网络与计算机安全丛书

计算机取证技术

殷联甫　编著

科学出版社
www.sciencep.com

网络与计算机安全丛书

计算机取证技术

殷联甫　编著

科学出版社
北京

内 容 简 介

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。

图书在版编目(CIP)数据

计算机取证技术/殷联甫编著. —北京：科学出版社，2008
（网络与计算机安全丛书）
ISBN 978-7-03-021529-1

Ⅰ. 计… Ⅱ. 殷… Ⅲ. 计算机犯罪—证据—调查—研究 Ⅳ. D915.13

中国版本图书馆 CIP 数据核字(2008)第 043341 号

责任编辑：任 静 王志欣 / 责任校对：陈玉凤
责任印制：刘士平 / 封面设计：耕者设计工作室

科 学 出 版 社出版
北京东黄城根北街 16 号
邮政编码：100717
http://www.sciencep.com

骏 走 印 刷 厂 印刷
科学出版社发行 各地新华书店经销
*
2008 年 6 月第 一 版 开本：B5(720×1000)
2008 年 6 月第一次印刷 印张：10 1/4
印数：1—3 000 字数：196 000

定价：30.00 元

（如有印装质量问题，我社负责调换〈环伟〉）

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与恢复等内容；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。作者的E-mail地址：ylf@mail.zjxu.edu.cn。

作　者

2008年2月

目　　录

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[1]。

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。

因此，计算机取证是指对能够为法庭所接受的、足够可靠和有说服力的、存在于计算机和相关外设中的电子证据的确定、收集、保护、分析、归档以及法庭出示

的过程。取证的目的是为了据此找出入侵者(或入侵的机器),并解释入侵的过程[2]。

计算机取证包括物理证据获取和信息发现两个阶段。物理证据获取是指调查人员来到计算机犯罪或入侵的现场,寻找并扣留相关的计算机硬件,物理证据获取是全部取证工作的基础,在获取物理证据时最重要的工作是保证取到的原始证据不受任何破坏。无论在任何情况下,调查者都必须牢记以下几点[3]:

(1) 不要改变原始记录。

(2) 不要在作为证据的计算机上执行无关的程序。

(3) 不要给犯罪者销毁证据的机会。

(4) 详细记录所有的取证活动。

(5) 妥善保存得到的物证。

信息发现是指从原始数据(包括文件、日志等)中寻找可以用来证明或者反驳什么的证据。为了保护原始数据,所有的信息发现工作都是在原始证据的物理拷贝上进行的,物理复制工作可以用 Unix 系统的 dd 命令或使用专用设备进行。一般情况下,取证专家还要用信息摘要算法(SHA-1 算法等)对原始证据上的数据作摘要,然后将原始证据和摘要信息及相关文档妥善保存。与其他证据一样,电子证据必须是真实、可靠、完整和符合法律规定的[3]。计算机取证不仅仅是计算机或网络的技术问题,还涉及法律和道德规范,同时需要计算机专家、执法官员和律师等多方人员的共同协作[4]。

1.1.2 计算机取证研究概况

1. 国外计算机取证研究概况

面对日益猖獗的计算机犯罪发展态势,如何加大计算机犯罪的打击力度,已成为世界各国普遍关心的问题。

2000 年 5 月,西方八国集团在法国巴黎举行了世界上首次以打击网络犯罪为主要内容的国际会议。2001 年 2 月,八国集团的司法和内务部长又在意大利召开会议,重点研究如何查找和确认那些将网络用作犯罪工具的罪犯们的犯罪行为。美国也颁布了一系列法律,目的在于为打击计算机犯罪提供法律依据,美国联邦调查局(FBI)设立了专门的计算机取证实验室,主要研究计算机取证的标准规范,为司法机关打击计算机犯罪提供技术支持。

在国外,尤其在美国等计算机技术较发达的国家,打击计算机犯罪已有二三十年的历史,在计算机取证方面积累了一定的经验,出现了许多专门的计算机取证部门、实验室和公司。1984 年,美国 FBI 和其他法律执行部门开始建立检查计算机证据的实验室。很多专门从事计算机取证的公司开发了许多非常实用的取

证产品，其中比较好的产品有以下几种。

（1）美国 Guidance 软件公司研制的 Encase 产品，它是一个 Windows 系统环境下用于犯罪数据收集和分析的系统，可在系统不关机的情况下，将系统的全部运行环境信息和数据生成一个映像文件，再对该文件进行分析，从而发现犯罪证据。

（2）美国计算机取证公司（Computer Forensics Ltd）开发的 DIBS 产品，它是一种数据镜像备份系统，使用独特的数据镜像和鉴定技术，确保了数据复制的绝对安全性和完整性。

（3）英国 Vogon 公司开发的基于 Windows、Macintosh 和 Unix 等系统的数据收集和分析系统 Flight Server，它可以将计算机犯罪现场中的计算机硬盘中的数据按扇区（包括坏扇区）进行复制，并生成一个物理映像文件，然后对该映像文件进行分析，从而辅助办案人员发现犯罪证据。

（4）美国 Sandstorm 公司开发的 NetIntercept 网络取证系统，它具有获取和分析网络数据以及数据恢复等功能，能产生详细的报告，可支持 60 多种网络协议。

国外各研究机构与公司所开发的计算机取证产品的功能主要覆盖了电子证据的获取、保全、分析和归档的过程。各研究机构与公司也都在进一步优化现有的各种工具和产品，提高利用这些工具进行电子证据收集、保全、鉴定和分析的可靠性和准确度，进一步提高计算机取证的自动化和智能化。

在计算机取证的程序和标准化研究方面，巴西学者 Marcelo Abdalla dos Reis 做了大量的工作，发表了多篇相关论文，并于 2002 年 7 月在美国夏威夷召开的第十四届 FIRST 技术论坛上提出了计算机取证协议和程序标准化的思想，指出标准化模型可分为合法标准和技术标准两类。合法标准包括合法原则和证据的法律规则；技术标准包括技术原则、分析策略、技术方案和解决方法。标准化模型如图 1.1 所示。

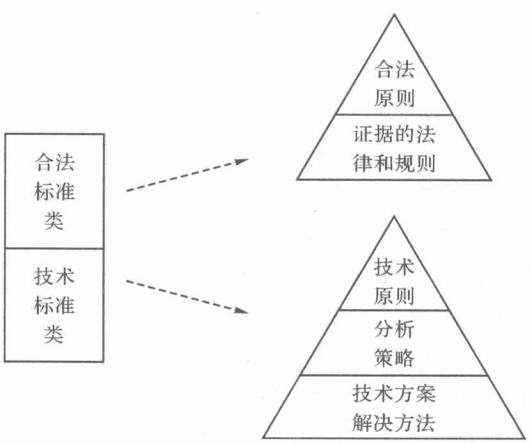

图 1.1　标准化模型

在学术界，最近每年都召开以计算机取证为主题的学术会议。1993 年和 1995 年、1996 年、1997 年分别在美国、澳大利亚和新西兰召开了以计算机证据为主题的国际会议，并最终成立了有关计算机证据的国际组织和电子证据科学工作组。另外，还有 SANS 主持的系统取证、调查和响应年会、FIRST 技术论坛年会等。国际著名的网络安全站点 SecurityFocus 也开辟了计算机取证专栏的邮件列表供全球从事计算机取证的研究人员讨论交流。从 2001 年在法国图鲁兹城和 2002 年在美国夏威夷召开的第十三届和第十四届 FIRST 技术论坛来看，在国外，计算机取证分析正日益成为计算机安全的重点课题。可以预见，计算机取证将是未来几年信息安全领域的研究热点[4~6]。

2. 国内计算机取证研究概况

在我国，近几年来，计算机证据开始出现在法庭审理中，有关计算机取证的研究与实践尚在起步阶段，只有少数法律法规涉及部分计算机证据，如《关于审理科技纠纷案件的若干问题的规定》、《计算机软件保护条例》等。目前，我国法庭案例中出现的电子证据还比较简单，仅有电子邮件、程序源代码等，不需要使用特殊的工具就能够获取。我国计算机取证工作的技术和水平与欧美发达国家相比存在相当大的差距。

首先，技术上还缺乏自主知识产权的优秀的计算机取证工具，许多企业和政府部门甚至金融系统的计算机和网络系统受到攻击造成重大损失时没法收集犯罪证据，使犯罪者逍遥法外。其次，在人们的意识当中，信息安全还仅仅停留在被动防护的层面上，只是尽量将自己的网络和数据保护好。因此，有必要鼓励 IT 从业人员跟上技术的发展，将信息安全提高到主动防护的高度，一旦发现入侵事件马上报告，并设法收集证据将犯罪者绳之以法。最后，由于计算机取证的高科技性，需要有专门的调查取证机构，同时还要颁布相关的法律法规来规范计算机取证，在这方面我们还有很多工作要做。

随着计算机和网络技术的不断发展，计算机犯罪的手段也在不断提高，严厉打击日益严重的计算机犯罪已迫在眉睫。目前，在广东、北京和上海等发达省市都已建立起专门打击计算机犯罪的网络警察队伍，在全国各省、市级公安机关也都有专门的部门处理计算机犯罪案件。但这些执法机关技术上还缺乏有效的工具，仅有的也只是利用国外一些常见取证工具或利用自身的技术经验，程序上还缺乏一套标准的计算机取证流程，提供给法庭的证据很容易遭到质疑[4,6]。

目前国内从事计算机取证产品研发的单位主要有深圳中科新业、上海金诺网安、上海盘石数码、北京天宇宏远、厦门美亚柏科等。目前国内比较成熟的计算机取证产品主要有中科新业开发的网络入侵取证系统、上海金诺网安开发的介质取证系统 DiskForen 和上海盘石数码开发的盘石计算机现场取证系统、盘石介质取

证分析系统、盘石手机取证系统等。

网络入侵取证系统是国家级重点课题，是由中科新业自主研发，并拥有自主知识产权和著作产权的新一代网络安全高端产品，该项目属国家级信息网络安全保障发展计划中的重点课题，对互联网的应用和普及起到关键的促进作用。

上海金诺网安开发的介质取证系统 DiskForen 是一个旨在对存储介质中的残缺数据进行恢复和勘查取证的系统，是国家“十五”重点科技攻关计划项目“打击计算机犯罪侦查技术研究”中的“存储介质中残缺数据的勘查取证技术”和国家高技术研究发展计划(“863”计划)“应急响应和事件恢复技术”中的“应急响应中的数据取证和恢复技术”的成果转化产品。DiskForen 系统可实现对各种介质和文件系统进行数据固定保全、恢复和分析取证等功能，系统具备良好的可视性和可靠性，并结合了有效的数字签名和灵活的报表分析功能，是国内具有自主知识产权的专业的数据恢复和勘查取证系统。

盘石计算机现场取证系统(SafeImager)由可以启动的光盘/U 盘、外接的数据存储设备构成，包括离线取证和在线取证。使用 SafeImager 光盘/U 盘启动对象计算机或者在对象计算机上直接运行 SafeImager 应用程序，可以快速有效地获取对象计算机上的数据，保存到外接的数据存储设备中。

1) 离线取证

通过光盘启动对象计算机，获取计算机中的硬盘/分区/目录/文件中的数据，同时生成有效的 MD5 数据校验码。

2) 在线取证

在目标系统运行或者不允许关机的情况下，获取目标系统内部的易失性数据，如系统运行信息、应用数据、内存信息、硬盘/分区等。

(1) 获取各种系统易失性信息，如网络、端口、进程等各类信息。

(2) 获取各种应用程序用户密码信息，包括常用邮件、聊天、浏览器、网络应用等。

(3) 获取应用数据信息，包括最近打开的文档、运行的程序、上网日志、Cookie 等信息。

(4) 系统内存获取。

(5) 整个硬盘的数据获取。

(6) 分区数据获取，包括加密程序加载的分区。

盘石介质取证分析系统(SafeAnalyzer)为执法部门提供全面、彻底的计算机数据分析、检查能力。它具有强大的数据恢复、过滤、分析、查找和报告功能，并提供简单易用的操作界面，是当前电子数据取证分析的首选工具，符合司法取证的需求。

（1）特性。

①自动进行系统分析：包括系统安装时间、操作系统版本、用户信息、网络配置信息、安装的程序、最后运行时间等，并可以选择性地纳入案件报告。

②文件过滤：系统缺省和自定义的过滤功能。

③时间线分析：通过设置时间区域，建立该区段修改、访问、创建的文件时间线，方便定位案件相关文件。

④删除恢复：文件系统中删除恢复、特征恢复。

⑤注册表分析：查看 Windows 的注册表文件，可根据系统缺省和自定义的注册表项目，快速定位浏览。

⑥关键词查找：各种编码格式的关键词查找，支持正则表达式。

⑦Web 分析：查看目标机器的浏览器历史、缓存记录、Cookie 信息和收藏夹等，支持缓存记录的预览和获取功能。

⑧报告生成：根据用户添加的书签和备注信息，生成案件报告。

（2）司法符合性。

①获取镜像生成 MD5 哈希校验值，并可随时校验。

②导出文件可以同时计算文件的 MD5 哈希。

③分析过程有详细的审计日志，便于案件的审查复核工作。

（3）支持的分区格式。

①NTFS。

②NTFS compressed。

③FAT 12/16/32。

（4）其他特性。

①支持 DD 镜像文件的直接分析。

②提供文件文本和十六进制查看功能，并可以直接查看扇区内的数据。

国内计算机取证学术活动主要有全国计算机取证技术研讨会和中国计算机取证技术峰会。2004 年 11 月在北京由北京人民警察学院、中国科学院软件研究所和北京市公安局网络信息安全监察处联合举办了首届全国计算机取证技术研讨会。2005 年 4 月 1 日在北京人民警察学院成立了中国电子学会计算机取证专家委员会并召开工作会议。几年来，除了学术专家的工作，由一群计算机信息安全、计算机取证技术爱好者自发组成的一个技术团体——中国计算机取证技术研究组，也活跃在我国计算机取证领域。该团体自 2005 年成立以来，每年在国内举办规模可观的中国计算机取证技术峰会，形成了中外专家、企业的交流论坛。中国计算机取证技术研究组的网址是 http://www.china-forensic.com。

1.2　电子证据的概念

1.2.1　电子证据的定义

计算机取证主要是围绕电子证据来展开工作的，目的是将存储在计算机及相关设备中的反映犯罪者犯罪的信息作为有效的诉讼证据提供给法庭。电子证据也称为计算机证据，是指在计算机或计算机系统运行过程中产生的、以其记录的内容来证明案件事实的电磁记录物。电子证据在计算机屏幕上的表现形式是多样的，尤其是多媒体技术的出现，更使电子证据综合了文本、图形、图像、动画、音频及视频等多种媒体信息，这种以多媒体形式存在的计算机证据几乎涵盖了所有传统证据类型。与传统证据一样，电子证据必须是可信的、准确的、完整的、符合法律法规的，即可为法庭所接受的[1]。

1.2.2　电子证据的特点

电子证据与其他种类的证据相比，有以下特点[1]：

1）表现形式的多样性

电子证据超越了以往所有的证据形式，不仅可以用文字、图像和声音等多种方式存储，还可以以多媒体的形式存在。

2）存储介质的电子性

电子证据依据计算机技术产生，化为一组组电子信息存储在特定的电子介质上，如计算机硬盘和光盘等。它的产生和重现必须依赖于这些特定的电子介质，而传统的证据（如笔录）则无需依赖于其他介质就可以独立重现，这点也正是电子证据的弱点，直接削弱了它的证明力度。因为，如果有人在电子介质上做手脚，如运用黑客手段入侵电脑网络，就能改变电子证据的本来面目，给证据的认定带来困难。

3）准确性

电子信息严格按照运行于计算机上的各种软件和技术标准产生和运行，其结果完全是“铁面无私”的机器对一组组二进制编码的运行结果，丝毫不会受到感情、经验等多种主观因素的影响。因此，如果没有人为的修改或毁坏，电子证据能准确地反映整个事件的完整过程和每一个细节，准确度非常高。

4）脆弱性

书面文件使用纸张为载体，不仅真实记录签署人的笔迹和各种特征，而且可以长久保存，如有任何改动或添加，都会留下“蛛丝马迹”，通过专家或司法鉴定等手段均不难识别。但电子证据使用电磁介质，储存的数据修改简单而且不易留下

痕迹，这导致了当有人利用非法手段入侵系统、盗用密码、操作人员误操作或供电系统和网络故障等情况发生时，电子证据均有可能被轻易地盗取、修改甚至全盘毁灭而不留下任何证据。它还容易被修改，比如，鉴定证据时，一旦不小心打开文件，那么文件的最近修改时间就会改变。电子证据的这种特点，使得计算机罪犯的作案行为变得更容易而事后追踪和复原变得更困难。

5）数据的挥发性

在计算机系统中，有些紧急事件的数据必须在一定的时间内获得才有效，这就是数据的“挥发性”，即经过一段时间后数据可能就无法得到或失效了，就像“挥发”了一样。因此，在收集电子证据时必须充分考虑到数据的挥发性，在数据的有效期内及时收集数据。表 1.1 描述了数据的挥发性。

表 1.1　数据的挥发性

数据	硬件或位置	存活时间
CPU	高速缓冲存储器，管道	数个时钟周期
系统	RAM	直至系统关闭
内核表	进程中	直至系统关闭
固定介质	swap/tmp	直至被覆盖或抹掉
可移动的介质	CD-ROM，floppy，HDD	直至被覆盖或抹掉
打印输出	硬拷贝打印输出	直至被毁坏

电子证据和传统证据相比，具有以下优点：

（1）可以被精确复制，这样只需对副本进行检查分析，避免原件受损坏的风险。

（2）用适当的软件工具（一般用信息摘要工具）和原件对比，很容易鉴别当前的电子证据是否有改变，数据中一个数据位的变化就会引起检验结果的很大差异。

（3）在一些情况下，犯罪嫌疑人完全销毁电子证据是比较困难的，如计算机中的数据被删除后还可以从磁盘中恢复，数据的备份可能会被存储在嫌疑犯意想不到的地方。

1.2.3　电子证据的来源

电子证据主要来自两个方面，一个是计算机系统方面；另一个是网络方面[6]。

来自计算机系统方面的电子证据主要包括：

（1）用户自建的文档（地址簿、E-mail、视/音频文件、图片影像文件、日程表、Internet 书签/收藏夹、数据库文件和文本文件等）。

（2）用户保护文档（压缩文件、加密文件、密码保护文件和隐藏文件等）。

（3）计算机创建的文档（备份文档、日志文件、配置文件、Cookies、交换文件、系统文件、隐藏文件、历史文件和临时文件等）。

（4）其他数据区中可能存在的数据证据（硬盘上的坏簇、其他分区、Slack 空间、计算机系统时间、被删除的文件、软件注册信息、自由空间、隐藏分区、系统数据区、丢失簇和未分配空间）。

（5）计算机附加控制设备（如智能卡和加密狗等）具有控制计算机输入/输出或加密等功能，这些设备可能含有用户的身份和权限等重要信息。

来自网络方面的证据主要包括：

（1）防火墙日志。

（2）入侵检测系统（IDS）日志。

（3）路由器日志。

（4）FTP、WWW 和邮件服务日志。

（5）实时聊天记录。

（6）网络监控流量以及其他网络工具所产生的记录和日志等。

1.3　计算机取证的原则和步骤

1.3.1　计算机取证的基本原则

实施计算机取证要遵循以下基本原则：

（1）尽早搜集证据，并保证其没有受到任何破坏。

（2）必须保证取证过程中计算机病毒不会被引入目标计算机。

（3）必须保证“证据监督链（chain of custody）”的完整性，也称为证据保全，即在证据被正式提交给法庭时必须保证一直能跟踪证据，也就是要能说明在证据从最初的获取状态到在法庭上出现状态之间的任何变化，当然最好是没有任何变化，还要能够说明证据的取证复制是完全的，用于复制这些证据的进程是可靠并可复验的，并且所有的介质都是安全的。

（4）整个检查、取证过程必须是受到监督的，也就是说，由原告委派的专家所作的所有调查取证工作，都应该受到由其他方委派的专家的监督。

（5）必须保证提取出来的可能有用的证据不会受到机械或电磁损害。

（6）被取证的对象如果必须运行某些应用程序，要确保该程序的运行只能影响一段有限的时间。

（7）在取证过程中，应当尊重不小心获取的任何关于客户代理人的私人信息，不能把这些信息泄露出去。

以上这些基本原则对计算机取证的整个过程都有指导意义。

1.3.2 计算机取证的一般步骤

国内有多位学者对计算机取证的一般步骤作了详细的归纳，将计算机取证过程划分为证据获取、证据分析和证据陈述三个阶段[1]。

1. 获取阶段

获取阶段保存计算机系统的状态，以供日后分析。这与从犯罪现场拍摄照片、采集指纹、提取血样或轮胎纹理等相类似。和自然世界里一样，并不知道哪些数据将作为证据，所以这一阶段的任务就是保存所有电子数据，至少要复制硬盘上所有已分配和未分配的数据，这就是通常所说的映像。在这一阶段中，可以利用相关的工具把可疑存储设备上的数据复制到可信任的设备上。这些工具必须尽可能少地更改可疑设备，并且复制所有数据，即要保证数据的完整性。为此在获取过程中要注意几点：

（1）获取数据前首先要咨询证人使用计算机的习惯。例如，他们是否为系统作了独立的备份？他们是否使用磁盘或光盘从系统上复制了一些信息作为备份或是其他目的之用？他们是否使用家用计算机查看过商务电子邮件？他们是否在家用计算机上办公过？他们将文档存储在什么地方？他们是否使用便携式计算机、PDA 或移动电话？

（2）可以通过询问来获取目标计算机网络上的相关信息。例如，处理的是何种类型的网络？网络是如何配置的？操作系统是什么？计算机的类型是什么？有哪些应用程序？使用的备份系统是什么类型的？磁带何时被重写？系统管理员是谁？是否存在远程访问？使用何种电子邮件包？是否使用了防火墙？是否有电子邮件服务器？谁是互联网服务提供者？

（3）咨询系统管理员和其他可能与计算机系统有关的人员，再次确保掌握了关于备份系统的所有信息和数据所有可能的存储位置。通常的办法是获取 6 个月到几年内的月备份磁带（或其他介质）。要切实掌握用于创建备份的硬件、软件的信息。为了从备份介质恢复数据，可以利用取证工具重新创建一个干净的环境。接着要获取所有备份的备份时间表副本，并了解该网络中写入什么日志，可能存在什么审计记录。因为用户本身可能对他们的行为可以跟踪的范围没有什么概念，但实际上审计记录可能说明何时何种人侵入到系统以及他们连接系统的时间和行为。也可以说明入侵者复制、打印、删除或下载的文件以及操作的时间。如果该公司使用了任何监控软件，可能提供大量的有用信息，如使用的程序、访问过的文件、雇员发送或接受的电子邮件和他们访问过的互联网站点的记录等。也可以发现安全通路是如何组织的，谁曾访问了那些文件和程序？谁有过只读访问而谁又执行了写操作？对这些相关个体，要记录下使用者姓名、登录名、密码和电