计算机安全学的新焦点——计算机取证

何明 （中山大学电子与通信工程系 516030）

摘要：网络的普及使得计算机犯罪正成为目前刑事犯罪的新特点。但由于电子信息的易破坏性，法律取证成为制裁犯罪者的障碍。于是计算机取证技术应运而生。本文介绍了计算机取证技术的基本要求、方法及发展。

关键词：计算机犯罪 计算机证据 法律效力 原始性 完整性 可信性

1 引言

绚丽多姿的网络世界，就像希腊神话中的"潘多拉的魔盒"，在给人带来希望的同时，也释放出"飘过世纪的乌云"——计算机犯罪。1960年10月，唐·帕克在美国斯坦福研究院调查与计算机有关的事故时，发现一位工程师通过非法修改程序在存款余额上做了手脚。这是世界上首例刑事追诉的计算机犯罪案件。

其后，这一犯罪形式便日渐增多，其作案手段五花八门，犯罪方法形形色色，同时犯罪数量也迅速增长，由此造成的经济损失已达到触目惊心的地步。1988年，美国康奈尔大学计算机研究生莫里斯通过美国最大计算机网络系统，把自己设计的病毒程序输入五角大楼远景规划网络，导致美国军事基地和国家航空航天局的8500台计算机瘫痪，造成直接经济损失1亿美元。2000年2月8日到22日，Yahoo在经受了突如其来的"重磅拒绝服务"攻击之后，从股票上看，市值便损失了172亿美元。

据统计，在全球范围内，由于信息系统的脆弱性而导致的经济损失，每年达数亿美元，并且呈逐年上升的趋势。据美国《金融时报》报道，现在平均每20秒就发生一次入侵计算机网络的事件；超过1/3的互联网防火墙被攻破。

面对这种现实，各国政府和企业不得不开始重视网络安全。美国政府已经颁布了《计算机安全法》，日本颁布了《反黑客法》，我国也制定了相关的法律、法规。要定罪，就要收集证据。电子证据本身和取证过程的许多要求都有别于传统物证和取证方法，这对司法和计算机科学领域都提出了新的研究课题。2001年6月18—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科学——计算机取证(Computer Forensics)正逐渐成为人们研究与关注的焦点。

2 "计算机取证"的定义

"计算机取证"这个名词由International Association of Computer Specialists (IACIS)在1991年举行的第一次年会中正式提出，它是将计算机调查和分析技术应用于对存在于计算机和相关外围设备中(包括网络介质)的潜在的、有法律效力的电子证据的确定与获取。此确定和获取的过程是对电子证据的确认、保护、提取和归档的过程。概括地说，计算机取证是指对能够为法庭接受的、足够可靠和有说服性的、存在于计算机和相关外设中的电子证据的确认、保护、提取和归档的过程。

3 "计算机取证"的基本要求

由于计算机数据容易被篡改、伪造、删除，并且往往不留下任何痕迹，所以，人们对计算机数据的证明力有很大的怀疑，这给采用计算机数据作为证据造成了很大的障碍。为了使收集到的电子数据能成为证据，我们必须加强它的证明力，必须保证在其生成、存储及传递的过程中保持原始性、可信性和完整性，保证证据的连续性，这样才可能被法庭所接受。为了达到这个要求，在"计算机取证"过程中，要遵循下面的基本原始：

(1) 不要对原始数据进行直接分析。由于证据必须要求原始性，所以，Forensic技术的关键是要在不破坏原始介质的前提下，对所获得的数据进行分析，从而提取出有效证据。因此，在进行Forensic分析之前，必须对原始证据进行按位拷贝，然后对这个拷贝进行分析。

(2) 分析数据的计算机系统及辅助的软件必须保证安全、可信。如果不能保证分析数据的主机及使用的辅助软件的安全及可信，那么由此得出的证据也无法做到可信性了。

(3) 分析前对数据进行数字签名。因为电子信息很容易被更改、破坏，为了说明获取证据的原始性，我们必须对原始数据先进行数字签名，每做一个分析动作，都要再生成数字签名，以和分析前的比较，看是否有改变，这样就保证了获取证据的可信性。

(4) 必须对受破坏的计算机系统的原始状态、周围环境，分析时采用的方法、具体操作、产生的结果、分析的结果等进行详细描述，并将文件归档，这些文件都必须有人员的姓名、操作时间、地点等附加说明。这些文件可证明证据的连续性，即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，是获取的电子证据能具有法律效力的必备条件。

(5) 每一次分析完成，都要进行备份。

(6) 必须对获取的证据妥善保存，不能存在使它发生损坏、更改等失去法律效力的事件。

4 "计算机取证"的基本分析方法

虽然，计算机犯罪的形式千变万化，可能遗留的痕迹也多种多样，但总有一套可以遵循的基本分析方法，"计算机取证"的流程一般为：保护数据、分析数据、抽取证据。

4.1 保护数据

(1) 对现场的环境、计算机配置、出现的情况等信息要详细记录在案。

(2) 对受破坏的计算机介质进行按位拷贝，即所有隐藏的、交换的、被删除的、正常的、空白的，未被使用的文件系统都包括在备份中。这个备份是原始数据的"克隆"，连1个bit的差异都不存在。

4.2 分析数据

(1) 在一个"安全"的系统里对备份进行分析，这里的"安全"是指此系统没有任何病毒，没有安装任何不被授权的软件，同网络已完全断开，不会接受任何不被授权的人的访问。

(2) 寻找目标系统中的所有文件，包括现在的正常文件、已经删除但仍存在于磁盘上(即还没有被新文件覆盖)的文件、隐藏文件、受到密码保护的文件和加密文件。

(3) 全部或尽可能地恢复发现的已删除文件，通常，一个入侵者会删除那些会暴露自己的文件，因此，恢复这些文件无疑是一个很重要的工作。

(4) 最大程度地显示操作系统或应用程序使用的隐藏文件、临时文件、交换文件、缓存里的文件的内容。

(5) 如果可能并且法律允许，访问被保护或加密的文件内容。

(6) 分析在磁盘的特殊区域中发现的所有相关数据。特殊区域至少包括下面两类：① 所谓的未分配磁盘空间——虽然目前没有被使用，但可能包含有先前的数据残留；② 文件中的slack空间——如果文件的长度不是簇长度的整数倍，那么分配给文件的最后一簇中，会有未被当前文件使用的剩余空间，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。

(7) 按照时间属性对文件进行排列。文件的时间属性包括：文件的最近一次访问时间、文件的最近一次修改时间、文件的创建时间。查看在怀疑的作案时间内，有哪些文件被修改、添加、访问。

4.3 抽取证据

(1) 根据数据重建犯罪过程：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。

(2) 打印对目标计算机系统的全面分析结果，包括所有的相关文件列表和发现的文件数据，然后给出分析结论：系统的整体情况，发现的文件结构、数据和作者的信息，对信息的任何隐藏、删除、保护、加密企图，以及在调查中发现的其他的相关信息。

(3) 给出必要的专家证明

5 计算机取证技术的现状及发展

目前普遍采用的计算机取证技术是一种静态方法，在事件发生后对数据进行提取、分析，抽取出有效的计算机证据。美国和英国的一些安全公司提供了很多基于这种思想的工具，包括数据"克隆"工具、数据恢复工具、数据分析工具，如：这种方法比较费时，而且对取证人员的要求比较高，需要有耐心，熟悉各种操作系统和计算机犯罪方法，还要有非常强的逻辑分析能力，能找出大量数据之间的联系，把从不同侧面证明犯罪过程的证据整合起来。

随着计算机犯罪技术的提高，单凭这种事后的静态取证已无法适应要求，发展趋势是将计算机取证结合到入侵检测等网络安全工具和网络体系结构中，进行动态取证。就象监视器，能识别可疑活动，保存现场记录，可以回放整个犯罪过程。这种方法能迅速生成计算机证据，减少调查的时间和降低对取证人员的要求。

动态取证的技术难点是：如何让记录设备旁路在网络中，对用户和黑客而言都是透明的，既不影响用户任何应用的运行效率，又采用了各种自我保护措施，避免审计设备本身遭到可能的攻击，保证取证系统自身的安全；其次，大流量信息的获取所需要的记录速度与记录空间的设计；再就是，如何保证这些记录满足证据的要求，即：原始性、可信性和完整性，使得法律部门可根据这些记录分析出时间、部位、行为及有关的犯罪证据来。

6 我国"计算机取证"的现状

目前我国刑法中的第285、286、287条对计算机犯罪的定刑做了规定，另外还有《中华人民共和国计算机信息系统安全保护条例》、《中华人民共和国计算机信息网络国际联网管理暂行规定》等法规，但对于计算机证据的相关要求并没有详细的规定，使得法律上的可操作性不强。目前，法庭案例中出现的计算机证据都比较简单，如电子邮件、程序源代码等，都是不需要使用特殊的工具就能够得到的信息，这种简单的证据获取方式已不能适应现在计算机犯罪的发展。所以我们必须制定、完善相关的法律法规，对计算机证据的收集、运用、判断进行规范要求，积极对相关司法人员进行计算机取证技术培训，同时还要自主开发相关的计算机取证工具，以适应社会的快速发展，使日益增加的计算机及网络犯罪受到应有的制裁。

One new focus of the computer security —— Computer Forensics

何明 （中同大学电子与通信工程系 516030）

参考文献

1 许榕生等，国际安全新课题计算机取证，中国计算机报，2001，8。

2 网威博士，计算机取证原则和步骤，中国计算机报，2001，11。

3 Computer Forensics Definifions，http://www.forensics-intl.com/define.html。