公安院校
招录培养体制改革
试点专业
系列教材

计算机犯罪侦查方向

丛书主编 李锦

# 电子数据取证

刘浩阳 李锦 刘晓宇 主编
韩马剑 程霁 董健 翟晓飞 田庆宜 副主编

清华大学出版社

D924.36
38

公安院校招录培养体制改革试点专业系列教材

# 电子数据取证

刘浩阳 李锦 刘晓宇 主编

韩马剑 程霁 董健 翟晓飞 田庆宜 副主编

徐志强 陆道宏 郭永健 毕连城 赵方圆

段涵瑞 崔立成 刘建军 葛军 潘光诚 张鑫 胡武宏

清华大学出版社

北京

## 内 容 简 介

“从实战出发”是本书的编写基础；“学以致用”是本书的根本目标。本书按照电子数据取证的学习和实践规律，按照技术和法律并重的编写思路，将“实践”与“理论”完美地进行结合。

本书的主要内容包括 Windows、Mac OS、UNIX/Linux、移动终端、网络数据取证的基本知识和取证技术、电子数据取证的相关法律规则和标准，基本涵盖了电子数据取证的所有方面；同时以实战出发，对于电子数据现场勘验、鉴定和检验、实验室建设与认可等进行深入阐述，最后辅以真实案例，提出各种网络案件的取证思路和过程。目的是培养电子数据取证的能力。

本书作者均为国内具有丰富实战经验的专家和公安院校具有深厚理论知识的老师。本书内容为业内领先和成熟的知识和技术，涵盖了目前最领先的电子数据取证技术，力求传递给读者最新和最实用的技术和方法。

本书融合了电子数据取证理论和实践的最新成果，是一本理论扎实、操作性强的教材。本书适合作为高等院校信息安全、网络犯罪侦查、网络安全、侦查学等专业的研究生、本科生、双学位学生的授课教材或者参考书，也可以作为公安机关、检察机关、海关缉私等执法部门培训教材和网络安全从业人员的参考书。

**本书封面贴有清华大学出版社防伪标签，无标签者不得销售。**
**版权所有，侵权必究。侵权举报电话：010-62782989　13701121933**

**图书在版编目(CIP)数据**

电子数据取证/刘浩阳等主编. --北京：清华大学出版社，2015
公安院校招录培养体制改革试点专业系列教材
ISBN 978-7-302-41343-1

Ⅰ. ①电… Ⅱ. ①刘… Ⅲ. ①计算机犯罪－数据收集－中国－高等学校－教材 Ⅳ. ①D924.36

中国版本图书馆 CIP 数据核字(2015)第 209095 号

**责任编辑**：闫红梅　柴文强
**封面设计**：常雪影
**责任校对**：李建庄
**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×230mm　　**印　　张**：29　　**字　　数**：650 千字
**版　　次**：2015 年 11 月第 1 版　　**印　　次**：2015 年 11 月第1次印刷
**印　　数**：1～2000
**定　　价**：49.50 元

产品编号：062990-01

# 丛书序

期待已久的由李锦同志主编的《公安院校招录培养体制改革试点专业系列教材》终于出版了！该系列教材是我国第一套计算机犯罪侦查专业系列教材，它的出版解决了国内相关院校教师与学生急需的教科书问题，也为从事信息安全专业和侦查执法人员提供一套极有价值的参考丛书。这实属一件可喜可贺的事！

由于信息技术空前迅速的发展，极具挑战的计算机网络空间形成了一个变幻无穷的虚拟空间。现实社会中的犯罪越来越多地涉及计算机、手机等工具，各种数字技术与网络虚拟空间的交汇，使计算机犯罪侦查技术变得空前重要与紧迫。从20世纪90年代兴起的数字取证调查，涌现出各种各样的技术和工具，使得数字取证成为计算机专业的一门新兴学科。国际上的一些大学近年来已设置了专门的系和研究生学位的授予，为计算机犯罪侦查的教学内容增添了丰富而又精彩的情景。他山之石可以攻玉，许多技术和教材可以借鉴，但数字取证牵涉到法学、法规，各国的国情不尽相同，唯一的解决办法就是必须自主创新、撰写适合国内需要的相应教材。

面临这一劈山开路的挑战，本教材从专业的技术层面为国内的本科生尝试提供全面的教学培训，内容包括了从互联网体系结构原理到电子商务应用与各种法规，以及计算机网络攻防技术与信息系统安全等级保护与管理等基础知识，重点围绕着计算机犯罪调查的手段、工具与方法以及数据证据的分析与鉴定等基础知识；教材注重在传授理论知识的同时，强化面向实战能力的培训，全套教材既适应了学科特点又考虑到学生层次的具体情况，处处反映出作者们的精心思索。

本系列教材参编的作者全部来自辽宁警官高等专科学校的师资队伍，该校地处辽东半岛，面临蓝色的大海，大浪淘沙涌现一批时代的人杰。庄严整洁的校园具有公安教育突出的特色，更为可贵的是他们倡导教学、科研、警务实践紧密结合，不断创新教学模式的一贯校风，每年从那里培养出大量信息时代专业特色明显、创新能力强的人才队伍。本套系列教材的出版充分体现了该校的学术水平与精神面貌，尤其映射出参编作者们拥有第一线资深的教学经验和扎实的实际专业知识，以及始终保持一股奋发上进、开拓创新的风范。我在此由衷地对本教材的出版表示祝贺，并预祝他们再接再厉，取得更加辉煌的成功！

许榕生

2012-6 写于北京

# 本书序

随着网络犯罪活动的日益猖獗和不断升级，网络安全得到了国际和国内社会的高度关注。电子数据取证作为网络安全的重要组成部分，在获取犯罪证据、打击网络犯罪起到不可替代的作用。

人类从“神证”、“人证”时代到今天的“物证”时代，在信息化的大趋势下，未来将进入“电子数据”的时代。电子数据已经在新刑诉法和民诉法中明确作为证据类型之一，是新的“证据之王”。电子数据取证在公安、海关、工商等执法部门已经成为重要的专业技术；高校、学术团体也在积极开展电子数据取证的相关研究。电子数据取证工作涉及领域广泛、技术标准严格，对于电子数据取证人员的学科背景和专业技能提出了较高要求。为了适应形势的挑战，迫切需要加强电子数据取证人才的培养，以维护网络环境的稳定和经济社会的发展。

本书将“实践”与“理论”完美地进行结合，主要有以下特点：

**1. 知识体系完整、结构合理**

本书遵循电子数据取证的学习和实践规律，按照技术和法律并重的编写思路。从网络安全和网络犯罪的基本概念和形势出发；阐述有关电子数据取证相关的法律和法规；介绍了包括 Windows、Mac OS、UNIX/Linux、移动终端的基本知识和取证技术，涵盖了电子数据取证的所有方面；同时以实际出发，重点讲述现场勘验、鉴定和检验实验室建设与认可，最后辅以真实案例，提出各种网络案件的取证思路和过程，目的是培养电子数据取证的能力。

**2. 实用性强、具有很强的操作性**

本书追求“真实”呈现电子数据取证的技术和方法。力求将深奥和复杂的电子数据取证知识以通俗易懂的语言、简洁明了的结构，深入浅出地阐述出来。同时要求整体内容具有“可复现”性，通过讲解技术内幕，辅以工具使用，能够重现取证过程和结果。力求做到理论与实践相结合。

**3. 技术领先、内容深入、引导未来的发展方向**

本书的内容为业内领先和成熟的技术，抛弃过时的技术和方法，力求不“误人子弟”。业内的电子数据取证专家将丰富的实战经验和技术呈现在教材中，力求传递给读者最新和最实用的技术和方法。针对难点问题，例如电子数据鉴定和检验、实验室建设和认可，都做了最权威的阐述。同时对于电子数据取证的未来发展趋势，也做了前瞻性的展望。

试读结束，需要全本PDF请购买 www.ertongbook.com

本书主要由执法行业的专家和公安院校的学者共同完成。通读本书，能够感觉他们在繁重的工作之余，潜下心来，本着为读者负责的态度认真撰写，将多年的技术和经验奉献在本教材中，实属不易！在此，我由衷地对本教材的顺利出版表示祝贺，并预祝他们再接再厉，取得更加辉煌的成功。

许剑卓

2015 年 5 月 30 日

# 前言

近年来，随着我国网络安全的需要，电子数据取证在我国得到了较快的发展，某些领域已经与世界水平比肩。电子数据取证在打击网络犯罪、营造网络良好安全环境起到不可或缺的作用。电子数据取证是一个相对“小众”的行业。也是一个高度依赖“个人能力”的工作，对从业人员的知识体系和经验要求极高。可以说，电子数据取证人员是网络安全行业中的佼佼者。

我很荣幸能够赶上这个时代。我从事网络安全工作十四年，将最美好的青春奉献给了这个事业，并为之自豪。在这里，我学到的不仅是电子数据取证技术，而且将法律作为信仰，将职业作为理想，更遇到了一批与我拥有共同梦想的优秀人才。

早在 2007 年，我就曾经与辽宁省警察学院的米佳校长联合出版过专著《计算机取证技术》，是国内首批电子数据取证专业教材之一。但是，技术的前进如此迅速以至于那本书的内容经受着实践的严峻考验，很多以前不可能取证的数据现在会变得易如反掌，而当时成熟的取证方法会因为技术的进步而变得过时。电子数据取证对象，已经从 Windows 操作系统扩展到包含 Windows、Mac OS、UNIX/Linux、移动终端甚至定制操作系统的数据；从简单的文件过滤、搜索深入到密码破解、数据挖掘和元数据分析等具有相当深度的层面。无论是“广度”还是“深度”，电子数据取证已经成为网络安全行业中要求较高的学科。电子数据取证相关人才的缺乏和网络安全行业的迫切需要形成了矛盾。因此，如果能将国内顶尖的电子数据取证的专家、学者聚集起来，按照各自专长写出一部理论与实践充分结合的教材，培养出更多的优秀人才，可以极大地缓解我国网络安全行业的迫切需要。

本书是一部“诚意之作”，也是一部“实力之作”。对于参与本书的诸位作者来说，将自己的技术和经验传授给大家，与在第一线同犯罪分子进行斗争一样有意义。本书由国内多位专家、学者编写，他们分布于公安、检察、行业公司，在技术方面是行业的领头人。诸位作者毫无保留地将宝贵的技术和经验奉献给本书，涵盖了电子数据取证的所有方面，每个数据都进行了详细考证，列举的工具均为具有实战意义的工具、使用的案例均为具有代表性的真实案例。因此，本书代表了电子数据取证的最新技术和未来发展趋势。

对于网络犯罪侦查或电子数据取证，由于信息系统的复杂性，每一个案(事)件都是独一无二的，侦查、取证人员都必须从实际出发来制定相应的处置方法。但是本书并不是一部百

科全书，也不是操作手册，不能完全解决所有的问题或者建立一个万能的规则，而是技术与经验结合之谈。目的是帮助电子数据取证人员建立自己的取证原则、技术和流程。希望读者通过本书能够深入学习电子数据取证，如果能够举一反三，成为此行业的“大牛”，那更是我们作者的荣幸。

本书的特点不是简单的理论堆积和令人厌烦的说教，而是第一次全面地完整呈现取证的知识体系；第一次深入地讲解取证的技术原理；第一次从法律规则角度出发，将法律与技术紧密融合。本书最终的目的为“源于实战、高于实战、引导实战”。

本书由刘浩阳、李锦、刘晓宇主编，韩马剑、程霁、董健、翟晓飞、田庆宜副主编。徐志强、陆道宏、郭永健、毕连城、赵方圆、段涵瑞等为编者。作者信息如下：

主编：刘浩阳，男，研究生学历，大连市公安局网络安全保卫支队七大队大队长、大连市公安局电子物证检验鉴定实验室主任、公安部网络侦查专家、全国刑事技术标准化技术委员会电子物证分技术委员会专家、中国合格评定国家委员会评审员、辽宁省警察学院客座老师、大连市五一劳动奖章获得者。出版专著《计算机取证技术》；公安院校本科统编教材《电子数据检验技术与应用》副主编、《电子数据勘查取证与鉴定（数据恢复与取证）》副主编、撰写论文10余篇；拥有国家专利一项。

主编：李锦，女，辽宁警察学院公安信息系主任，硕士，教授，二级警监，入选“辽宁省百千万人才工程千人层次”、大连市“三育人”先进个人。主持参与省部级教科研项目十余项，市厅及项目十余项，撰写论文10余篇，其中多篇论文被EI收录。主要研究方向：网络安全与计算机犯罪侦查。

主编：刘晓宇，男，公安部网络安全保卫局研发中心勘查取证处处长、全国刑事技术标准技术委员会电子物证分技术委员会专家组组长、中国合格评定国家认可委员会信息技术专业委员会委员。电子数据取证技术实战化发展的引领者，主持了公安机关网安部门计算机、手机、分布式等一系列取证技术和系统的研究与开发，组织起草制定了一系列的电子数据取证相关技术标准，指导并参与了全国公安机关网络安全部门一系列重、大、要案的侦查与电子数据勘查取证工作。

副主编：韩马剑，男，河北省公安厅网络安全保卫总队电子数据鉴定支队支队长，公安部网络侦查专家。从事电子数据取证工作10余年，在网络案件侦查和电子数据取证工作方面具有较深的造诣，侦办了多起重大黑客攻击、网络赌博、网络淫秽色情案件。

副主编：程霁，男，工学、法学双学士。安徽省公安厅电子数据鉴定实验室技术负责人，公安部网络侦查专家。《电子数据勘查取证与鉴定(电子证据搜索)》副主编。

副主编：董健，男，副研究员，毕业于中国人民公安大学。国内首届计算机物证专业硕士、博士，公安部网络侦查专家，信息网络安全公安部重点实验室专家。现任职于公安部第三研究所、公安部网络技术研发中心、信息网络安全公安部重点实验室、国家反计算机入侵和防病毒研究中心，曾任山东省公安厅网络案件侦查支队长，从事网络案件侦查、电子证据勘验鉴定、网络安全科研工作十余年，参与国家“十二五”、“十三五”相关科研项目，承担公安部重点和国家级科研课题多项。

副主编：翟晓飞，男，公安部网络侦查专家，公安部网络安全保卫局电子数据取证实验室技术负责人、授权签字人，中国合格评定国家认可委员会评审员，具有丰富电子数据取证工作经验，曾参加多起具有国际影响力和国内重特大案件的侦办工作，多次参加电子数据有关司法解释、法律法规的制定工作，主持修订公安机关电子数据取证有关规章。

副主编：田庆宜，男，高级工程师，公安部网络侦查专家、全国刑事技术标准化技术委员会电子物证分技术委员会专家、重庆市“反恐专家”，参与编写多个取证相关技术标准及专著2部，领衔负责各级科研项目20余项，参加一系列重特大案件，多次立功受奖，具有丰富的实战经验。

编者：徐志强，男，美亚柏科企业电子数据取证事业部总经理，兼任美亚柏科技术专家委员会首席技术专家，拥有近10年电子数据取证从业经验。江西警察学院计算机犯罪研究中心特聘研究员、福建省公共网络信息安全协会专家组专家、中国刑警学院客座讲师。拥有多年电子数据取证教学及案件调查经验，带领团队创立国内首个电子数据取证调查员(MCE)培训及认证体系。主编《电子证据提取与分析》、《数据恢复与取证》、《手机取证技术》《信息加解密技术》。

编者：陆道宏，男，上海弘连网络科技有限公司总经理，国内第一代电子数据取证从业者。开发了一系列电子数据取证专用工具，在介质、手机、服务器和网络取证等众多领域具有深入的研究，电子数据司法鉴定人。

编者：郭永健，男，香港资讯保安及法证公会(ISFS)中国大区联络官，国际高科技犯罪调查协会(HTCIA)亚太区分会中国联络官，中国电子学会计算机取证专家、委员会委员，中国政法大学法务会计研究中心客座研究员。CCFC计算机法证技术峰会的发起人，中国计算机取证技术的国际交流和发展的积极推动者。

编者：毕连城，男，大连市人民检察院技术处副处长、全国检察机关“信息技术专家”。主持2项大连市科研立项，发表省级、国家级论文10余篇。

编者：赵方圆，女，在读博士研究生，潍坊市公安局网安支队四大队大队长，公安部网络安全专家，山东省公安厅电子数据取证省队队员，潍坊市警官培训基地兼职教官。主持参与多项科研项目，其中获山东省公安机关科技进步二等奖一项，入选公安部应用创新计划一项。

编者：段涵瑞，男，新疆维吾尔自治区公安厅网络安全保卫总队案件侦查队队长。高级工程师、公安部网络侦查专家、全国刑事技术标准化委员会电子物证检验分技术委员会委员。参与了一系列电子物证检验规范的制定工作。工作17年来直接参与了一批大要案的侦查取证和检验鉴定工作，为侦查破案提供了确实有效的证据。撰写的多篇论文发表在《中国刑事警察》等国家级和省部级刊物上。

编者：崔立成，男，讲师，博士研究生，辽宁警察学院公安信息系从事电子取证研究与教学工作。

编者：刘建军，男，硕士，工程师，南京市公安局网络安全保卫支队副大队长，侦办多起重特大涉网案件，荣获全国公安机关优秀专业技术人才奖。

试读结束，需要全本PDF请购买 www.ertongbook.com

编者：葛军，男，就职于安徽天达网络科技有限公司。“灰鸽子”远程控制软件的作者。现致力于网络安全事业，主要研究恶意程序代码的取证。

编者：潘光诚，男，山东省公安厅网安总队五支队支队长、电子数据检验鉴定中心质量主管、公安部网络侦查专家、CNAS 授权签字人。曾获山东省科技进步二等奖一项，山东省公安机关科技进步二等奖二项，三等奖二项。承担公安机关科技攻关 2 项。多次组织指导全省重特大案件侦破及取证工作。

编者：张鑫，男，国家计算机病毒应急处理中心应急部部长，硕士，高级工程师，公安部网络安全专家组专家。从事网络安全恶意代码分析工作 10 余年，协助破获“熊猫烧香”等重大网络犯罪案件 20 余起，出具各类分析鉴定报告 30 余份，参予多项省部科研项目和行业标准，撰写论文 10 余篇。

编者：胡武宏，男，1997 年毕业于中国人民警官大学，2006 年获得复旦大学软件工程硕士(MSE)学位。现就职于安徽省公安厅电子数据鉴定中心。

其中，主编刘浩阳负责全书的架构设计和内容统编，并编写了第 1 章、第 2 章中的第 2.11.1、2.11.2、2.13 节、第 3 章、第 4 章、第 5 章、第 6 章中的第 6.1、6.2.1、6.2.2、6.2.3、6.2.4、6.8、6.9、6.13、6.14 节、第 7 章、第 8 章、第 9 章、第 10 章、第 11 章；李锦编写了第 2 章中的第 2.14 节、第 6 章中的第 6.7 节；刘晓宇编写了第 1 章；韩马剑编写了第 2 章中的第 2.6、2.12 节、第 6 章中的第 6.11、6.12 节；程霁编写了第 6 章中的第 6.2.8、6.6 节；董健编写了第 7 章；翟晓飞编写了第 7 章；田庆宜编写了第 3 章；徐志强编写了第 2 章中的第 2.9 节、第 6 章中的第 6.2.2、6.4 节；陆道宏编写了第 2 章中的第 2.11.3、

2.11.4 节、第 6 章中的第 6.2.6、6.2.7、6.4 节；郭永健编写了第 6 章中的第 6.3 节；毕连城编写了第 4 章；赵方圆编写了第 2 章中的第 2.6～2.8、2.10 节、第 11 章中的第 11.2、11.3 节；段涵瑞编写了第 7 章；崔立成编写了第 2 章中的 2.1～2.4 节；刘建军编写了第 11 章中的第 11.1、11.6 节；葛军编写了第 6 章中的第 6.10 节；潘光诚编写了第 4 章；张鑫编写了第 11 章中的第 11.4 节；胡武宏编写了第 2 章中的第 2.5 节。

本书不包含任何涉密内容，使用的工具均为商业版或者开源免费版本。

行文仓促，不免有纰漏之处，欢迎读者提出宝贵意见，请发到 dzsjqz@163.com 邮箱。

感谢辽宁省警察学院信息安全系李锦主任和公安部十一局研发中心刘晓宇处长的帮助指导、感谢帮助我们成长的各位家人、领导和战友。感谢公安部十一局、大连市公安局、河北省公安厅、安徽省公安厅等多地部门和中国合格评定国家认可委员会的支持。感谢郭弘、黄道丽、唐丹舟、王彦斌、胡海洋老师为此书提出的宝贵意见。感谢诸位专家学者提供的宝贵资料和意见，能够使得本书得以顺利出版。

谨以此书纪念我最亲爱的妈妈！

刘浩阳

2015 年 5 月 10 日

# 目录

试读结束，需要全本PDF请购买 www.ertongbook.com