<<计算机取证技术>>

图书基本信息

书名：<<计算机取证技术>>

13位ISBN编号：9787030215291

10位ISBN编号：703021529X

出版时间：2008-6

出版时间：科学出版社

作者：殷联甫

页数：155

<<计算机取证技术>>

前言

计算机取证技术是一门涉及计算机科学、法学等多个领域的交叉学科。
作为一个新领域，计算机取证技术在我国研究与实践的时间都不长，但打击计算机犯罪等现实需要，使得对此领域产生兴趣的人越来越多。
计算机取证技术在我国必将会有更加迅速的发展。
目前国内正式出版的计算机取证方面的书籍较少。
本书作者多年来一直致力于计算机取证方面的研究，从2004年开始编写此书，历时四载，经过反复修改，终于完成了此书。
作者编写本书的主要目的是抛砖引玉，希望有更多的人了解、关注计算机取证技术，从而推动、促进我国计算机取证技术的发展。
全书共分8章。
第1章介绍计算机取证的基本概念，主要有电子证据的概念、计算机取证的原则和步骤、计算机取证模型及计算机取证的发展趋势等内容；第2章介绍计算机取证的常见工具，主要包括计算机取证的相关工具、取证复制工具包、取证分析工具包、国内外计算机取证设备对比与分析及Linux环境下的计算机取证工具介绍等内容；第3章介绍硬盘结构及文件系统基础，主要包括硬盘结构、硬盘数据组织及文件的删除号恢复等内容；第4章介绍Windows系统取证方法，主要包括windows系统初始响应方法及windows系统取证实例等内容；第5章介绍Unix系统取证方法，主要包括Unix系统初始响应方法及Unix系统取证分析等内容；第6章介绍Linux系统取证方法，主要包括Linux系统初始响应方法、Linux磁盘介质备份及Linux系统取证方法等内容；第7章介绍计算机反取证技术，主要包括数据擦除、数据隐藏、Linux环境下常见的计算机反取证工具介绍及Windows环境下常见的计算机反取证工具介绍等内容；第8章介绍可引导取证-工具Helix及其使用。
本书在编写过程中参考、引用了国内外相关文献及有关网站的内容，在此表示衷心的感谢。
由于作者水平有限，书中难免存在疏漏与不妥之处，恳请广大读者和同行专家批评指正。

<<计算机取证技术>>

内容概要

本书系统地讲述了计算机取证的基本概念、原理及方法，主要涉及计算机取证的基本原则和步骤、计算机取证的常见工具、硬盘结构及文件系统基础、Windows系统取证方法、Unix系统取证方法、Linux系统取证方法、计算机反取证技术及可引导取证工具Helix及其使用等内容。

本书共分8章，通过阅读，可使读者在较短的时间内对计算机取证技术有比较系统、全面的了解，为进一步学习和研究打下良好的基础。

本书可作为高等院校计算机、信息安全等相关专业的教材或教学参考书，也可供公安网络监察、网络安全管理等领域的相关人员参考。

<<计算机取证技术>>

书籍目录

章节摘录

插图：第1章 计算机取证的基本概念随着信息技术的不断发展，计算机越来越多地参与到人们的工作与生活中，与计算机相关的法庭案例也不断出现。
一种新的存在于计算机及相关外围设备（包括网络介质）中的电子证据逐渐成为新的诉讼证据之一。
人们每天面对大量的计算机犯罪案例，如商业机密信息的窃取与破坏、计算机欺诈、对政府或金融网站的破坏等，这些案例的取证工作需要提取存在于计算机系统中的数据，甚至需要从已被删除、加密或破坏的文件中获取信息。
电子证据本身和取证过程存在许多有别于传统物证和取证的特点，它们对司法和计算机科学领域都提出了新的挑战。
2001年6月8日至22日，在法国图鲁兹城召开的为期5天的第十三届全球FIRST（Forum of Incident Response and Security Teams）年会上，入侵后的系统恢复和分析取证成为此次大会的主要议题。
由此可见，作为计算机领域和法学领域的一门交叉学科——计算机取证（Computer Forensics）正逐渐成为计算机安全领域一个新的研究热点。
在计算机犯罪手段与网络安全防御技术不断升级的形势下，单靠网络安全技术打击计算机犯罪不可能非常有效，因此需要发挥社会和法律的强大威力来对付网络犯罪，计算机取证正是在这种形势下产生和发展的，它标志着网络安全防御理论的成熟。
1.1 计算机取证的基本概念1.1.1 计算机取证的定义什么是计算机取证？
计算机取证资深专家Robbins给出了如下的定义：计算机取证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提取上。
计算机紧急事件响应组和取证咨询公司New Technologies进一步扩展了该定义：计算机取证包括了对以磁介质编码信息方式存储的计算机证据的保护、确认、提取和归档。
系统管理审计和网络安全协会SANS则归结为：计算机取证是使用软件和工具，按照一些预先定义的程序，全面地检查计算机系统，以提取和保护有关计算机犯罪的证据。

<<计算机取证技术>>

编辑推荐

《网络与计算机安全丛书·计算机取证技术》可作为高等院校计算机、信息安全等相关专业的教材或教学参考书，也可供公安网络监察、网络安全管理等领域的相关人员参考。

<<计算机取证技术>>

版权说明