<<计算机取证调查指南>>

图书基本信息

书名：<<计算机取证调查指南>>

13位ISBN编号：9787562446484

10位ISBN编号：7562446482

出版时间：2009-1

出版时间：重庆大学出版社

作者：Bill Nelson

页数：529

前言

近年来世界范围内发生的重大事件，已经影响和改变了我们对于证据收集的思考方式。
2001年9月11日美国纽约世贸中心遭到袭击后不久，许多青年男女都自发地以不同的方式为国家效力。
没有参军的年轻人，则选择加入了执法和安全机构。
随着诸如CSI、罪案取证和NCIS等主流电视节目越来越受欢迎，加上国土安全问题重新被重视，使得对计算机取证领域方面的专家需求大增。
这种需求正通过在全美的大专院校甚至高中所开设的计算机取证专业课程来得以满足。

然而，计算机取证绝不是一门还处于探索阶段的新兴领域。
早在20世纪90年代，当时我在海军犯罪调查机构里担任特别调查员，就已经意识到个人电脑，更专业地说是无安全保障的个人电脑，给国家安全带来了潜在的威胁。
那时，我开始指导对白领犯罪、网络攻击，以及通信诈骗等案件的取证调查。
今天，大多数新的计算机取证专家可能会参与更广泛和更多样化的取证调查，包括反恐间谍活动、反洗钱、知识产权窃取、电子监视等问题。

不同的取证专家所必须具备的技能是不一样的。
最低限度来说，他们必须具备深厚的刑事司法体系知识、计算机硬软件系统知识、调查和证据收集规范方面的知识。
下一代的“电子侦探”将必须具备相应的知识、技能和经验，才能完成涉及多种操作系统和文件类型的、复杂的、数据密集型的取证调查工作。

<<计算机取证调查指南>>

内容概要

本书包括计算机取证调查所需的工具和技巧，解释了文档结构、数据恢复、电子邮件和网络调查以及专家证人的证词等主要问题。
除了可以学到基本的概念，读者还可以掌握处理数字调查证据和保存支持呈堂证据或者企业查询证据的实践知识。
主要特点：　　涵盖最新的两个正在着手调查的案例，一个企业案件和一个刑事案件。将所学的概念运用到真实世界中。
全面更新的技术内容，包括更多种类的取证调查软件和关于网络取证的最新一章内容。
功能广泛的学习工具，包括练习、贯穿全书的项目和案例，让学生能实践所学技能。

作者简介

Bill Nelson专门进行计算机取证调查工作长达8年之久。
他曾是犯罪用自动指纹识别系统的软件工程师。

<<计算机取证调查指南>>

书籍目录

章节摘录

术语“企业环境”是指大型企业的计算机系统，该系统可能包含一个或多个无关联的系统或者先前独立的系统。
在小型企业中，一个小组就可能完成调查三角形中所示的这些任务，或者一个小型企业与其他企业签订合同共同来完成这些任务。
当你在脆弱性评估和风险管理小组工作时，一定要测试并证明独立工作站与网络服务器的完整性。
此项完整性检验包括系统的物理安全及操作系统与运行的安全，这个小组的成员要对全网做测试，找出已知的操作系统和应用系统安全隐患。
该小组成员对网络、计算机工作站和服务器进行攻击，旨在评估其脆弱性。
一般来说，完成该任务的人员应具有多年在UNIX和Windows NT/2000/XP管理方面的经验。
脆弱性评估和风险管理小组中的专业人员还需具备网络入侵检测和事件响应方面的技能。
他们通过使用自动化软件工具和人工监控网络防火墙日志来检测入侵者的攻击。
当检测到攻击时，事件响应小组就对入侵者进行跟踪、定位和识别，并拒绝他／她进一步访问网络。
如果入侵者的攻击会造成重大或是潜在的破坏，响应小组则要收集必要的证据用来提起对入侵者的民事或刑事诉讼。
诉讼是在法庭上证明某人有罪或无罪的法律程序。
如果未授权用户正在访问网络，或任一用户正在进行非法操作，网络入侵检测和事件响应组就要通过定位或阻断该用户的访问来作出响应。
例如，一社区大学成员发送煽动性电子邮件给网络上的其他用户，网络组立刻意识到此电子邮件来自于本地网络上的一节点，于是派出安全组到节点所在地去。
在过去，脆弱性评估成员对高端计算机调查的贡献是非常大的。

<<计算机取证调查指南>>

版权说明