工商网络交易监管及电子数据证据取证培训教材

国家工商总局网络商品交易监管司

电子数据检查及证据固定

系列丛书

中国工商出版社

电子数据检查及证据固定

国家工商总局网络商品交易监管司　编

中国工商出版社

责任编辑/李轶群　张丽娟
封面设计/慧　子

图书在版编目(CIP)数据

电子数据检查及证据固定 / 国家工商总局网络商品交易监管司编. —北京:中国工商出版社,2014.11
ISBN 978-7-80215-754-5

Ⅰ.①电… Ⅱ.①国… Ⅲ.①计算机犯罪—数据收集—研究—中国
Ⅳ.①D924.364

中国版本图书馆 CIP 数据核字(2014)第 257565 号

书名/电子数据检查及证据固定
编者/国家工商总局网络商品交易监管司

出版·发行/中国工商出版社
经销/新华书店
印刷/北京海纳百川印刷有限公司
开本/680 毫米×960 毫米　1/16　**印张**/17.375　**字数**/260 千
版本/2014 年 12 月第 1 版　2014 年 12 月第 1 次印刷

社址/北京市丰台区花乡育芳园东里 23 号(100070)
电话/(010)63730074,63725178　**电子邮箱**/zggscbs@163.com

书号:ISBN 978-7-80215-754-5/D·475
定价:39.00 元

编委名单

主　编：刘红亮　国家工商总局网络商品交易监管司司长

副主编：杨洪丰　国家工商总局网络商品交易监管司副司长

王应涛　福建省工商局副局长

编　委：刘宝恒　国家工商总局网络商品交易监管司网络商品交易规范处处长

吴东平　国家工商总局网络商品交易监管司网络商品交易监管处处长

夏　超　国家工商总局网络商品交易监管司网络商品交易规范处干部

翟　泳　国家工商总局网络商品交易监管司网络商品交易规范处干部

余　华　福建省工商局市场处副处长

肖湘华　福建省工商局市场处主任科员

王粟洋　福建省工商局市场处科员

卿斯汉　中国科学院知识创新工程项目首席科学家，北京大学、武汉大学客座教授、博士生导师

许榕生　中国电子学会计算机取证专家委员会副主任委员，中科院高能物理所计算网络安全实验室首席科学家

丁丽萍　中科院软件所基础软件国家工程研究中心研究员，中国电子学会计算机取证专家委员会秘书长

秦玉海　东北大学博士生副导师，专业技术二级警监

王永全　华东政法大学刑事司法学院副院长兼信息系主任，中国电子学会计算机取证专家委员会委员
马国富　中央司法警官学院信息系实验中心副主任
马　丁　中国人民公安大学信息安全工程系副主任、教授、理学博士
孙国梓　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
陈　龙　重庆邮电大学教授、博士，CAAI 智能数字内容安全专委会委员，国际期刊 IJCS 编委
陈垂聪　厦门市美亚柏科信息股份有限公司副总经理
林远近　厦门市美亚柏科信息股份有限公司培训中心技术部经理
蔡菲娜　厦门市美亚柏科信息股份有限公司培训中心培训部讲师
王　菲　厦门市美亚柏科信息股份有限公司培训中心技术部讲师

序 言

近年来，网络商品交易以其成本低、覆盖面广、使用灵活、易于参与等优势得到了广大消费者的认可和青睐，成为人们日常生活中的重要消费方式，在释放消费需求、拉动经济增长、扩大社会就业、转变经济发展方式等方面发挥了重要作用。但与此同时，由于网络的虚拟性、开放性、跨地域性的特点，网络市场在发展过程中也出现了一些不容忽视的问题，制假售假、不正当竞争、虚假宣传、网络传销等违法行为时有发生。这些问题影响了网络市场环境，扰乱了网络经济秩序，成为阻碍网络市场健康持续发展的重大瓶颈。加强网络交易监管，维护网络交易正常秩序，保障网络交易安全和消费者合法权益，是工商机关在网络时代肩负的神圣使命和重要职责。

网络商品交易通过电子数据传递信息，网络商品交易及相关服务的全过程也以电子数据的形式来记录和保存。虚拟的电子数据具有分散性、隐匿性、易被篡改的特点，电子证据通常具有外在实体上的无形性、表现形式的多样性和易灭失破坏性。因此，收集固定网络交易的电子数据证据，是网络交易监管执法的重要前提。如何科学规范地收集、固定电子数据证据并确保其证据效力，成为工商机关切实履行网络交易监管职责时不可回避的重大课题。

国家工商总局于2011年专门下发了《关于工商行政管理机关电子数据证据取证工作的指导意见》（工商市字[2011]248号），对电子证据的定义、取证原则、取证方式、取证程序，以及询问笔录和检查查封的具体要求作出了规定。但基层工商机关在电子取证执法实践中仍然面临电子证据提取手段匮乏、办案人员技术水平有待提高等诸多困难，在办理网络案

件时难以在第一时间提取和固定网络违法证据，经常陷入“看得到”却“拿不到”，甚至因法律无法认定而导致证据失效，让违法者逍遥法外的窘境。

为进一步加大电子数据证据取证相关业务知识的普及和培训力度，增强并规范工商行政管理机关电子数据证据取证工作，国家工商总局网络商品交易监管司组织编写了工商网络交易监管及电子数据证据取证培训系列教材。系列教材由《网络交易规范和监管》、《电子数据检查及证据固定》、《电子数据取证分析技术》、《移动互联网及手机取证技术》组成，系统介绍了网络商品交易监管特别是电子数据取证工作的理论背景、法律依据与实践经验，为各级工商网监机构开展业务培训提供了有益范本。以系列教材的出版为契机，大力开展网络商品交易监管业务培训，打造一支熟练掌握相关法律法规、信息网络技术、工商行政管理实践经验的工商网络交易监管复合型人才队伍，将会有力地提升工商机关网监队伍的履职能力和监管效能，实现从传统实地市场巡查模式向利用现代信息技术“以网管网”的转变，以更加规范有力的网络商品交易监管执法工作，为中国网络市场健康持续发展保驾护航。

甘霖

2014 年 10 月

前 言

工商行政管理机关在实施网络监管和对经营者利用互联网或计算机实施违法行为进行查处时，常常会遇到调查取证难以下手的问题，如违法经营主体在工商部门展开调查时，立即删改网络违法信息，并对其前期违法行为予以否认，使得执法人员无从取证其违法事实；又如部分违法经营者利用网络虚标身份及经营地，使执法人员难以对其进行落地定位，等等。电子取证难直接影响到网络交易监管的成效，影响工商网络监管执法的权威。甚至有些涉网案件由于取证不当导致错罚，不仅损害了行政相对人的合法权益，也使得工商执法机关在行政诉讼和行政复议中处于不利地位。因此，电子数据取证的重要性在工商行政执法中的作用日趋显现，作为执法人员应该掌握更专业、更全面的电子数据取证技术，为日常的执法提供更加有利的帮助。

与传统的取证对象不同的是，电子数据更加难以提取，表现为易丢失、易损坏、易被篡改、数据分散及格式繁多等，电子数据的这些特点给执法取证带来了很大麻烦。计算机硬盘、U 盘、手机等设备中所存储的电子数据，往往会遇到存储介质被损坏、数据被删除等情况，因此必须通过电子数据取证技术进行恢复、提取和分析，从而客观、真实地反映存储介质中的电子数据记录。电子数据取证应当严格遵守国家法律、法规、规章的有关规定，除与案件有关联的电子数据外，不得随意复制、泄露案件当事人储存在计算机系统中的私人材料和商业秘密。为规范工商行政管理机关电子数据取证工作，加强网络交易违法行为查处工作，本书主要从以下几个方面阐述电子数据检查及证据固定。

1. 电子证据检查对象：介绍常见个人计算机和服务器设备的各种形态、存储介质及取证检查过程中需要重点关注的软件和文件；重点掌握作为取证对象的常见软件与文件所包含证据的检查要点。

2. 电子数据取证技术装备：在电子数据检查取证过程中，可能会用到各种取证硬件设备和相关软件工具，这取决于不同类型的案件、不同的现场情况。在前期准备阶段，应充分考虑现场可能出现的情况，携带尽可能完备的装备前往。

3. 现场检查取证：现场检查取证一般的流程主要包括前期准备、现场保护、收集相关证物、电子数据载体处理、证据保全、填写清单、证物封存及提存笔录，在本书中将详细介绍每个步骤的操作规范及注意事项。

4. 远程检查：以案例的形式展示了针对利用互联网进行违法经营活动的取证，如通过某些网络交易网站进行高仿、伪劣商品销售，从而侵害广大消费者权益的违法经营行为。同时还介绍了如何通过远程检查取证的方式对涉案对象进行处理、如何把经营者发布在互联网上的违法信息进行存证等。

5. 证据保全技术：从常规电子证据保全方法、电子证据复制技术、电子证据镜像技术、电子证据校验技术、电子证据公证与互联网保全技术等方面介绍如何将电子证据固定并妥善保管，以便作为涉案证据使用。

总之，电子数据取证已日益成为人们研究与关注的焦点，如何获取与案件相关的电子证据，将违法分子绳之以法，已成为司法和计算机科学领域中研究的重要课题。近年来，电子数据取证在工商执法中的应用越来越广泛，部分单位建立起统一的电子数据取证实验室，电子数据取证的重要性在工商网络市场监管和行政执法中的作用日趋显现，作为执法人员应该掌握更专业、更全面的电子数据取证技术，为日常的监管执法提供更加有利的帮助。

目 录

第1章 电子数据取证概述

本章学习目标：

1. 熟悉电子数据法律法规；
2. 掌握电子证据类型、特点及基本原则。

1.1 电子数据检查法律依据

如何确保收集到的电子数据证据真实、有效，是电子数据检查工作的关键，也是目前电子数据取证要解决的主要问题。为了适应新形势的发展，世界各国纷纷加快了相关法律法规的制定和完善工作。我国也在电子商务监管方面做出了相关规定。

1.1.1 国内相关的法律法规

电子数据取证是一项集技术和法律要求于一身的特殊工作。对于取证程序规范的研究和制定需要从技术和法律双层面进行探索，这对计算机和法学领域的专家和学者提出了新的挑战，目前我国对于电子数据取证程序还未制定统一的标准。

《最高人民法院关于行政证据的若干问题的规定》第12条规定："当事人向人民法院提供计算机数据或者录音、录像等视听资料的，应当符合以下要求：提供有关资料的原始载体。提供原始载体确实有困难的，可以提供复制件，并注明制作方法、制作时间、制作人和证明对象等。声音资料应当附有该声音内容的文字记录。"

《最高人民法院关于民事诉讼证据的若干规定》第22条规定："调查人员调查收集计算机数据或者录音、录像等资料的，应当要求被调查人提供有关资料的原始载体。提供原始载体确有困难的，可以提供复制件。提供复

制件的,调查人员应当在调查笔录中说明来源和制作经过。”

《刑事诉讼法》修改稿给视听材料的定义:以录音、录像、电子计算机以及其他高科技设备所存储的信息证明案件真实情况的证据。

2013 年 1 月 1 日起正式实施的修订稿《刑事诉讼法》第五章第四十八条明确规定:可以用于证明案件事实的材料,都是证据。

证据包括:

(一)物证;

(二)书证;

(三)证人证言;

(四)被害人陈述;

(五)涉嫌违法当事人、被告人供述和辩解;

(六)鉴定意见;

(七)勘验、检查、辨认、侦查实验等笔录;

(八)视听资料、电子数据。

1.1.2 工商行政执法电子取证相关规定

《网络交易管理办法》(第 60 号令)

《关于工商行政管理机关电子数据证据取证工作的指导意见》(工商市字[2011]248 号)

1.1.3 国外常见的法律法规

《网络犯罪公约》(Cyber - crime Convention)

是于 2001 年 11 月由欧洲理事会的 26 个欧盟成员国以及美国、加拿大、日本和南非等 30 个国家的政府官员在布达佩斯共同签署的国际公约,它是全世界第一部针对网络犯罪活动所制定的国际公约。《网络犯罪公约》制定的目的之一是期望国际间对于网络犯罪的立法有共同一致的参考标准,同时在进行网络犯罪侦查时有共同遵守的国际公约予以支持,进而实现有效的国际合作。

《网络犯罪公约》除序言外,全文分为四章,共计 48 个条文。序言是说明《网络犯罪公约》的功能、目标;第一章为术语的使用,即对网络犯罪涉及的术语进行名词定义,其中包括电脑系统(computer system)、电脑资料(com-

puter data)、服务提供者(service provider)与电信资料(traffic data)等都有明确定义;第二章为国家层面上的措施,包括刑事实体法、刑事程序法和管辖权三个部分,要求各签约国于各自国内应采取的措施,且在程序法部分规定了有关电子证据调查的特殊程序法制度,而值得注意的是在规范非法撷取(Illegal access)的行为方面,《网络犯罪公约》要求各国应立法明定非法撷取为犯罪行为并应予处罚;第三章为国际合作,包括一般原则和特殊规定两个部分,在一般原则中包含规范引渡及相互合作等相关问题,而特殊规定则是有关电脑证据取得的问题,签约国应建立一周七天且一天二十四小时皆能联络合作机制的网络,各国也要对相关人员加强训练,并配以必要的装备以配合各国合作事项的进行;第四章为最后条款,主要规定《网络犯罪公约》的签署、生效、加入、区域应用、公约的效力、声明、联邦条款、保留、保留的法律地位和撤回、修订、争端处理、缔约方大会、公约的退出和通告等事项。

《网络犯罪公约》在第二章自第二条至第十条中制定了签署国需要对九类网络犯罪行为予以刑法处罚 ,分述于下:

1. 非法存取(Illegal access):指任何故意威胁或攻击电脑系统及电脑资料的行为,如电脑黑客等行为。这些行为不仅带给电脑系统及合法使用者极大困扰,更是影响电脑系统的正常运作,且若电脑系统因此故障,更需耗费人力、物力等资源去修复,故此类行为应予惩罚(原文请参照《网络犯罪公约》第二条)。

2. 非法截取(Illegal interception):此类行为包括非法截取电脑传送的"非公开性质"电脑资料,此项规定是用以保障电脑资料的机密性。根据欧洲理事会说明,如果电脑资料在传送时,没有意图将资讯公开,即使电脑资料是利用公众网络进行传送,也属于"非公开性质"的资料(原文请参照《网络犯罪公约》第三条)。

3. 资料干扰(Data interference):包含任何故意毁损、删除、破坏、修改或隐藏电脑资料的行为。此项规定是为了确保电脑资料的真实性和电脑程序的可用性 (原文请参照《网络犯罪公约》第四条)。

4. 系统干扰(System interference):此项规定与第四条的"资料干扰"不同,此项规定是针对妨碍电脑系统合法使用的行为。根据欧洲理事会的说

明,任何电脑资料的传送,只要其传送方法足以对他人电脑系统构成"重大不良影响",将会被视为"严重妨碍"电脑系统合法使用。所以在此原则下,利用电脑系统传送电脑病毒、蠕虫、特洛伊木马程序或滥发垃圾电子邮件,都符合"严重妨碍"电脑系统,即构成"系统干扰"的行为(原文请参照《网络犯罪公约》第五条)。

5. 设备滥用(Misuse of devices):包含生产、销售、发行或以任何方式提供从事上述各项网络犯罪的设备。由于进行上述网络犯罪,最简便的方式便是使用黑客工具,因而间接催生了这些工具的制作与买卖,因此有必要严厉惩罚这些工具的制作与买卖,从根本上杜绝网络犯罪行为(原文请参照《网络犯罪公约》第六条)。

6. 伪造电脑资料(Computer - related forgery):包括任何虚假资料的输入,更改、删除、隐藏电脑资料,导致相关资料丧失真实性。目前欧洲理事会各成员国法律规定,伪造文件是犯罪行为,必须受到刑事制裁,所以此规定等于将无实体存在的电脑资料也纳入"伪造文书"的文书范围(原文请参照《网络犯罪公约》第七条)。

7. 电脑诈骗(Computer - related fraud):包括任何有诈骗意图的资料输入,更改、删除或隐藏任何电脑资料,干扰电脑系统的正常运作,为个人谋取不法利益而导致他人财产损失。这都是需要予以刑事处罚的犯罪行为(原文请参照《网络犯罪公约》第八条)。

8. 儿童色情的犯罪(Offences related to child pornography):包括一切在电脑系统生产、提供、发行或传送、取得及持有儿童的色情资料。此项规定是泛指任何利用电脑系统进行的上述儿童色情犯罪行为(原文请参照《网络犯罪公约》第九条)。

9. 侵犯著作权及相关权利的行为(Offences related to infringements of copyright and related rights):此项规定包括一系列保护知识产权国际公约列为侵犯著作权的行为,《网络犯罪公约》同时规定这些行为必须为故意、大规模进行,并使用电脑系统所达成的(原文请参照《网络犯罪公约》第十条)。

《网络犯罪公约》为世界上第一个打击网络犯罪的国际公约,必将对世界多数国家的相应立法产生重要影响。遵循《网络犯罪公约》能建立更广泛