“十二五”职业教育国家规划教材（经全国职业教育教材审定委员会审定）
高等职业教育精品示范教材 信息安全系列

计算机取证与司法鉴定

主 编 张 湛 武春岭
副主编 瞿 芳 邓 晶

本书特色：

- 以就业为导向，以能力为本位
- 项目案例引导，任务需求驱动
- 生活实例链接知识点，案例增加趣味性
- 通用教学内容与特殊教学内容协调配置

中国水利水电出版社
www.waterpub.com.cn

“十二五”职业教育国家规划教材（经全国职业教育教材审定委员会审定）

高等职业教育精品示范教材（信息安全系列）

计算机取证与司法鉴定

主　编　张　湛　武春岭

副主编　瞿　芳　邓　晶

中国水利水电出版社
www.waterpub.com.cn

内 容 提 要

本书针对信息安全产业实际和信息安全专业人才对计算机取证和司法鉴定技能的迫切需要，结合高职高专教学特点和计算机取证课程教学改革成果编写而成。

本书采用“项目牵引、任务驱动”的模式，全面系统地介绍了计算机取证和司法鉴定的基本理论以及实际案例调查的操作规程和技术运用。借鉴了国内高职高专教材编写的成功经验，强调理论以够用为度，以既相互独立又有所联系的计算机取证和司法鉴定的各个案例为主线，强调计算机取证调查技术的实际运用，可操作性强。

本书主要读者对象为计算机专业和法学专业的高职高专学生和本科学生，也可作为企业安全取证人员、行业信息安全管理人员的培训教材。

本书提供免费电子教案，读者可以从中国水利水电出版社网站以及万水书苑下载，网址为：http://www.waterpub.com.cn/softdown 或 http://www.wsbookshow.com/。

图书在版编目（CIP）数据

计算机取证与司法鉴定 / 张湛，武春岭主编. -- 北京 : 中国水利水电出版社，2014.9
“十二五”职业教育国家规划教材. 高等职业教育精品示范教材. 信息安全系列
ISBN 978-7-5170-2560-3

Ⅰ. ①计… Ⅱ. ①张… ②武… Ⅲ. ①计算机犯罪－证据－调查－高等职业教育教材－教材②计算机犯罪－司法鉴定－高等职业教育教材－教材 Ⅳ. ①D918

中国版本图书馆CIP数据核字(2014)第226328号

策划编辑：祝智敏　责任编辑：宋俊娥　加工编辑：夏雪丽　封面设计：李　佳

书　名	“十二五”职业教育国家规划教材(经全国职业教育教材审定委员会审定) 高等职业教育精品示范教材（信息安全系列） **计算机取证与司法鉴定**
作　者	主　编　张　湛　武春岭 副主编　瞿　芳　邓　晶
出版发行	中国水利水电出版社 （北京市海淀区玉渊潭南路1号D座　100038） 网址：www.waterpub.com.cn E-mail：mchannel@263.net（万水） sales@waterpub.com.cn 电话：（010）68367658（发行部）、82562819（万水）
经　售	北京科水图书销售中心（零售） 电话：（010）88383994、63202643、68545874 全国各地新华书店和相关出版物销售网点
排　版	北京万水电子信息有限公司
印　刷	北京蓝空印刷厂
规　格	184mm×240mm　16开本　18.5印张　406千字
版　次	2014年9月第1版　2014年9月第1次印刷
印　数	0001—4000册
定　价	38.00元

高等职业教育精品示范教材（信息安全系列）

丛书编委会

序　言

随着信息技术和社会经济的快速发展，信息和信息系统成为现代社会极为重要的基础性资源。信息技术给人们的生产、生活带来巨大便利的同时，计算机病毒、黑客攻击等信息安全事故层出不穷，社会对于高素质技能型计算机网络技术和信息安全人才的需求日益旺盛。党的十八大明确指出“高度关注海洋、太空、网络空间安全”，信息安全被提到前所未有的高度。加快建设国家信息安全保障体系，确保我国的信息安全，已经上升为我国的国家战略。

发展我国信息安全技术与产业，对确保我国信息安全有着极为重要的意义。信息安全领域的快速发展，亟需大量的高素质人才。但与之不相匹配的是，在高等职业教育层次信息安全技术专业的教学中，还更多地存在着沿用本科专业教学模式和教材的现象，对于学生的职业能力和职业素养缺乏有针对性的培养。因此，在现代职业教育体系的建立过程中，培养大量的技术技能型信息安全专业人才成为我国高等职业教育领域的重要任务。

信息安全是计算机、通信、数学、物理、法律、管理等学科的交叉学科，涉及计算机、通信、网络安全、电子商务、电子政务、金融等众多领域的知识和技能。因此，探索信息安全专业的培养模式、课程设置和教学内容就成为信息安全人才培养的首要问题。高等职业教育信息安全与管理专业丛书编委会的众多专家、一线教师和企业技术人员，依据最新的专业教学目录和教学标准、结合就业实际需求，组织了以就业为导向的高等职业教育精品示范教材（信息安全系列）的编写工作。该系列教材由《网络安全产品调试与部署》、《网络安全系统集成》、《Web 开发与安全防范》、《数字身份认证技术》、《计算机取证与司法鉴定》、《操作系统安全（Linux）》、《网络安全攻防技术实训》、《大型数据库应用与安全》、《信息安全工程与管理》、《信息安全法规与标准》、《信息安全风险评估》等组成，在紧跟当代信息安全研究发展的同时，全面、系统、科学地培养信息安全类技术技能型人才。

本系列教材在组织规划的过程中，遵循以下几个基本原则：

（1）体现就业为导向、产学结合的发展道路。学科和专业同步加强，按企业需要、按岗位需求来对接培养内容。既能反映信息安全学科的发展趋势，又能结合信息安全专业教育的改革，且及时反映教学内容和教学体系的调整更新。

（2）采用项目驱动、案例引导的编写模式。打破传统的以学科体系设置课程体系、以知识点为核心的框架，更多地考虑学生所学知识与行业需求及相关岗位、岗位群的需求相一致，坚持“工作流程化”、“任务驱动式”，突出“走向职业化”的特点，努力培养学生的职业素养、职业能力，实现教学内容与实际工作的高仿真对接，真正以培养技术技能型人才为核心。

（3）专家和教师共建团队，优化编写队伍。由来自信息安全领域的行业专家、院校教师、企业技术人员组成编写队伍，跨区域、跨学校进行交叉研究、协调推进，把握行业发展和创新

教材发展方向，融入信息安全专业的课程设置与教材内容。

（4）开发课程教学资源，推进专业信息化建设。从充分关注人才培养目标、专业结构布局等入手，开发补充性、更新性和延伸性教辅资料，开发网络课程、虚拟仿真实训平台、工作过程模拟软件、通用主题素材库以及名师讲义等多种形式的数字化教学资源，建立动态、共享的课程教材信息化资源库，服务于系统培养技术技能型人才。

信息安全类教材建设是提高信息安全专业技术技能型人才培养质量的关键环节，是深化职业教育教学改革的有效途径。为了促进现代职业教育体系的建设，使教材建设全面对接教学改革、行业需求，更好地服务区域经济和社会发展，我们殷切希望各位职教专家和老师提出建议，并加入到我们的编写队伍中来，共同打造信息安全领域的系列精品教材！

丛书编委会

2014 年 6 月

前　言

随着近20年信息技术和计算机网络技术的发展，特别是近年来云计算技术的普遍运用，公众的生活和工作已与计算机和信息网络紧密联系在一起。在这样的环境下，计算机犯罪或利用计算机工具的犯罪活动急剧增加，与计算机或电子证据相关的民事纠纷也越来越多，这使得涉及计算机取证的案例调查和司法实践的需求越来越迫切，社会迫切需要培养计算机取证和司法实践的专业职业人才。

计算机取证通常是一个需要严谨且训练有素的团队，历时数十小时甚至上百小时并利用各种工具认真发现、比对和归类的过程，也是一个小心翼翼进行证据保全和准备取证报告的过程，是一个既枯燥又有趣的充满挑战的过程。本书会深入介绍在计算机取证和司法鉴定的实施中，那些极其重要的不可忽略的部分。

一、结构

本书没有按部就班地介绍深奥枯燥的计算机取证理论，而是切合高等职业人才的培养特点，强调理论以够用为度，以既相互独立又有所联系的计算机取证和司法鉴定的案例为主线，分六个大的项目，从计算机取证准备和现场处理开始，依次论述 Windows 环境单机取证、非 Windows 环境的单机取证、原始证据的深入分析、网络取证和针对多媒体的取证六个计算机取证的重要领域和过程，全面系统地介绍了计算机取证和司法鉴定的基本理论以及实际案例调查的操作规程和技术运用，且每个项目均以实训和习题的形式配备大量来自工程实践的应用案例。全书立足于计算机取证调查技术的实际运用，可操作性强。本书具体内容和建议课时如下表所示。

章节序号	章节名称	子任务数量	理论课时	实践学时
1	计算机取证准备和现场处理	3	6	3
2	Windows 环境单机取证	5	6	6
3	非 Windows 环境的单机取证	2	5	6
4	原始证据的深入分析	2	6	9
5	在网络中进行取证	2	6	6
6	针对多媒体进行取证	3	5	4

每个项目名称本身就是一个大的学习任务，以“项目说明－项目任务－基础知识－项目分析－项目实施－应用实训－拓展练习”为主线，每个项目内容在涵盖基本理论知识的基础上，

以项目案例调查为实践落脚点，通过“项目说明和项目任务”让学生首先了解要解决的实际问题，激发学习兴趣；然后通过“基础知识”的学习，奠定相应的理论和技术基础；进而通过“项目分析”使学生明确具体项目的实施策略，并在“项目实施”中以项目任务为规划分步完成项目，体现学以致用；最后通过“应用实训”和“拓展练习”巩固学生学习成果，从而实现理实一体化的高效教学。整个内容结构步步为营、环环相扣，理论实践浑然天成，体现了任务驱动和“教学做”一体化的思想。

二、特色

1. 实用——贴近企业

本书在编写过程中，查阅了大量国际一流计算机取证公司的产品技术和规范，并得到多家计算机取证产品公司的技术支持，内容取舍来源于企业需求，实用性高。

2. 实效——理实一体

教材在编写过程中，以“项目引导、任务驱动”为思路，从项目案例的“项目说明和项目任务”入手，使学生通过真实的案例了解所学内容的实用价值，提高学生兴趣，然后展开“基础知识”的学习。通过“项目分析和项目实施”完成项目，并通过“应用实训和拓展练习”强化学生技能，体现了任务驱动和“教学做”一体化的思想，实效性高。

三、面向对象

本书主要面向计算机专业和法学专业的高职高专院校学生（建议教学学时为 68 学时，课堂讲授和取证实践学时各占一半），也可作为相关专业本科学生、企业信息安全人员、行业信息安全管理人员的培训教材；对于 IT 行业人士、司法鉴定人士、司法和执法工作者、律师以及法学理论研究者也具有良好的参考价值。

四、致谢

本书由重庆电子工程职业学院张湛、武春岭任主编，瞿芳、邓晶为副主编。张湛负责组织策划，并编写项目 4 和项目 6，武春岭负责结构规划、统稿，并编写项目 1，瞿芳负责编写项目 2 和项目 3，邓晶负责编写项目 5。在本书编写过程中，廖浩一、史海深和胡雨薇同学提供了大量的帮助，在此对他们表示感谢。

由于本书作者水平所限，书中错漏之处，敬请读者批评指正。作者邮箱：blacksnown@126.com。

编　者

2014 年 6 月于重庆

目　录

1 计算机取证准备和现场处理

学习目标

- 理解计算机取证的概念和计算机取证的原则
- 了解计算机取证的法律程序
- 了解企业内部取证和司法取证的异同
- 掌握计算机取证前的程序准备和文档准备的方法
- 掌握计算机取证前的取证启动盘和取证工具箱的准备方法
- 掌握计算机取证现场的处理方法

项目说明

某公司一名部门经理 Adam 和一名技术骨干 Bob，在工作四年以后突然离职，并开办了另一家公司，新成立公司的业务范围与原公司几乎完全相同，从而导致原公司产品的销售量急剧减少。在发现这样的情况后，原公司的主管 Alice 怀疑这两名雇员在原公司工作期间就利用上班时间发展自己的私人业务，并窃取公司机密资料为新创办公司做准备，因此授权企业 IT 部门的调查人员 Tom 来调查这两名雇员的办公电脑和所有公司给予他们的存储介质，以便找到相关证据。

项目任务

Tom 接受这个取证任务后，应当首先完成三个任务：

1．在进入计算机取证现场之前分析案例性质，并根据案例性质进行计算机取证的程序和文档准备；

2．进行进入取证现场前的外围调查，并根据案例特点进行计算机取证的设备和工具准备；

3．在进入取证现场的时候对原始证据进行妥善处理。

基础知识

1.1 计算机取证调查和鉴定的概念

1.1.1 计算机取证和司法鉴定

计算机取证的权威性定义目前尚未完全统一，许多专业机构和学者均从不同的角度给出了计算机取证的定义。根据http://whatis.com的定义，“计算机取证是一种调查和分析技术，这种技术是用来从特定计算机设备中收集和保存证据，并向法庭出示该证据。计算机取证的目的是进行结构性调查并保存证据链，从而确切地找出在特定计算机设备上发生了什么，谁应为此负责。”；著名计算机取证专家 Judd Robbins 则认为“计算机取证不过是将计算机调查和分析技术应用于对潜在的、有法律效力的证据的确定与获取”；另一位专家 R C Mark 认为计算机取证是“从计算机中收集和发现证据的技术和工具”。

国内著名计算机取证专家麦永浩教授则根据计算机取证的发展状况给出了较为全面的定义：计算机取证（Computer Forensics）是研究如何对计算机犯罪的证据进行获取、保存、分析和出示的法律规范和科学技术。

司法鉴定是指在诉讼活动中，鉴定人运用科学技术或者专门知识对诉讼涉及的专门性问题进行鉴别和判断，并提供鉴定意见的活动。或者说，司法鉴定是指在诉讼过程中，对案件中的专门性问题，由司法机关或当事人委托法定鉴定单位，运用专业知识和技术，依照法定程序做出鉴别和判断的一种活动。

2005 年 2 月，全国人民代表大会常务委员会通过的《全国人民代表大会常务委员会关于司法鉴定管理问题的决定》规定，国家对从事下列司法鉴定业务的鉴定人和鉴定机构实行登记管理制度：

- 法医类鉴定；
- 物证类鉴定；
- 声像资料鉴定；
- 根据诉讼需要由国务院司法行政部门、最高人民法院、最高人民检察院确定的其他应当对鉴定人和鉴定机构实行登记管理的鉴定事项。

1.1.2 计算机取证调查和鉴定的业务范围

目前与计算机取证（Computer Forensics）相关的提法还有数字取证（Digital Forensics）以及电子取证（Electronic Forensics），严格地说，这两种提法和计算机取证是有一定区别的。

这种区别主要表现在取证调查针对的主体对象不同，计算机取证的主体对象是计算机系统内与案件有关的数据信息，数字取证的主体对象则是存在于各种电子设备中与案件有关的数字信息，电子取证的主体对象是所有与案件有关的电子信息。因此，严格地说，计算机取证包含于数字取证，数字取证包含于电子取证。但是由于目前计算机系统已经通过嵌入式系统的方式，在许多电子设备当中运行，因此在实际的技术运用中，通常我们所说的计算机取证涵盖了一定的数字取证和电子取证的内容。

计算机取证通常包含单机取证、网络取证、手机取证和多媒体取证等诸多方面。所谓单机取证主要指通过对单台或多台独立的计算机进行调查，从而获取、保存、分析和出示与案件相关的证据。而网络取证则不同，其主要针对的是计算机网络，调查的重点在于各种网络设备（服务器、路由器、防火墙、入侵检测系统等），也即主要是通过对各种网络行为的调查和分析，从而获取与案件相关的证据。手机取证的对象不仅包含各种手机，也包含各种智能数据终端（如 PDA、PAD 等），通过对各种数据终端的分析和调查，从而获取与案件相关的证据。多媒体取证包含的内容较广，其主要对象是各种多媒体文件（如文档、图像、音频、视频等），其主要业务范围包含多媒体版权鉴定、多媒体内容真假认证、多媒体中隐藏和嵌入隐秘信息的可能性和对隐藏的内容进行取证等。

司法鉴定通常包括：法医鉴定，即对与案件有关的尸体、人身、分泌物、排泄物、胃内物、毛发等进行鉴别和判断的活动；司法精神病鉴定，即对人是否患有精神病、有没有刑事责任能力进行鉴别和判断的活动；刑事技术鉴定，即对指纹、脚印、笔迹、弹痕等进行鉴别和判断的活动；会计鉴定，即对账目、表册、单据、发票、支票等书面材料进行鉴别和判断的活动；技术问题鉴定，即对涉及工业、交通、建筑等方面的科学技术进行鉴别和判断的活动等。

2007 年颁布实施的《司法鉴定程序通则》（中华人民共和国司法部令第 107 号）对我国司法鉴定的实施程序进行了详细规定。把司法鉴定的业务范围较为详细地划分为法医病理鉴定、法医临床鉴定、法医精神病鉴定、法医物证鉴定、法医毒物鉴定、文书鉴定、痕迹鉴定、微量鉴定、声像资料鉴定、计算机司法鉴定、环境监测司法鉴定、工程造价司法鉴定、产品质量司法鉴定、司法会计鉴定、知识产权司法鉴定、税务司法鉴定、农业司法鉴定、资产评估司法鉴定、建筑工程司法鉴定和枪弹痕迹司法鉴定。

其中“计算机司法鉴定”是指依法取得有关计算机司法鉴定资格的鉴定机构和鉴定人受司法机关或当事人委托，运用计算机理论和技术，对通过非法手段使计算机系统内数据的安全性、完整性或系统正常运行造成的危害行为及其程度等进行鉴定并提供鉴定结论的活动。而“声像资料鉴定”，是指运用物理学和计算机学的原理和技术，对录音带、录像带、磁盘、光盘、

图片等载体上记录的声音、图像信息的真实性、完整性及其所反映的情况过程进行鉴定，并对记录的声音、图像中的语言、人体、物体做出种类或同一认定。

因此本书中所讲的司法鉴定，在涉及计算机文档、资料、信息等与计算机取证相关的司法鉴定时，应属于上述的计算机司法鉴定；在涉及多媒体内容认证等问题时，应属于声像资料鉴定。

通常计算机取证与司法鉴定的业务类型主要分为以下六类：

（1）存在性认定：认定在特定的存储媒介中存储有特定的信息。

（2）信息量认定：认定在特定媒介中存在的信息量的大小，例如对于制作或传播淫秽信息案件，通常需要认定淫秽信息的数量以及点击数量等。

（3）同一性认定：同一性认定或相似性认定分为两个方面，一方面是通过信息比对和统计分析，认定两个信息是否具有同一性或它们相似的程度，另一方面是通过对特定程序的对比分析，认定两个程序在功能上是否具有同一性或它们相似的程度，同一性分析常常在知识产权侵权案件中运用。

（4）来源认定：通过分析时间信息、生成方式、传播渠道等认定特定信息的最初来源，例如某张照片是否是某台特定的数码相机拍摄的，某个程序的源代码的作者是谁，网上某个谣言传播的源头等。

（5）功能认定：通过对特定程序的静态和动态分析，对该程序是否具有某种特定的功能进行认定，例如对程序代码是否具有盗窃信息、远程控制、自我复制、逻辑炸弹等恶意功能的认定。

（6）事件重构：通常包含四个方面：

- 对犯罪主体进行认定，例如通过对特定事件的分析，描绘嫌疑人的技术水平、行为习惯等；
- 对犯罪主观方面进行认定，也即嫌疑人的特定行为是主观故意的还是过失性的；
- 对犯罪客观方面进行认定，主要是分析认定何人在何时实施了何种行为等；
- 对犯罪客体进行认定，例如对于恶意网络攻击，通常需要对攻击的范围、规模进行认定，从而认定攻击造成的破坏程度。

1.1.3 计算机取证的发展状况

当前计算机技术的应用已经深入社会生活的方方面面，计算机技术成为一种犯罪手段，计算机信息成为犯罪目标人们也已经司空见惯，但是就计算机的根本性质而言，其仅仅是存储和处理证据的场所。

20 世纪 70 年代以来，计算机犯罪的数量一直在增长。最初由于计算机以大型机为主，因此计算机犯罪通常针对大型机，且常常发生在金融领域。最出名的案例就是发生在美国的“半分钱犯罪”，即计算机程序员修改了银行利息计息的程序，将所有不足一分钱的利息自动转入自己开设的账户中，从而在普通账户不易察觉的情况下获得巨额经济利益。

随着 20 世纪 80 年代个人计算机开始普及并逐渐进入社会经济的各个领域，众多操作系统也开始出现，如 Apple 公司的 Macintosh、PC-DOS、IBM-DOS 和 MS-DOS 等。针对各种操作系统的计算机取证的初期工具开始出现，但当时的工具大多采用 C 语言或汇编语言编写，只提供给特定的执法机构使用。

到 20 世纪 90 年代初期，出现了计算机取证的专业工具，IACIS（国际计算机调查专家协会）提供了对当时取证调查软件的培训，IRS（美国国税局）则制定了针对计算机取证搜查的方案。

随后，ASR Data 公司为 Macintosh 操作系统开发出第一款商用的计算机取证工具——Expert Witness，从而将计算机取证工具从执法机构的专用工具推向商用领域，使得计算机取证不仅仅用于调查计算机犯罪，也用于公司内部违规方面的调查。ASR Data 公司的合伙人之一后来离开该公司，开发了 EnCase 软件，该软件也成为目前最为流行的计算机取证工具之一。

随着计算机技术的持续发展，人们开发出越来越多的计算机取证软件，计算机取证领域也正在快速走向成熟。来自 SANS 研究院和 Guidance 等公司的资格认证计划专门培训计算机取证分析师。一些功能完全的取证软件包为计算机取证分析人员提供了技术支持和得到法庭证明的解决方案，如由 IRS 刑事调查局维护并仅限于执法部门使用的 iLook 软件、AccessData 公司的 FTK（Forensics Toolkit）软件、EnCase、NTI 套装、Coroners Toolkit（TCT）、针对苹果 MacOS 的 Mac Forensics Lab 取证分析软件等。

在这个领域共享知识和实践经验的计算机安全专家组成了一些组织机构，如由企业界和 FBI 建立的关键设施保护组织（www.infraGard.org），高科技犯罪调查协会（HTCIA）（http://htcia.asia/），计算机应急响应组织（CERT）（http://www.cert.org.cn）等。一些大学也正在从事计算机取证的研究和教学，在国际上较为知名的有美国卡内基-梅隆（Carnegie-Mellon）大学、加利福尼亚大学伯克利分校、宾夕法尼亚州立大学等。

当前计算机取证领域的新工具和新技术正不断涌现，在可预见的未来，由于数字信息的指数级增长，计算机取证领域将充满活力和引人注目。

1.1.4 计算机取证调查与个人隐私和公司秘密的保障

一般认为，计算机空间也是一个私密空间，当事人使用计算机等设备必然有一定的隐私，所以在美国等国家如果需要实施司法计算机搜查是需要申领搜查令的。在我国，进行司法计算机搜查是否需要申请令状，本质上需要在国家机关顺利开展侦查与公民生活不受打扰两方面进行利益权衡。

隐私权已然成为我国公民日常生活的一项基本人权。因此除法律特别规定的情形外，计算机搜查原则上必须以申请令状为前提。需要申请搜查令的计算机搜查应当至少满足三项基本条件。

（1）建立在正当理由的基础上，即申请令状的计算机取证调查人员必须有相当的证据表