

<<Windows取证>>

图书基本信息

书名：<<Windows取证>>

13位ISBN编号：9787030190376

10位ISBN编号：7030190378

出版时间：2007-6

出版时间：科学

作者：C.斯帝尔

页数：309

字数：379000

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>

<<Windows取证>>

内容概要

本书主要论述Windows系统平台的计算机取证问题，从理论、实践、技术等多角度进行详细阐述，给出了在目标机和分析工具方面均立足于Windows平台的操作指南，旨在为UNIX/Linux专家提供Windows操作系统中适合取证分析的工作步骤，为那些希望进入计算机取证世界的Windows专家们提供坚实的基础，让更多的取证爱好者得以借助本书进入Windows取证这个充满魅力和挑战性的领域。

本书主要读者对象为企业网络安全管理人员、网络（监察）警察、本科生、研究生、科研人员、教学人员和普通读者。

本书适合于在企业、高校内进行计算机取证人才培训，包括作为企业安全管理员和取证分析师培训教材，高校信息安全专业的本科生、研究生专业课教材，或计算机、信息技术等相关专业的本科生和研究生（尤其是工程硕士）等选修课教材。

<<Windows取证>>

作者简介

Chad Steel调查了300多起计算机安全事件，具有丰富的经验。在美国宾夕法尼亚州的工程师培养计划中，他作为兼职教师设立并承担了研究生课程“计算机取证”，并且为美国联邦和地方执法机关、商业客户和研究生提供取证分析方面的指导。他曾任一家全球百强企业的IT调查负责人

<<Windows取证>>

书籍目录

译者序 作者简介 出品团队致谢 第1章 Windows取证 1.1 企业计算机取证分析师 1.2 Windows取证 1.3 人、程序和工具 1.4 计算机取证：当前和未来 1.5 补充参考资源 第2章 处理数字犯罪现场 2.1 确认现场 2.2 执行远程调查 2.3 保护现场 2.4 记录现场 2.5 处理物理证据现场 2.6 处理数字证据现场 2.7 保管链 2.8 最佳证据 2.9 与执法机关共事 2.10 补充参考资源 第3章 Windows取证基础 3.1 历史和版本 3.1.1 MS-DoS 3.1.2 Windows 1.x、2.x和3.x 3.1.3 Windows NT和Windows 2000 3.1.4 Windows 95/98/Me 3.1.5 Windows xP/2003 3.2 非易失性存储器 3.2.1 软盘 3.2.2 磁带 3.2.3 CD和DVD 3.2.4 USB闪存驱动器 3.2.5 硬盘 3.3 补充参考资源 第4章 分区和文件系统 4.1 主引导记录 4.2 windows文件系统 4.2.1 FAT 4.2.2 VFAT 4.2.3 NTFS 4.3 补充参考资源 第5章 目录结构和特殊文件 5.1 windows NT/2000/XP 5.1.1 目录 5.1.2 文件 5.2 windows 9X 5.2.1 目录 5.2.2 文件 5.3 补充参考资源 第6章 注册表 6.1 历史 6.2 注册表基础知识 6.3 注册表分析 6.3.1 常规注册表键 6.3.2 文件夹位置 6.3.3 自启动项目 6.3.4 智能表单 6.4 高级注册表分析..... 第7章 取证分析 第8章 系统联机分析 第9章 取证复制 第10章 文件系统分析 第11章 日志文化分析 第12章 因物网使用分析 第13章 电子邮件调查 附录

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>