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

网络犯罪侦查

刘浩阳 编著

清华大学出版社

公安院校招录培养体制改革试点专业系列教材

网络犯罪侦查

刘浩阳 编著

清华大学出版社
北 京

内 容 简 介

网络犯罪侦查集法律、谋略和实践于一体，具有相当的知识广度和深度。本书按照网络犯罪侦查的学习和实践规律，按照法律、谋略和技术并重的编写思路，将网络犯罪侦查的实践与理论完美结合。

“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。本书的主要内容包括网络犯罪和网络犯罪侦查的历史和理论，网络犯罪的法律规制，网络犯罪侦查的程序、谋略、技术和取证，提出各类网络犯罪案件的侦查思路和方法。全方位地展现了网络犯罪侦查的知识体系。

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。本书内容涵盖了目前最新的网络安全法律法规、先进的网络犯罪侦查技术和经典案例，力求传递给读者最新和最实用的技术和方法。

本书融合了网络犯罪侦查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和参考书；也可以作为公安机关、检察机关、海关缉私等侦查部门的培训教材和参考书。

图书在版编目(CIP)数据

网络犯罪侦查/刘浩阳编著. —北京：清华大学出版社，2016
(公安院校招录培养体制改革试点专业系列教材)
ISBN 978-7-302-44971-3

Ⅰ. ①网… Ⅱ. ①刘… Ⅲ. ①互联网络－计算机犯罪－刑事侦查－高等学校－教材 Ⅳ. ①D918

中国版本图书馆 CIP 数据核字(2016)第 214157 号

责任编辑：闫红梅　李　晔
封面设计：常雪影
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 装 者：三河市金元印装有限公司
经　　销：全国新华书店
开　　本：185mm×230mm　　**印　　张**：38.25　　**字　　数**：832 千字
版　　次：2016 年 11 月第 1 版　　**印　　次**：2016 年 11 月第1 次印刷
印　　数：1～1500
定　　价：79.00 元

产品编号：062989-01

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！

许耀生

2012年6月于北京

前言

网络空间的无限扩展在给予人类便利的同时，也为犯罪提供了滋生的土壤。一方面，网络犯罪借助技术的发展更加隐蔽，变化形式多样，没有规律可循，给侦查取证带来了严峻的挑战。另一方面，习惯了传统侦破方法的侦查不能及时变换思路，工作方式和技术已经过时，侦查机关的人员业务素质和技能都无法适应现实斗争的需要。网络犯罪的快速蔓延与执法部门的应对乏力形成了巨大的反差。

要改变这一切，首先要认识到我们国家的执法部门整体上侦查能力落后于时代的要求。侦查机关的侦查技术、侦查理念都远滞后于时代要求。对于网络犯罪的打击仍然关注“抓人”而非“证据”，重视“结果”而非“过程”，盲目地相信技术侦查措施，强调“走捷径”。这将无法跟上飞速变化的网络社会发展需要。

解决问题的核心，一是改变网络犯罪的现有侦查机制。打击网络犯罪不仅是“网警”一个部门，而是公安机关乃至所有执法部门共同的责任与目标；二是提高网络犯罪侦查能力。网络犯罪法律知识和侦查技术是每个执法者必备并能熟练运用的技能。执法者需要在认识计算机网络的特点和趋势的基础上，将法律和技术加以有效的运用，建立符合实际需求的侦查机制，形成高效率的侦查体系，才能从容应对网络犯罪的变化。

目前，学术界研究对于网络犯罪给予了更多的关注和思考。但是由于所处地位和关注角度的不同，更多地集中在刑法学和证据学角度，与一线实战存在脱节，无法形成指引实战的侦查机制。而广大网络安全执法人员认为，网络犯罪侦查主要依赖技术侦查措施，对此讳莫如深，长此以往，导致网络侦查知识无法普及，难以提高网络安全侦查技术和技能。

2005 年，笔者编写出版了电子数据取证的专著——《计算机取证技术》；2015 年，又出版了《电子数据取证》。从一个理想青年成长为一名网络安全保卫战线的执法者，十年破茧成蝶。看到很多的执法者面对网络犯罪侦查的无计可施，笔者决定编写《网络犯罪侦查》。这对于笔者来说，不仅是研究领域的扩展，更是水到渠成。

网络犯罪侦查涉及多门学科和业务方向。本书的编写集中了全国网络犯罪侦查的顶尖专家学者，他们工作于网络安全保卫的各条战线，具有丰富的侦查经验和高超的侦查技术。各位作者都是网络犯罪侦查领域的佼佼者，他们能够无偿地奉献出自己独到的知识和丰富经验，体现出无私的胸怀。将实践中积累的知识和经验跃然纸上，不仅是对个人能力的一种肯定，而且是整个侦查体系的传承和升华，更是侦查机关与教育机构联系的纽带。

本书从侦查的角度出发，紧密结合实践，对网络犯罪侦查的各个方面进行了全方位的解读。本书在法律方面邀请网络犯罪侦查法律的制定者参与编写，技术方面集中了网络犯罪侦查的前沿技术；案例方面根据典型的案件类型，从技术和谋略角度，做了详尽的阐述。尽管如此，本书不是“葵花宝典”，读者不会从中得到侦查秘籍，而且由于网络的飞速发展使得本书不可能预见未来的网络犯罪。本书的目的是给予读者从事网络犯罪侦查的相关知识和技术，从而形成符合自己工作需要的侦查谋略。

本书的作者团队介绍如下：

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、中国电子学会计算机取证专家委员会委员、辽宁省警察学院客座老师、公安部优秀专业技术人才一等奖获得者、大连市五一劳动奖章获得者。出版专著《计算机取证技术》；公安院校招录培养体制改革试点专业系列教材《电子数据取证》主编、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，撰写论文十余篇；拥有国家专利一项。

副主编：董健，男，副研究员。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10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：张宏大，男。沈阳市公安局网络安全保卫支队案件大队大队长，沈阳市劳动模范，中国刑警学院客座讲师，多次在全省网警侦查培训班、全省警督培训班授课。组建了沈阳市公安局电子物证鉴定中心、沈阳市反信息诈骗中心。成功侦破公安部督办网络案件10余起，荣立个人一等功1次，个人二等功5次。

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，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》副主编，多次参加网络犯罪、电子数据等相关司法解释的制定工作。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、网络传销、网络诈骗等案件。

副主编：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。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》编者。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，直接参与了一批大要案的侦查取证和检验鉴定工作。

副主编：侯钧雷，男，理学学士、工程硕士。公安部网络安全保卫局副处长，主要从事网络犯罪案件侦查、电子数据取证以及相关法律法规制订工作。先后参与起草了危害计算机信息系统安全刑事解释、办理网络犯罪案件适用刑事诉讼程序相关意见以及公安机关电子数据取证规则等文件。

副主编：张鑫，男，硕士。国家计算机病毒应急处理中心应急部部长，高级工程师，公安部网络安全专家组专家。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》编者。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，参与多项省部科研项目和行业标准，撰写论文10余篇。

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。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》副主编；《电子数据勘查取证与鉴定（电子证据搜索）》副主编。

编者：童瀛，男。江苏省公安厅网络安全保卫总队支队长，公安部网络侦查专家、追逃专家，江苏省“333高级人才”。盐城团市“十大杰出青年”“新长征突击手标兵”。3次获得二等功。《童瀛信息化工作法》获“首届江苏省公安机关科技创新奖项”。

编者：喻海松，男，法学学士、硕士、博士。留学德国马普外国刑法暨国际刑法研究所。现任最高人民法院研究室法官，主要从事刑事司法解释起草和参与立法机关有关刑事立法工作。先后参与起草了危害计算机信息系统安全刑事解释、刑事诉讼法解释等多部司法解释和网络犯罪刑事诉讼程序意见等多部规范性文件。出版专著《刑法的扩张——刑法修正案（九）及新近刑法立法解释司法适用解读》。

编者：卢睿，女，工学博士。辽宁警察学院公安信息系副教授。“辽宁省高等学校杰出青年学者成长计划”入选者。近年来主持和参与了公安部软科学、辽宁省教育厅重点实验室、大连市社会科学独立研究等多个项目的研究，发表核心期刊论文10余篇，其中9篇被Ei检索。

编者：刘洋洋，女，工学硕士。辽宁警察学院公安信息系计算机犯罪侦查教研室主任，副教授，现从事网络犯罪侦查及电子数据取证相关教学及研究工作。主持和参与公安部软科学、辽宁省公安厅软科学、大连市社会科学等多类项目研究，发表专业相关论文多篇。

编者：李小恺，男，法学博士，美国加州大学戴维斯分校访问学者。现为中国政法大学刑事司法学院侦查学研究所讲师，主要研究证据法、物证技术和司法鉴定。在《法学杂志》《证据科学》《中国司法》《西北大学学报》等期刊以及“证据科学国际研讨会”等学术会议上发表论文10余篇，出版专著《证据法视野下的谎言》，参与《中华人民共和国刑事诉讼法释义及适用指南》《司法鉴定质量控制法律制度研究》等多部专著的编写和翻译，主持及参与多项科研项目。

编者：刘煜杰，男，硕士学位。南京市公安局网络安全保卫支队第九大队副大队长。荣获江苏省公安厅“全省公安机关执法示范岗位”，南京市公安局“网安和科技标兵”“石城百名杰出青年卫士”称号；先后荣获个人三等功4次。先后参与、指挥数十起大要案件侦破

工作。

编者：李锋，男，硕士。工作于江苏省公安厅网络安全保卫总队案件查处科，负责网络犯罪案件查处和电子数据取证工作，牵头侦破了10余起公安部督办特大网络犯罪案件，实战经验丰富。

编者：刘琨，男。成都市公安局网络安全保卫支队七大队大队长，公安部网络侦查专家。曾获四川省科技进步三等奖1项、四川省公安厅科技进步二等奖1项、四川省基层技术革新奖三等奖1项。参与多起大要案的侦办工作，多次立功受奖。

编者：吕毅，男。大连市公安局网络安全保卫支队电子物证检验鉴定实验室副主任，质量负责人。参与多起大案要案的侦办工作，实战经验丰富。

本书的编写工作分工如下：刘浩阳负责全书的架构设计和内容统校，韩马剑、张宏大、董健、段涵瑞对本书进行了认真细致的校审。其中，刘浩阳编写了第1章、第2章、7.1节、7.2节、7.4节、7.7节、7.8节、7.12节、第9章；董健编写了第15章、第16章；张宏大编写了第5章；韩马剑编写了7.9节、第8章；段涵瑞编写了第6章；侯钧雷编写了第3章；张鑫编写了7.11节、第14章；程霁编写了7.5节、7.6节、第10章；童瀛编写了7.10节、第11章；喻海松编写了第3章；卢睿编写了4.5～4.9节；刘洋洋编写了4.1～4.4节；李小恺编写了第3章；刘煜杰编写了7.2节、7.4节、第13章；李锋编写了第12章；刘琨编写了7.2节、7.3节；吕毅编写了第17章。

网络犯罪侦查涉及的方面多，技术发展日新月异。与《电子数据取证》一书深耕10年相比，本书的广度和深度远超前者，作者团队在工作之余笔耕不辍，十易其稿，耗时一年，但仍感觉远不能全面、深入地展现网络犯罪侦查的全部知识，更难免有纰漏之处。在此，诚挚欢迎读者提出宝贵意见，意见请发送到 wlfzzc2016@163.com。

感谢公安部网络安全保卫局、大连市公安局、沈阳市公安局、河北省公安厅、新疆维吾尔自治区公安厅、天津市公安局、安徽省公安厅、公安部第三研究所等部门对本书的支持；感谢帮助我们成长的各位家人、领导和战友；感谢诸位专家学者为此书提供的宝贵资料和意见、建议。

本书不包含任何涉密内容，使用的技术均为公开技术，使用的案例均为公开或脱密案例，使用的工具均为商业版或者开源免费版本。

谨以此书向恪守职责，为网络安全献出汗水、青春，乃至生命的公安机关网络安全保卫部门的干警以及其他侦查机关的执法者致敬！

谨以此书献给最亲爱的爸爸！

刘浩阳

2016年3月23日

目录