中国刑事警察学院
教材建设专项资助项目

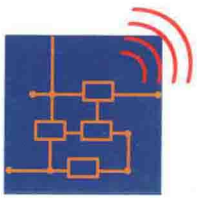
当代世界警务理论与侦查实务译丛
丛书主编　王世全　马玉生

CYBER FORENSICS

From Data to Digital Evidence

网络取证

从数据到电子证据



[美]阿尔伯特·J. 马塞拉 Albert J. Marcella, JR.
[美]弗雷德里克·吉罗索 Frederic Guillossou　著

高洪涛　等译

中国人民公安大学出版社

中国刑事警察学院
教材建设专项资助项目

当代世界警务理论与侦查实务译丛
丛书主编　王世全　马玉生

CYBER FORENSICS

From Data to Digital Evidence

网络取证

从数据到电子证据

[美] 阿尔伯特·J. 马塞拉　Albert J.Marcella,JR.

[美] 弗雷德里克·吉罗索　Frederic Guillossou　著

高洪涛　等译

中国人民公安大学出版社
·北　京·

图书在版编目（CIP）数据

网络取证：从数据到电子证据/［美］马塞拉，［美］吉罗索著；高洪涛等译. —北京：中国人民公安大学出版社，2015.6
（当代世界警务理论与侦查实务译丛）
ISBN 978-7-5653-2069-9
Ⅰ. ①网… Ⅱ. ①马… ②吉… ③高… Ⅲ. ①计算机网络—应用—证据—调查—研究Ⅳ. ①D915.13-39

中国版本图书馆 CIP 数据核字（2014）第 256968 号

本书版权登记号：图字：01-2014-7850

网络取证：从数据到电子证据

［美］阿尔伯特·J. 马塞拉 Albert J.Marcella,JR.
［美］弗雷德里克·吉罗索 Frederic Guillossou 著
高洪涛 等译

出版发行：中国人民公安大学出版社
地　　址：北京市西城区木樨地南里
邮政编码：100038
经　　销：新华书店
印　　刷：北京通天印刷有限责任公司

版　　次：2015 年 6 月第 1 版
印　　次：2015 年 6 月第 1 次
印　　张：19.75
开　　本：787 毫米×1092 毫米　1/16
字　　数：360 千字

书　　号：ISBN 978-7-5653-2069-9
定　　价：85.00 元

网　　址：www.cppsup.com.cn　www.porclub.com.cn
电子邮箱：zbs@cppsup.com　zbs@cppsu.edu.cn

营销中心电话：010-83903254
读者服务部电话（门市）：010-83903257
警官读者俱乐部电话（网购、邮购）：010-83903253
教材分社电话：010-83903259

网络取证：从数据到电子证据

译者名单

高洪涛　李子川　赵广晔　高　杨

序 一

习近平总书记在2014年中央外事工作会议上强调："认识世界发展大势，跟上时代潮流，是一个极为重要并且常做常新的课题。中国要发展，必须顺应世界发展潮流。要树立世界眼光、把握时代脉搏，要把当今世界的风云变幻看准、看清、看透，从林林总总的表象中发现本质，尤其要认清长远趋势。"2015年中央政法工作会议明确提出，要深入学习贯彻党的十八届四中全会精神，全面推进依法治国，推动政法工作向善于运用法治思维和法治方式转变、向着力解决深层次问题转变、向善于运用信息化手段转变、向更加开放转变。可以看到，开放、发展、合作的观念正在深刻影响着当代中国和中国的法治建设。

警察作为人类社会发展到一定阶段所共有的社会现象，既有一定的历史延续，也存在着国与国之间的横向联系。近二百年来，随着五次警务革命的潮起潮落，西方国家的警察科学研究日趋繁荣，学术成果硕果累累，形成了较为先进、完善的警察科学理论体系与操作模式。尽管西方国家与我国的社会制度、国情、治安状况不同，但是其百余年的警务革命和实践对我国警务工作的发展不无启示。作为人才培养的主阵地和科教强警的生力军，公安教育战线更应树立世界眼光，积极借鉴世界警

务理论发展成果，切实加强对事关公安工作全局性、前瞻性、规律性重大问题的研究，不断丰富具有中国特色的现代警务理论，努力为解决在警务实践中遇到的新情况、新问题提供有力支持。

为深入了解和借鉴国外先进的警务理论研究成果，推动现代警务理论研究和实践创新，更好地服务公安教育和公安实战，中国刑事警察学院组织开展了“当代世界警务理论与侦查实务译丛”的翻译出版工作。本译丛包括12本译著（其中英文版著作10种、德文版著作1种、俄文版著作1种），具有以下特点：一是原著作者普遍具有较高的研究水平和学术影响力。他们中有的是学术造诣精深的学者，有的是警务实战经验丰富的专家，其成果代表了相关专业领域的最新进展以及发展趋势，权威性强，学术水平高。二是在警务理论研究学派的选择上具有广泛性和代表性，包括了英美法系国家、大陆法系国家以及其他具有独特法律传统的国家等多个具有代表性的流派。本译丛内容的广泛性有助于全面客观地认识和借鉴具有代表性的国家在警务工作中的共性特色和个性魅力。三是具有很强的警务理论研究和实用价值。本译丛包括警务工作的诸多领域，涉及警务与执法、全球缉毒、刑事侦查、网络犯罪侦查、鞋印证据、实用爆炸现场调查、司法语言学、犯罪与恐怖主义、犯罪现场摄影技术等专业科技领域。这些成果贴近警务工作实际，对警务理论研究和实战应用具有重要的借鉴价值和指导意义。

“当代世界警务理论与侦查实务译丛”的付梓是中国刑事警察学院教材建设的重大推进，凝聚了有关方面和专家学者的辛勤付出，不仅填补了公安学和公安技术两个一级学科专业译著的空白，也为我国公安教

育训练工作、警务理论研究和公安实战应用带来了新理念和新方法。作为一名在公安教育战线工作了30多年的“老兵”，我很高兴为本译丛作序。冀望“当代世界警务理论与侦查实务译丛”的面世能够激发越来越多的公安院校和学者对世界警学名著引进与翻译的热情，能够对公安学和公安技术的学术研究有所推动，为公安工作和公安队伍建设提供更加有力的理论支持和智力保障。

是为序。

中国刑事警察学院党委书记、院长 王世全
2015年5月

序二

由中国刑事警察学院编译的“当代世界警务理论与侦查实务译丛”即将出版，邀我作序，我很高兴。中国刑事警察学院与我渊源极深，1960年至1962年期间，我曾经在民警干校任教，也就是中国刑事警察学院的前身。

近日收到书稿，认真阅读了这部译丛，不禁生出许多感慨，既被书中原著很多的新理念所触动，又感动于编译者的辛苦付出，于是迫不及待地拿起笔，翻出一些记忆，写下一些感受。

这部译丛收录的原著，大多是关注现场或者证据的，贴近实战，非常受用。这倒十分符合我从事刑事侦查工作多年的经验和认知。国内也好，国外也罢，关于刑事侦查的很多理念和实践往往是趋同的。记得2005年，我这个所谓“中国的福尔摩斯”和有“当代福尔摩斯”之称的美籍华裔专家李昌钰博士在中央电视台同做一档节目，我们的人生经历不同，遇到的案件不同，但我们对犯罪现场的重视和刑侦现场证据理论的推崇却高度一致。每到一个案件现场我常说的一句话是“现场，现场，还是现场，现场是破案的源泉”，我参与侦办的如“马加爵案”、“5·7”空难、“彭妙计案”等一系列重大要案的关键线索，无一例外

都源于对犯罪现场的缜密分析。

曾有人说，我有所谓的“超能力”，所以才能找到犯罪分子的蛛丝马迹，这当然是一句笑谈，如果说要找到一个途径去获得这所谓的“超能力”，我想那就是要坚持不断地学习。当今世界，国际合作日渐紧密，科技发展日新月异，刑事犯罪侦查也正面临着越来越大的挑战，只有经验是不够的，更不可能闷头过日子，必须要学习世界最前沿的科学理念，掌握最先进的侦查方法和技术，我们才能始终保持优势、先发制敌，让犯罪无处遁形。

本译丛严格地讲是一套教材，读者更多应该是有志于从事刑事侦查工作的同志，笔尖停留之处，我更想对你们说点什么，就算于书内容不妥，我想也算得题中之义。如何做一名合格的刑事侦查工作者，除了技术，除了学习，究竟还需要点什么？我想应该是对事业的忠诚，还有对生命的敬畏吧。每一件大案结案之际，我都不会有太多的轻松和愉悦，因为刑事侦查是以罪恶发生和人民群众生命财产安全被侵害为起点，那么结局就注定不会有什么完美可言。我们刑侦人所能做到的，就是尽早地发现真相，尽早地还世界一份清宁。真心地希望你们用心体味生命，热爱生活，做一个有血有肉、侠骨柔肠的神探。

“风雨多经人不老，关山初度路犹长。”本译丛的编译工作是在中国刑事警察学院65周年华诞之际启动的，65年栉风沐雨，65年薪火传承，中国刑事警察学院这所中国刑警的最高学府已桃李天下、硕果累累，作为老校友，我倍感骄傲和欣慰，同时感谢中国刑事警察学院领导和各位同仁多年来的关心和帮助。衷心希望中国刑事警察学院在这项工

作中有更多的新成果面世！祝愿中国刑事警察学院在建设国际一流刑警院校的新征程中取得新的更大的成绩！

是为序。

公安部首席特邀刑侦专家 乌国庆

2015 年 5 月

译者说明

随着计算机技术的迅速发展和计算机网络的广泛普及，越来越多的人开始使用网络进行工作和交流，网络已经成为人们生活中不可或缺的一部分。因此，网络调查取证在各类案件的侦查和举证中所起的作用也越来越大，也越来越受到办案人员的重视。在我国2012年新修订的《刑事诉讼法》中，电子证据正式作为法定证据种类之一。同时，新《刑事诉讼法》第187条第3款规定，“公诉人、当事人或者辩护人、诉讼代理人对鉴定意见有异议，人民法院认为鉴定人有必要出庭的，鉴定人应当出庭作证。经人民法院通知，鉴定人拒不出庭作证的，鉴定意见不得作为定案的根据。”这就要求司法鉴定人员不仅要有良好的取证鉴定能力，而且还要具备应对法庭质询的能力。换句话说，司法鉴定人员不仅要能够从计算机和网络设备中获得线索或证据，还需要对调查取证的原理和过程有深入的理解。

本书以一起侵犯知识产权案的调查取证过程为线索，详细地介绍了将原始的二进制数据一步一步转化成证据的原理和方法。作者还以时间的不一致性为例，说明网络取证调查人员除需要具备扎实的理论基础外，在调查中还应具有怀疑和探究精神，只有这样，才能成功应对庭审质证。同时，作者在书中还提出了一种明智的取证调查策略，可以作为网络取证调查人员进行取证调查时的行动参考。

本书的作者阿尔伯特·J. 马塞拉和弗雷德里克·吉罗索都是信息安全领域的资深专家。马塞拉博士在信息技术、安全和内部控制评估领域拥有超过34年的工作经验。吉罗索先生有超过8年的信息安全领域工作经验。他们都拥有网络侦查取证领域的丰富实践经验，而本书正是他们这些宝贵经验的结晶。因此，对于网络调查取证人员来说，这是一本不可多得的参考手册。

本书主要由中国刑事警察学院高洪涛、李子川、赵广晔、高杨翻译。李子川负责翻译第1章至第4章及第11章；高洪涛负责翻译第5章至第9章，其中高杨负责翻译第9章附录；赵广晔负责翻译第10章、第12章、第13章，以及

引言、致谢、目录、书后附录部分、作者等。译者力求反映原书的特点和风貌，为网络调查取证人员和相关从业人员提供帮助。但由于时间关系及水平所限，不当和疏漏之处在所难免，敬请广大读者批评指正。

2014 年 10 月

作 者

阿尔伯特·J. 马塞拉，国际信息系统审计师（Certified Information Systems Auditor，CISA），注册信息安全员（Certified Information Security Member，CISM），是商业自动化顾问有限责任公司（Business Automation Consultants，BAC）总裁。这是一家全球化的信息技术和管理顾问公司，为国际客户提供信息技术（IT）管理顾问，以及信息技术审计和安全的评估及培训。

马塞拉博士是一位国际知名的公众演说家、研究人员、作者、研修班和研讨会负责人，在信息技术审计、安全和内部控制评估领域有超过34年的工作经验。著有与信息技术、审计和安全相关内容的多篇文章和26本书籍。马塞拉博士的作品曾被刊登在ISACA期刊、灾难恢复期刊、取证和调查会计学期刊、EDPACS平台、ISSA期刊、应用商务搜索期刊和内部审计师杂志上。

马塞拉博士是国际内部审计师协会2000年度Leon R. Radde教育者奖的获得者。他曾为国际内部审计师协会（Institute of Internall Auditors，IIA）的信息技术审计研修班课程授课，还为国际信息系统审计协会（Information Systems Audit and Control Association，ISACA）讲授了多门与信息技术和信息技术审计相关的课程。

弗雷德里克·吉罗索，注册信息系统安全师（Certified Information Systems Security Professional，CISSP），CMS认证工程师（CMS Certified Engineer，CCE），拥有在信息安全领域超过8年的工作经验，包括私人业务和公司业务。他的安全领域经验包括应急处置、数字取证、项目管理、网络安全、互联网协议群（Internet Protocol Suite，IPS）管理和反恶意软件。

吉罗索先生大部分工作都是为一个财务机构的信息安全领域工作，这就使得他熟知各种监管标准，如PCI、ISO 27001、NIST、SOX和SEC。他与内部和外部法律顾问、反欺诈调查员、人力资源部门和审计师合作密切。

在他的职业生涯中，吉罗索先生调查过侵犯知识产权案、劳动力资源及人力资源问题，并参与过其他内部调查。

引言

网络取证调查人员的角色和职责是准确地描述数据的识别、提取和分析的专业过程，这些数据最终会被作为嫌疑人从事未经授权活动的证据。

作为专业人士，如果网络取证调查人员过度地依赖取证软件工具自动生成的结果，却不了解这些结果的具体产生过程，那么他不仅是在用他的职业声誉冒险，更是在用调查成功的可能性冒险。

众所周知，构成信息的原始素材——数据，最开始只是作为表示电荷是否存在的电脉冲出现的。了解这些电脉冲最终是如何成为数据的，以及这些数据又是如何成为潜在的证据的，是网络取证调查人员的必备能力。

从比特和字节演化成数据，并最终演化为人们可以理解的文本并不是很复杂的过程；有些技术是比较复杂的，但是不至于影响从专业角度进一步了解如何将数据转换为电子证据，面对数亿字节的数据从哪里寻找埋藏在其中的证据，以及何种特定数据可以引导调查人员发现所谓的“铁证”。

在陈述网络取证调查结果的过程中，如果没有深入地了解某个计算机取证工具是如何得出结果的，却企图以使用该取证工具来回避“你是如何通过检验出的数据得出结论的”这个问题，从专业角度说是十分危险的。

依赖软件来获得答案，却没有对“如何”、“什么”、“为什么”这些获得答案过程背后的原理和逻辑的深入理解，有点像在数学考试中只写出了正确结果却没有通过考试，因为你并没有展示你做了什么。知道答案，却不知道怎样得到答案或者解释答案是如何得到的，并不等于拥有了问题的解决方案。

本书将为读者提供在综合网络取证调查中，如何使用特定的知识对数据的真实性进行识别、访问并加以分析。

本书在解释了数据的起源和发展之后，从数据单位比特和字节入手，进一步说明寻址的概念与数据存储、引导记录、分区、卷和文件系统等相关概念，以及在网络取证过程中它们是如何联系在一起的。最终得出调查人员在案件调查中扮演的角色，以及是如何在上述区域中认定这些电子证据的。

同时，本书还论述了两个经常被忽视的问题：字节序和时间。每个主题自成一章，深入讨论分析结构，并说明了它们对于电子证据的最终鉴定结果会产生怎样的影响。

为了更有效地引入信息技术和网络取证的概念以及讨论关键网络取证过程，此书介绍了约瑟·麦卡锡涉嫌参与的侵犯知识产权案。以罗娜尔调查活动作为背景，在前12章中，为学习网络取证设计了具体应用实例。我们围绕这个案例撰写了一份取证调查报告样例（取证调查，ABC公司）作为本书的附录。这份样例报告为读者提供了一个基础的取证报告模板，按照提交给相应的授权收件人的形式编制了取证调查过程和案件数据的总结。

虽然每个调查是独一无二的，但是它们都会有相似之处，而且每个案例的独特性只在于其本身。鉴于此，本书构造了一个泛化的明智的调查策略，叫作ISPs，以此来帮助调查人员磨炼和发展自身的调查经验。虽然这种调查策略并不是每个案件的最佳实施方法，但它却是最灵活和聪明的办案步骤、过程或者行为，因此它适用于大多数的网络调查取证情况。

试图找到一个调查过程或方法并声称它是普遍的，而且可以被应用在一切情况下，虽然这听起来可能有点不合逻辑，但是本书中提到的明智的调查策略是以大面积撒网的形式进行覆盖，以使其适用于大多数调查案件的。读者可以在该方法的基础上进行扩充，通过添加特定的专业公司、部门或机构规定的步骤和程序，来形成独特的具体调查过程。

无论你对于通过自己努力调查或使用专用或通用的电子取证软件得到的数据多么有信心，请牢记那句俄罗斯谚语“поверяй, но проверяй”，也就是罗纳德·里根总统的口头禅：“信任，但要核查！”

本书将为读者提供一个全面科学的网络取证调查体系，并且揭示在调查幕后数据发生了什么以及如何寻找到这些数据……即从数据到电子证据。

阿尔伯特·J. 马塞拉和弗雷德里克·吉罗索

目 录

CONTENTS