

## <<计算机取证>>

### 图书基本信息

书名：<<计算机取证>>

13位ISBN编号：9787115108753

10位ISBN编号：7115108757

出版时间：2003-8-1

出版时间：人民邮电出版社

作者：Warren G.Kruse ,Jay G.Heiser

页数：268

字数：427000

译者：克鲁泽

版权说明：本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问：<http://www.tushu007.com>

## <<计算机取证>>

### 内容概要

计算机越来越多地被卷入到犯罪活动中，或者是受攻击的目标，或者是犯罪的工具。

计算机取证是计算机安全领域中的一个全新的分支，涉及计算机犯罪事件证据的获取、保存、分析、证物呈堂等相关法律、程序、技术问题。

本书的作者结合信息安全领域多年的经验和计算机取证培训班学员的需求，详细介绍了计算机取证相关的犯罪的追踪、密码技术、数据隐藏、恶意代码、主流操作系统取证技术，并详细介绍了计算机取证所需的各种有效的工具，还概要介绍了美国司法程序。

本书适合计算机网络和信息安全领域的工程技术人员阅读。

对执法部门的计算机犯罪调查人员以及计算机安全事件调查处理人员，本书是目前非常难得的参考书

。

## &lt;&lt;计算机取证&gt;&gt;

## 书籍目录

第1章 计算机取证概述 1.1 什么是取证 1.2 计算机犯罪日趋严重 1.3 计算机取证究竟是什么 1.4 第一步：获取证物 1.4.1 处理证据 1.4.2 记录调查工作 1.5 第二步：鉴定证物 1.6 第三步：分析 1.7 结论 1.8 更多资源 1.8.1 Listserv 1.8.2 机构 1.8.3 协会 1.8.4 正式的培训 1.8.5 其他网络资源 第2章 跟踪罪犯 2.1 Internet基础 2.2 应用程序地址 2.3 走近潜伏者 2.4 拨号会话 2.5 跟踪电子邮件和新闻组 2.5.1 跟踪电子邮件 2.5.2 解读邮件来源 2.6 SMTP服务器日志 2.7 网络新闻组（Usenet） 2.8 网络输入输出系统（NetBIOS） 2.9 第三程序 2.9.1 NetBIOS工具 2.9.2 Whois帮助 2.9.3 核实 2.9.4 入侵检测系统（IDS） 2.10 查找Internet所属单位的网络资源 2.10.1 国际注册机构 2.10.2 网络诊断和调查站点 2.10.3 新闻组和电子邮件滥用信息 第3章 硬盘驱动器和存储介质基础 3.1 到底什么是硬盘 3.1.1 控制器 3.1.2 硬盘的参数 3.1.3 硬盘的软配置 3.1.4 查看和操作分区表 3.2 操作系统 3.2.1 文件系统 3.2.2 在未分配空间中淘金 3.2.3 你能真正删除硬盘上的数据吗 3.3 便携式电脑 3.4 结论 3.5 更多资源 第4章 加密和取证 4.1 密码完整性服务 4.2 密码私密性服务 4.3 时间戳 4.4 编码和压缩 4.5 结论 4.6 更多资源 第5章 数据隐藏 5.1 使用和破解加密应用程序 5.2 改变密码 5.3 隐藏和发现数据 5.4 别忘了网络 5.5 隐写术 5.6 戴上眼罩 5.7 结论 第6章 恶意代码 第7章 取证电子工具箱 第8章 调查Windows计算机 第9章 取证员Unix入门 第10章 攻击Unix主机 第11章 调查Unix主机 第12章 美国司法系统简介 第13章 总结 附录A Internet数据中心应急响应指南 附录B 事件响应调查表 附录C 怎样成为Unix高手 附录D 导出Windows 2000的个人证书 附录E 怎样“撬开”Unix主机 附录F 创建Linux启动光盘 附录G 取证光盘的内容

## <<计算机取证>>

### 版权说明

本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问:<http://www.tushu007.com>