普通高等教育“十一五”国家级规划教材

高等院校信息安全专业系列教材

教育部高等学校信息安全类专业教学指导委员会
中国计算机学会教育专业委员会 共同指导

顾问委员会主任：沈昌祥 编委会主任：肖国镇

网络侦查与电子物证系列丛书主编：秦玉海

电子物证检验与分析

汤艳君 主编

高洪涛 罗文华 副主编

秦玉海 审

http://www.tup.com.cn

根据教育部高等学校信息安全类专业教学指导委员会编制的《高等学校信息安全专业指导性专业规范》组织编写

清华大学出版社

普通高等教育“十一五”国家级规划教材

高等院校信息安全专业系列教材

电子物证检验与分析

汤艳君 主编

高洪涛 罗文华 副主编

Information Security

http://www.tup.com.cn

清华大学出版社

北京

内 容 简 介

本书以电子物证检验分析过程中所需要的知识为主线展开，从电子数据、电子数据取证、电子物证检验等相关概念入手，介绍了电子物证检验与分析基本过程、制作电子数据的保全备份的方法、常用的电子物证检验工具的使用方法、不同操作系统环境下电子数据的检验方法以及手机信息的检验方法。特别是在最后章节中结合目前比较典型的案件（如网络赌博、网络敲诈、伪造证件印章、网上非法制造假发票、有害信息传播、侵犯知识产权、窃取商业机密等）开展检验，从而为从事电子物证的检验人员提供有益的帮助。

本书的特点是实用性强，内容全面，注重理论与实践的结合，突出专业特色。本书既可作为网络犯罪侦查和电子物证检验相关专业学生的教材，也可作为从事网络犯罪侦查和电子物证检验人员的参考书。

图书在版编目（CIP）数据

电子物证检验与分析/汤艳君主编. --北京：清华大学出版社，2014
高等院校信息安全专业系列教材
ISBN 978-7-302-34883-2

Ⅰ. ①电… Ⅱ. ①汤… Ⅲ. ①计算机应用－物证－司法鉴定－高等学校－教材 Ⅳ. ①D919.2-39

中国版本图书馆 CIP 数据核字（2013）第 311406 号

责任编辑：张　民　薛　阳
封面设计：傅瑞学
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×260mm　　**印　　张**：16.25　　**字　　数**：402 千字
版　　次：2014 年 2 月第 1 版　　**印　　次**：2014 年 2 月第1次印刷
印　　数：1～2000
定　　价：33.00 元

产品编号：056206-01

高等院校信息安全专业系列教材

编审委员会

出版说明

21世纪是信息时代，信息已成为社会发展的重要战略资源，社会的信息化已成为当今世界发展的潮流和核心，而信息安全在信息社会中将扮演极为重要的角色，它会直接关系到国家安全、企业经营和人们的日常生活。随着信息安全产业的快速发展，全球对信息安全人才的需求量不断增加，但我国目前信息安全人才极度匮乏，远远不能满足金融、商业、公安、军事和政府等部门的需求。要解决供需矛盾，必须加快信息安全人才的培养，以满足社会对信息安全人才的需求。为此，教育部继2001年批准在武汉大学开设信息安全本科专业之后，又批准了多所高等院校设立信息安全本科专业，而且许多高校和科研院所已设立了信息安全方向的具有硕士和博士学位授予权的学科点。

信息安全是计算机、通信、物理、数学等领域的交叉学科，对于这一新兴学科的培养模式和课程设置，各高校普遍缺乏经验，因此中国计算机学会教育专业委员会和清华大学出版社联合主办了“信息安全专业教育教学研讨会”等一系列研讨活动，并成立了“高等院校信息安全专业系列教材”编审委员会，由我国信息安全领域著名专家肖国镇教授担任编委会主任，指导“高等院校信息安全专业系列教材”的编写工作。编委会本着研究先行的指导原则，认真研讨国内外高等院校信息安全专业的教学体系和课程设置，进行了大量前瞻性的研究工作，而且这种研究工作将随着我国信息安全专业的发展不断深入。经过编委会全体委员及相关专家的推荐和审定，确定了本丛书首批教材的作者，这些作者绝大多数都是既在本专业领域有深厚的学术造诣、又在教学第一线有丰富的教学经验的学者、专家。

本系列教材是我国第一套专门针对信息安全专业的教材，其特点是：

① 体系完整、结构合理、内容先进。

② 适应面广，能够满足信息安全、计算机、通信工程等相关专业对信息安全领域课程的教材要求。

③ 立体配套，除主教材外，还配有多媒体电子教案、习题与实验指导等。

④ 版本更新及时，紧跟科学技术的新发展。

为了保证出版质量，我们坚持宁缺毋滥的原则，成熟一本、出版一本，并保持不断更新，力求将我国信息安全领域教育、科研的最新成果和成熟经验反映到教材中来。在全力做好本版教材、满足学生用书的基础上，还经由专家的推荐和审定，遴选了一批国外信息安全领域优秀的教材加入到本系列教

材中，以进一步满足大家对外版书的需求。热切期望广大教师和科研工作者加入我们的队伍，同时也欢迎广大读者对本系列教材提出宝贵意见，以便我们对本系列教材的组织、编写与出版工作不断改进，为我国信息安全专业的教材建设与人才培养做出更大的贡献。

“高等院校信息安全专业系列教材”已于2006年年初正式列入普通高等教育“十一五”国家级教材规划（见教高[2006]9号文件《教育部关于印发普通高等教育“十一五”国家级教材规划选题的通知》）。我们会严把出版环节，保证规划教材的编校和印刷质量，按时完成出版任务。

2007年6月，教育部高等学校信息安全类专业教学指导委员会成立大会暨第一次会议在北京胜利召开。本次会议由教育部高等学校信息安全类专业教学指导委员会主任单位北京工业大学和北京电子科技学院主办，清华大学出版社协办。教育部高等学校信息安全类专业教学指导委员会的成立对我国信息安全专业的发展将起到重要的指导和推动作用。“高等院校信息安全专业系列教材”将在教育部高等学校信息安全类专业教学指导委员会的组织和指导下，进一步体现科学性、系统性和新颖性，及时反映教学改革和课程建设的新成果，并随着我国信息安全学科的发展不断修订和完善。

我们的E-mail地址 zhangm@tup.tsinghua.edu.cn；联系人：张民。

清华大学出版社

前言

在网络犯罪以及涉网络的违法犯罪案件中，计算机扮演着重要的角色。通常计算机既是犯罪分子攻击的目标，也是犯罪分子作案的工具。但无论作为哪种角色，计算机及其外设以及电子设备中都会留下大量与犯罪相关的数据。而对于打击网络犯罪而言，最重要的就是利用电子物证检验方法和技术检验出与犯罪活动相关的电子数据，证明犯罪事实，为有力地打击犯罪提供有效的证据。

为了培养高素质的电子物证检验人员，我们编写本书，全书共分 8 章。第 1 章电子物证检验与分析概述，简要介绍什么是电子数据、电子数据取证、电子物证检验等相关概念和电子物证封存与固定方法；第 2 章电子物证检验与分析基本过程，主要内容包括电子物证检验与分析的对象、电子物证检验与分析条件、电子物证检验与分析过程等；第 3 章制作电子数据的保全备份，主要内容包括存储介质的擦除、保全备份、数据完整性校验等内容；第 4 章常用电子物证检验工具，主要内容包括 EnCase 检验工具、X-Ways 检验工具、FTK 检验工具，特别针对目前主流的电子物证检验工具各自特点进行了比较；第 5 章 Windows 系统的检验方法，主要内容包括不同类型文件的检验方法，如松弛空间、自由空间、未分配空间中数据的检验方法，日志文件、注册表、交换文件、Internet Explorer 的访问历史记录、临时文件、回收站、打印脱机文件、隐藏文件、聊天记录、电子邮件文件等文件的检验方法等；第 6 章 UNIX/Linux 系统的检验方法，主要内容包括 UNIX/Linux 环境下文件系统、日志文件、用户账号与用户组信息、系统启动任务、特殊文件的检验方法；第 7 章手机的检验，主要内容包括收缴手机制的保管与封装、手机常用信息的获取、手机信息的检验等内容；第 8 章典型案例分析与检验，主要针对目前比较典型的案件如网络赌博、网络敲诈、伪造证件印章、网上非法贩卖枪支弹药、非法制造假发票、有害信息传播、侵犯知识产权、窃取商业机密等案件开展检验，从而为从事电子物证检验人员提供有益的帮助。

本书的特点是实用性强，内容全面，注重理论与实践的结合，突出专业特色。本书既可作为网络犯罪侦查和电子物证检验相关专业学生的教材，也可作为从事网络犯罪侦查和电子物证检验人员的参考书。

本书由汤艳君主编、统稿并编写了第 1 章、第 3.1～3.2 节、第 5 章、第 8.7 节；范德宝编写了第 2 章；于晓聪编写了第 3.3 节，高洪涛编写了第 4 章、第 8.1～8.3 节；罗文华编写了第6 章、第 8.8～8.11 节，马贺男编写了第 7 章、

第8.4节，高杨编写了第8.5节，李子川编写了第8.6节。

在编写本书的过程中我们参考和吸收了国内外同行的研究成果，在此一并表示感谢！

尽管在编写此书过程中作者做了很多努力，但由于水平有限，书中难免有错漏之处，敬请读者批评指正。

编　者

2014年1月

目录

第1章 电子物证检验与分析概述

在网络犯罪以及涉网络的违法犯罪案件中，计算机扮演着重要的角色。通常计算机既是犯罪分子攻击的目标，也是犯罪分子作案的工具。但无论作为哪种角色，计算机及其外设中都会留下大量与犯罪相关的数据。而对于打击网络犯罪而言，最重要的就是利用电子物证检验方法和技术检验出与犯罪活动相关的电子数据，证明犯罪事实，为有力地打击犯罪提供有效的证据。

本章将从什么是电子数据、电子物证检验以及电子物证检验与分析的原则、步骤等方面进行介绍。

1.1 电子数据

十一届全国人大第五次会议于2012年3月14日表决通过了关于修改《中华人民共和国刑事诉讼法》的决定，时任国家主席胡锦涛签署第55号主席令予以公布。修改后的刑事诉讼法于2013年1月1日开始施行。修改后的刑事诉讼法的第五章第四十八条规定：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)犯罪嫌疑人、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。证据必须经过查证属实，才能作为定案的根据。

十一届全国人大第二十八次会议于2012年8月31日表决通过了关于修改《中华人民共和国民事诉讼法》的决定，时任国家主席胡锦涛签署第59号主席令予以公布。修改后的刑事诉讼法于2013年1月1日开始施行。修改后的民事诉讼法的第六章第六十三条规定，证据包括：(一)当事人的陈述；(二)书证；(三)物证；(四)视听资料；(五)电子数据；(六)证人证言；(七)鉴定意见；(八)勘验笔录。证据必须查证属实，才能作为认定事实的根据。

人们常说“事实胜于雄辩”，证据作为诉讼的核心，正是事实的体现和反映。此次《中华人民共和国刑事诉讼法》和《中华人民共和国民事诉讼法》均增加了电子数据作为证据法定形式，又为客观反映案情增加了一种重要体现形式。

虽然在修改后的《中华人民共和国刑事诉讼法》和《中华人民共和国民事诉讼法》中均增加了电子数据作为证据的法定形式，但没有明确什么是电子数据。有关电子数据的定义应该有广义和狭义之分。

1.1.1 电子数据定义

从广义上来讲，只要是以电子形式存储、处理、传输的信息都是电子数据。而狭义上的电子数据即刑事诉讼法和民事诉讼法中所规定的电子数据，应该是指“由电子设备产生、存储或传输的有证据价值的电子数据”，即电子数据证据，简称电子证据。这一定义具有以下三个方面的含义：

第一，电子数据既包括以电子形式存在的数据，也包括其派生物。所谓电子形式就是一种以程序、文本、声音、图像、视频等形式存在的信息。可以将其概括为“由介质、磁性物、光学设备、计算机内存或类似设备生成、发送、接收、存储的任一信息的存在形式”。它是一种由电子技术带来的存在形式，无法为人眼或人耳直接阅读或聆听，必须予以转换才能为人所知。”

在实际工作中，还常常会遇到那些由电子形式材料转化而来的附属材料，即派生物。如将计算机内部文件打印在纸面或胶片上得来的计算机打印输出，虽然表面上同传统纸质文件没有太大的不同，但绝不能一概地视为书证，而应作具体分析。如果该打印输出具有独立性，则作传统书证处理；如果该打印输出不具有独立性，即其能否证明待证事实取决于能否同计算机系统内部的证据鉴证一致，则应当视为处于派生证据地位的电子证据。

第二，电子数据是借助信息技术或信息设备形成的。随着科学技术的发展，信息技术与设备已出现了很多种类，而且还将以人类难以想象的速度继续发展。信息技术包括但不局限于计算机技术，信息设备包括但不局限于电子计算机设备。

第三，电子数据必须与案件有联系，且具有证据价值。

电子数据必须是客观存在的，且与需要证明的案情之间有一定的关系或联系，由法定机关、法定人员依照法定程序收集和取得的证据才能称为电子数据，否则不能作为法定证据来使用。

1.1.2 电子数据特点

电子数据的承载介质是包括硬盘、磁盘、光盘等在内的存储媒介，存储媒介必须通过包括计算机硬件在内的电子设备才能访问，主要具有如下的特点。

1. 表现形式的多样性与复杂性

电子数据的外在表现形式具有多样性，不仅可以表现为文字、图像、声音或它们的组合，还可以是交互式的、可编译的，因此电子数据能够更加直观、清晰、生动、完整地反映特征事实及其形成过程。

2. 依赖介质性与无形性

电子数据需要借助一定的介质存在，如硬盘、光盘等。在介质上保存实质上是由按照一定编码规则以 0 和 1 的序列保存，其记录的内容不但肉眼看不到，具有无形性，而且凭人的思维也很难解读，只有在经过一系列的处理程序后通过屏幕显示或打印机打印才能为人识别，而且丝毫不会受到感情、经验等多种主观因素的影响。