计算机犯罪证据的取证问题探讨

郑永红

（湖北警官学院，湖北　武汉　430034）

摘　要　计算机犯罪证据的提取与分析是侦办计算机犯罪案件的重点和难点。由于计算机证据本身的特点，取证过程及证据分析与传统物证差别较大，因此需要对计算机证据的提取与分析技术进行研究。从侦查工作的实际出发，对计算机证据的基本取证步骤、证据分析及证据审查等问题进行探讨。

关键词　计算机证据　证据提取　数据分析

中图分类号　DF794　　**文献标识码**　A　　**文章编号**　1001－7348(2003)02－144－01

随着信息技术的飞速发展，以计算机信息系统为犯罪对象和犯罪工具的各类新型犯罪活动成倍增长。犯罪主体的智能化，犯罪手段的多样化、复杂化，使计算机犯罪在现场保护和确定、证据的搜集和保全、证据的证明能力等方面明显区别于传统刑事犯罪。侦破计算机信息系统犯罪案件能否成功，取证是关键。大量的计算机犯罪取证需要提取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重获信息。因此，为有效控制计算机犯罪和侦破计算机犯罪案件，必须高度重视计算机犯罪证据的提取和分析技术。

1　计算机证据与计算机取证

1.1　计算机证据

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内容来证明案件事实的电磁记录物。与传统证据相比，它有如下特点：

(1) 脆弱性。计算机数据在人为因素作用下，极易发生改变，且不留下痕迹。即使在搜集计算机证据的过程中，由于技术或设备等原因，也可能对原始数据造成修改、破坏，甚至毁灭。

(2) 隐蔽性。计算机证据隐藏在繁杂的数据中，必须借助适当的工具读取。

(3) 混合性。计算机证据兼有书证、物证、视听资料等特点。

1.2　计算机取证

由于计算机证据的特殊性，计算机取证非常困难，如果方法不当或程序失误，就会导致证物毁损，资料无法读取，证据丧失证明能力。目前，作为计算机领域和法学领域的一门交叉科学的计算机取证，正逐渐成为研究和关注的焦点。

什么是计算机取证？Judd Robbins 先生定义为：计算机取证不过是简单地将计算机调查和分析技术应用于潜在的、有法律效力

我们采取了身份验证、保密通信、访问控制、库文加密等技术来加强其安全性。

(1) 身份验证。在执行真正的数据访问操作之前，我们要在分站点和主站点数据库服务器之间进行双向用户身份验证。如用户在登录分布式数据库时，或进行远程学生成绩传输时，都需要验证身份。

(2)保密通信。在身份验证成功后，就可以进行数据传输了，为了对抗报文窃听和报文重发攻击，需要在通信双方之间建立保密信道，对数据进行加密传输。因在远程教育分布式数据库系统中传输的数据量很大，为了节约加解密的时间，我们采用对称加解码算法来进行加解密。通常我们将这一过程和身份验证结合在一起使用。

(3)访问控制。在远程教育分布式数据库管理系统中，为了防止越权攻击，任何用户不能直接操作库存数据。用户的数据访问请求先要送到访问控制模块审查，然后系统的访问控制模块代理有访问权限的用户去完成相应的数据操作。用户的访问控制有两种形式：自主访问授权控制和强制访问授权控制。

(4) 库文加密。为了对抗黑客利用网络协议、操作系统安全漏洞绕过数据库的安全机制而直接访问数据库文件，我们还要对库文进行加密。我们采用 ANSI(美国国家标准协会) 颁布的数据加密标准 DES。DES 使用 64 位密码，算法实现在一小块集成电路芯片上以 1Mb/S 的运算速度处理密文。

4　结束语

远程教育作为一种新的教育模式，与计算机技术的发展有着密不可分的关系。对于一个实用的分布式系统而言，在考虑复杂性问题的同时，还需要考虑实际网络的通信状况，以提出可行的方案。信息的获取和系统的安全性问题只是其中两个最重要的问题，其余的许多问题还有待于我们进一步的研究和探讨。

参 考 文 献

1　王以和，涂小平．分布式数据库系统[M]．北京：电子工业出版社，1988

2　王鹏．大型分布式系统如何获取信息[J]．计算机世界报，2002(7)

3　曹红双，梁建军．ORACLE 分布式数据库远程数据访问的安全性[J]．微电脑世界，2002(7)

(责任编辑　胡俊健)

收稿日期：2002－06－20

的证据的确定与获取上。计算机紧急事件响应和取证咨询公司 New Technologies 将其定义扩展为：计算机证据包括了对以磁介质编码信息方式存储的计算机证据的确认、保护、提取和归档。SANS 公司则提出：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。

所以，计算机取证是指对能够为法庭接受的、足够可靠的和有说服性的、存在于计算机和相关外设中的电子证据的确认、保护、提取和归档过程。因此，广义的计算机取证应包括计算机犯罪证据的提取与分析。

2 计算机取证的基本步骤

由于计算机犯罪与传统犯罪不同，其行为人多受过一定教育和技术训练，且熟悉计算机技术，行为人作案后会想方设法利用计算机自身的特点，制造假象，隐匿或销毁罪证。因此，计算机犯罪的侦查与取证除按传统方法采用现场勘验、现场调查等常用侦查措施外，还应根据计算机数据证据的特点，采用特定的方式和技术进行计算机取证。其基本步骤是：

2.1 计算机取证的准备

(1)勘查保护外部现场。提取现场脚印、指纹、现场遗留物、监控器录相资料等，封存各类备份资料(备份程序、数据、打印材料、系统信息、日志、工作记录)，这些证据虽不直接与计算机发生联系，但很可能作为划定嫌疑人范围或嫌疑人同一认定的有力证据；提取与计算机犯罪相关的实物，如伪造、篡改的各种票证、文书，撕毁或烧毁的计算机打印结果，记录的残片、计算机磁盘残片等。

(2)绘制、拍摄现场图。绘制计算机犯罪现场图、网络拓扑图，对现场的计算机作案工具进行编号，为案件模拟和犯罪现场还原提供依据；拍摄计算机尾部的线路结构。如有必要，拍摄下计算机屏幕上显示的内容。

(3)访问相关人员。包括知情人(系统管理员、操作员、保安人员、现场人员等)、嫌疑人等。了解案发前后设备及系统运行状态、有无异常、有过何种相关操作、相关人员有无异常表现等。特别是在专用网络中，应用系统会因开发工具和人员的不同而存在差异，侦查人员必须取得证人或其他相关人员的配合协作，从他们那里初步了解操作系统、储存数据的硬盘位置、文件目录等等。

2.2 计算机数字证据的提取

计算机犯罪的手段复杂多变，遗留的计算机信息也各不相同，稍有经验的行为人会大量删除系统日志和相关文件，取证需要从隐蔽之处如未分配的磁盘空间、“slack”空间、临时文件、交换文件中获得和重建数据。虽然如此，就目前使用的静态取证技术来说，其基本的搜集提取程序主要包括保护数据、发现和获取数据。

保护数据的主要工作是：分析当前计算机的类型，看是否为多操作系统或隐藏的分区，有无可疑外设，有无远程控制、特洛伊木马程序，当前计算机系统网络环境；保护目标计算机系统，特别注意开机、关机环节，避免正在运行的进程数据丢失或存在不可逆转的删除程序，避免发生任何的改变、伤害、数据破坏、病毒感染；为保证在获取数据的同时不破坏原始介质，一般不用原始介质进行取证，而对原始介质进行按位拷贝、备份证据。

发现获取数据的基本步骤是：发现目标系统中的所有文件，包括现存正常文件、已删除但仍存在于磁盘上的文件、隐藏文件、受密码保护的文件和加密文件；尽可能全部恢复发现的已删除文件；最大程度地显示操作系统或应用系统使用的隐藏文件、临时文件和交换文件的内容；如果法律允许并有可能，访问被保护和加密文件的内容；在磁盘的特殊区域中，如未分配磁盘空间、文件中的“slack”空间发现所有相关数据。其中可能包含了先前文件遗留下来的信息，可能是有用的证据。

2.3 提取计算机证据应注意的问题

必须由 2 名以上的计算机安全监察警察进行提取操作，一般情况应邀请见证人；保证证据的连续性，保证证据从最初获取状态到法庭出现状态无变化，或能够清楚地说明其变化和原因；在数据提取过程中，不仅要依靠经验，还要借助一些相关的软件工具。

3 计算机证据的分析

在计算机犯罪侦查中，侦查人员往往要面对繁杂的计算机数据，如何从中分析辨别变动数据与正常数据，审查判断出与案件相关的、反映案件客观事实的计算机证据，也是计算机取证的重要内容。这项工作通常要运用专用的辅助分析软件工具对数据进行筛选，根据数据确定犯罪实施的过程，包括入侵的时间、使用的 IP 地址、修改的文件、增加的文件(后门、木马、病毒等)、删除的文件、下载和上载的文件等。

3.1 分析技术

在已经获取的数据流或信息流中寻找、匹配关键词或关键短语是目前的主要分析技术。主要有：文件属性分析技术；文件数字摘要分析技术；日志分析技术；根据已获得的文件或数据的用词、语法和写作(编程)风格，推断可能作者的分析技术；发掘同一事件的不同证据间联系的分析技术；数据解密技术；密码破译技术；对电子介质中的被保护信息强行访问技术等。

3.2 数据分析中应注意的问题

打印对目标计算机的技术分析结果，包括所有的相关列表和发现的文件数据。给出分析结论：系统整体情况；发现的文件结构；数据和作者的信息；在调查中发现的其它相关信息。对专业性较强的计算机数据出具必需的专家证明或鉴定书。

4 计算机证据的审查

由于计算机证据本身的特点以及计算机取证的复杂，计算机证据的审查是计算机犯罪案件侦查中不可缺少的一环，它贯穿于侦查工作的始终。

(1) 证据能力审查。审查计算机证据的取证合法性。包括计算机系统自身的安全性和工作过程的可靠性；取证程序、证据固定保全是否符合法定要求等。

(2) 证据的证明力审查。审查计算机证据的客观性和关联性，结合全案其它证据进行综合审查。计算机证据是否同其它证据相互印证、相互联系，建构成坚实可靠的证据体系，并据以认定案件的真实情况。

参 考 文 献

1 缪世淮．公安机关办理刑事案件程序规定的适用 [M]．北京：中国人民公安大学出版社，1998

2 刘广三．计算机犯罪论 [M]．北京：中国人民大学出版社，1997

3 胡振辽，孙晓东．计算机犯罪侦查途径的探讨[J]．网络安全技术与应用，2001(8)

4 许榕生，吴海燕．国际安全新课题：计算机取证[N]．中国计算机报，2001－08－02

(责任编辑 高建平)