<<计算机数据分析技术与应用>>

图书基本信息

书名：<<计算机数据分析技术与应用>>

13位ISBN编号：9787560966137

10位ISBN编号：7560966136

出版时间：2010-11

出版时间：华中科技大学出版社

作者：凌彦 编

页数：392

前言

自1994年3月中国加入互联网始，计算机和互联网开始慢慢融入我们的生活。
经过近十五年的发展，计算机和互联网已经成为中国数以亿计网民生活中不可或缺的部分。
每天，我们都有数小时甚至更多的时间是在计算机前度过的，如通过互联网收发电子邮件、查询最新资讯、跟世界各地的朋友愉快交流以及进行其他的活动。
近年来，随着电子商务的发展成熟，电子货币广泛应用，计算机和互联网开始进入我们的实际生活，如电子银行、电子货币、虚拟货币等等。
然而，与方便快捷的计算机生活一同到来的是越来越多的计算机问题，比如，侵犯个人隐私、盗窃虚拟财产、病毒和木马攻击等等，我们用计算机犯罪来形容这类活动。
计算机犯罪是一种在虚拟空间、使用虚拟身份、通过虚拟手段来完成，但却可以在现实空间获得利益的犯罪方式。
正是由于计算机犯罪具有犯罪主体的专业化、犯罪行为的智能化、犯罪客体的复杂化、犯罪对象的多样化、犯罪后果的隐蔽化等特征，使其有别于传统的刑事犯罪。
此外，一旦发生计算机犯罪事件，对计算机犯罪证据的提取和展示也成为亟须解决的问题。
在对计算机犯罪进行司法调查的过程中，计算机数据分析技术起到了至关重要的作用。
计算机数据分析技术是全世界的计算机安全专家在长期同计算机犯罪分子进行信息安全较量的过程中，集思广益，由实战经验总结出来的计算机安全领域的一个全新分支。
计算机数据分析技术在中国已经发展了近十年的历史，在实际的案件调查过程中已经形成一套符合中国国情的计算机数据分析方法和流程。
但是，由于计算机数据分析技术形成晚、技术新，因此在涉及计算机犯罪案件分析调查的过程中，广大信息安全领域的技术人员还是存在诸多疑问，涉及调查的工具、调查的软件、调查的方法、调查的规范等等。
本书通过对计算机数据分析技术的简要介绍，结合实际生活中一些典型的计算机犯罪案例，对计算机数据分析技术在计算机司法调查分析过程中的应用做了阐述。
如何阅读本书：第1章和第2章用简要的篇幅，回顾了一下计算机硬件以及操作系统的结构，供刚参加计算机调查的人员参考。
第3章介绍了计算机犯罪概述以及一些理论知识，作为计算机数据分析的入门理论基础。

<<计算机数据分析技术与应用>>

内容概要

面对日趋严重的计算机犯罪，汁算机数据分析技术正变得越来越重要。
本书系统地阐述了计算机数字证据分析的基本概念、原理及方法，全书由l2章组成。
基础部分的内容包括了计算机系统基础知识、数据存储原理。
数据分析理论部分包括了计算机犯罪概述、数据分析内容和工作流程、调查现场的处理、数字证据固定技术。
数据分析技术部分主要以EnC。
s。
为例介绍了数据分析技术的实际应用以及如何编制计算机调查分析报告。
本书面向那些想深入了解计算机系统的工作原理，对计算机数据分析工作有兴趣的读者，也适用于计算机系统管理员、开发人员、安全专家等查阅参考。

<<计算机数据分析技术与应用>>

书籍目录

第1章　计算机系统基础知识　1．1　计算机硬件系统组成　1．2　计算机硬件系统启动过程　1．3　DOS系统启动过程　1．4　WindowsNT／2000／XP启动　1．5　系统分区原理　1．6　文件系统　本章总结第2章　数据存储原理　2．1　硬盘基础知识　2．2　硬盘的物理结构　2．3　硬盘的逻辑结构　2．4　硬盘数据的存储　本章总结第3章　计算机犯罪概述　3．1　计算机犯罪的概念和特征　3．2　电子证据的概念　3．3　电子证据的法律定位　3．4　电子数据的证据效力　3．4．1　电子数据的特性　3．4．2　电子数据的证据效力　本章总结第4章　计算机数据分析概述　4．1　什么是计算机数据分析技术　4．2　什么是电子数据鉴定　4．3　计算机数据分析的对象　4．4　电子数据分析的基本思路和手段　……第5章　计算机调查现场处理第6章　计算机证据固定技术第7章　计算机数据分析软件第8章　EnCase工作环境第9章　基础查找与书签数据第10章　文件签名与菜列分析第11章　EnCase高级功能第12章　计算机调查分析报告附录参考文献后记

章节摘录

插图：在检查服务器系统的时候要注意一下，有时，一个工作站可能运行着各种数据库服务器。
在家庭使用中很少会出现这种情况，但有些公司会这样做。
如果你怀疑有重要的应用程序在运行的话，必须执行一个正常的关机过程。
如果是拔下插头来关机的，应该把插头从计算机的背部拔下来。
如果你已经养成从墙上把插头拔下的，就可能会遇到一个情况，就是IJPS在工作着，如果在拔墙上的插头的话，将会触发LIPS发出一个关机信息。
所有的行为可能会被写入系统，触发潜在的破坏工作，而不是固定证据了。
请养成从计算机的背部把插头拔下的习惯。
与此类似，若尝试去关闭一台笔记本电脑，并把它的插头拔下的话，无论是墙上的插头，还是背部的插头，电池还是会正常工作的，因此必须同时把电池除下。
同时别忘记把电池和电源适配器一起带走。
最后，在关机计算机系统的时候，应该记录下所有的行为。
例如什么时间做的，做了什么，是如何处理的，及其这样做的原因是什么。
出于讨论的意图，假如你必须关机并捕获一个Windows2000专业版系统，它运行了一个大的基于SQL的商务业务应用程序。
当把插座拔下的时候，必须有更多的措施以保护突然断电带来的数据丢失问题。
在这个案例里，我们推荐正常关闭操作系统。
7.包装与封存一旦计算机已经关闭，这就要求打包与贴标签了。
在此之前，需要把所有在计算机尾部的线缆做一个标识，并且要给它们拍照。
如果已经在此之前把网络从计算机中移除，需要把它们重新连接起来。
在拍摄计算机的背部时，必须要把标签贴到电缆上，然后开始拍摄这一过程。
要标记一根电缆的连接，在它的终端的尾部都贴上标签，并把它放到相应的计算机的接口上。
对于每根电缆和每一个端口，使用唯一的字母来进行标识，从A开始，直接把所有的设备都贴上标签。
使用同样的方式，电缆A接在端口A上，电缆B接在端口B上。
从不同的角度拍摄计算机背部。
完成之后，把电缆移除，并且准备开始制作标签。
使用这种方法，可以显示计算机是如何进行连接的。
包装与标签的意图，就是给产品加上一个外壳。
打包可以使证据免遭破坏。
标签提供了把相关的证据进行标识的功能，可以指定日期、位置、时间、案件、事情和相关的机构。
标签也同时提供了流程监管的功能。
流程监管是一个对证据文件进行控制并且确保证据完整性，并提供给法庭的过程。

后记

计算机数据分析技术是近几年来新兴的一门犯罪调查前沿技术，受到了广大信息安全专家的关注，然而，由于国内计算机犯罪调查工作起步晚，目前计算机数据分析技术在一定程度上还落后于发达国家，尽管我们的网民数量远远高于发达国家。
计算机数据分析技术要快速发展，还需要广大信息安全专家和国内高科技企业共同努力。
计算机数据分析技术的发展同广大信息安全工作者的辛勤努力是分不开的，我们愿意同广大信息安全专家一起努力，为我们国家的信息安全事业贡献自己的力量。

编辑推荐

《计算机数据分析技术与应用》：高职高专教育法律类专业教学改革试点与推广教材

版权说明