录概述 234
- 二、聊天记录的可靠性分析 239
- 三、聊天记录真伪鉴定的基本思路 242

第三节 数字图像真伪鉴定 244

- 一、数字图像真伪鉴定概述 244
- 二、数字图像常见伪造手法 245
- 三、伪造数字图像的常见特征 246
- 四、数字图像真伪鉴定的主要方法 252

第十章 相似性鉴定 259

第一节 计算机软件相似性鉴定 259

- 一、计算机软件相似性鉴定概述 259
- 二、软件著作权侵权手法与行为认定 262

- 三、计算机软件相似性鉴定的基本思路 268
- 四、计算机软件相似性鉴定的可靠性分析 276
- 第二节 文件内容相似性鉴定 277
 - 一、文件内容相似性鉴定的主要类型 278
 - 二、文件内容相似鉴定的基本方法 279

第十一章 系统安全性评估 283

- 第一节 系统安全性评估概述 283
 - 一、信息安全管理 283
 - 二、系统安全性评估 288
 - 三、“系统安全性评估”的特殊性 288
- 第二节 系统安全性评估方法 290
 - 一、信息系统安全保护能力评估 290
 - 二、系统安全漏洞评估 292

第十二章 功能鉴定 296

- 第一节 恶意代码鉴定 296
 - 一、恶意代码概述 296
 - 二、恶意代码鉴定的基本思路 301
- 第二节 技术措施鉴定 310
 - 一、技术措施鉴定概述 311
 - 二、技术措施鉴定的基本思路 315

主要参考文献 318

第一篇 计算机司法鉴定基本理论问题

第一章

计算机司法鉴定概述

第一节 计算机司法鉴定研究的基本范畴

一、计算机司法鉴定概念

随着信息科学技术突飞猛进的发展,人类社会生产、生活发生着天翻地覆的巨大变化。在信息时代的今天,无论国家、社会组织、企业,还是个人都离不开计算机和国际互联网络,人们的工作、学习和生活都与数字化信息密切相关。与此同时,如果社会出现纠纷、产生冲突、发生犯罪,在纠纷解决或案件侦破过程中也可能涉及数字证据。当案件中需要对数字证据的真实性、关联性等问题进行审查时,离不开对它们进行技术分析和判断。这种分析判断实际上不是对案件法律问题而是事实问题进行审查。有时,这种技术性较强的案件事实审查单凭法官自身掌握的知识难以完成,此时便需要专业人员借助其掌握的计算机理论、技术和相关专业知识的这些事实问题进行专业判断、分析和鉴别。以上所涉及的技术是当前兴起的

法庭科学技术分支之一——计算机司法鉴定技术。

计算机司法鉴定是司法鉴定学(法庭科学技术)中一门新兴的子学科。近年来,计算机司法鉴定是司法鉴定学科的热点问题之一,在很多法庭科学国际会议上都被列为讨论的重点主题之一。然而,司法鉴定活动具有较强的法律和文化特征,它往往与一个国家实施的司法鉴定体制密切相关。我国司法鉴定不同于当事人主义诉讼模式的英美法系国家和职权主义诉讼模式的大陆法系国家的法庭科学,计算机司法鉴定也与其他国家所述的计算机法庭科学存在一定差异。

因此,研究什么是计算机司法鉴定,还应参考和依据我国司法鉴定学科中关于司法鉴定的研究成果。离开我国国情和司法鉴定体制,单纯地研究计算机司法鉴定是不全面的。因此,必须从理论、技术、法律等多个角度深入分析计算机司法鉴定是什么、可以做什么和怎样做等问题。

(一) 计算机司法鉴定概念分析

在《司法鉴定执业分类规定(试行)》中,“计算机司法鉴定”被列为执业类别的一种,而在《全国人民代表大会常务委员会关于司法鉴定管理问题的决定》等法律中并未将计算机司法鉴定纳入强制登记管理范围。但在司法鉴定实务中,常常将计算机司法鉴定作为声像资料类司法鉴定的一个分支,按照声像资料鉴定类予以管理。很多地区声像资料司法鉴定人同时也是计算机司法鉴定人。司法部司法鉴定管理局每年统计“三大类”司法鉴定案件时,也将其纳入到声像资料类中。

根据国家司法鉴定人和司法鉴定机构名册公告情况,2010年北京市从事计算机司法鉴定的机构(注:北京市司法鉴定执业业务没有单列计算机司法鉴定,其涵盖在声像资料鉴定中)有8家,上海市有9家,四川省有6家,重庆市有5家,辽宁省有5家,广东省有4家,湖北有4家,