计算机取证技术研究

Research on Computer Forensics

殷联甫（嘉兴学院信息工程学院 314001）

摘要：本文首先介绍了计算机取证的基本概念、发展历史及国内外研究概况，然后给出了计算机取证的基本步骤和一个具体的计算机取证实例，最后说明了目前计算机取证尚存在的问题及发展趋势。

关键词：计算机犯罪 计算机安全 计算机取证

1 什么是计算机取证

计算机取证也称数字取证、电子取证，是指对计算机入侵、破坏、欺诈、攻击等犯罪行为，利用计算机软硬件技术，按照符合法律规范的方式进行识别、保存、分析和提交数字证据的过程。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[3]。

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[2]。无论在任何情况下，调查者都必须牢记以下几点[2]：

(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 MD5 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。与其它证据一样，电子证据必须是真实、可靠、完整和符合法律规定的[2]。计算机取证不单单是计算机或网络的技术问题，还要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]。

2 计算机取证的历史及国内外研究概况

计算机取证这一术语是 1991 年在美国召开的国际计算机专家会议上首次提出的，近几年每年都有相关的国际会议召开。许多国家相继出现了许多专门的计算机取证部门、实验室和咨询服务公司，并有一些产品问世。如美国 Guidance 软件公司研制的 Encase 产品，它是基于 Windows 系统用于法庭数据收集和分析的系统，可将正在运行的系统在不停机的情况下，将系统的全部运行环境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；英国 Vogon 公司开发的基于 PC 、Mac 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逐个扇区（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；美国的 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 多种网络协议的数据格式。国外各研究机构与公司所开发的产品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产品，提高利用其进行电子证据收集、保全、鉴定、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。

在我国，有关计算机取证的研究与实践尚处于起步阶段。目前，全国各省市级公安机关已建立了专门打击计算机犯罪的执法机构。但这些执法机构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自身的技术经验，程序上还缺乏一套计算机取证的流程，提供给法庭的证据很容易遭到质疑。因此急需有效组织社会资源，加强打击计算机犯罪的技术研究。目前在研的项目主要有国家 863 项目子课题——电子物证保护与分析技术；中科院高能物理研究所计算中心主持了国家网络安全课题——网络安全入侵取证系统，并于 2002 年 10 月在深圳举行的第四届高交会和 2002 年 12 月上海的网络安全论坛上，推出了一部“取证机”的模拟机器，称为网络安全入侵取证系统，该系统可将局域网络上的所有数据安全地保存在取证机上，事后向人们提交分析报告，作为法庭上的呈堂证据[4]。

总之，我们国家在计算机取证研究方面起步较晚，有许

多工作需要大家努力去做。

3 计算机取证的基本步骤

计算机取证一般包括数据保护、数据分析和证据抽取三个步骤[5]。

3.1 数据保护

(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) 对被破坏的计算机介质进行按位拷贝,即所有隐藏的、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 的差异也不存在。

3.2 数据分析

(1) 在一个"安全"的系统里对备份进行分析,这里的"安全"是指系统没有任何病毒、没有安装任何未授权的软件,与网络已完全断开,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、已经删除但还存在于磁盘上的文件、隐藏文件、受到密码保护的文件和加密文件;

(3) 全部或尽可能多地恢复已发现的"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,恢复这些文件是一件很重要的工作;

(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、缓存中的文件的内容;

(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。特殊区域至少包括以下两类:一类是所谓的未分配空间——虽然目前没有被使用,但可能包含有先前的数据残留;另一类是文件中的 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:文件的最后一次访问时间、文件的最后一次修改时间、文件的创建时间等。查看在怀疑的作案时间内,有哪些文件被修改、添加和访问。

3.3 证据抽取

(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相关信息;

(3) 给出必要的专家证明。

4 计算机取证的常见工具

一个好的取证工具可以使取证过程更容易,下面介绍一些常见的计算机取证工具。

4.1 Encase

Guidance Software 是计算机取证工具的主要开发商之一,它的客户包括美国国防部、财政部等。Guidance Software 的 Encase 软件在运行时能建立一个独立的硬盘镜像,而它的 FastBloc IDE 工具则能从物理层阻止操作系统向硬盘上写数据。Encase 软件包括 Encase 取证版解决方案和 Encase 企业版解决方案。

(1) Encase 取证版解决方案。Encase 取证版解决方案是国际领先的受法院认可的计算机调查取证的工具。它具有直观的图形界面,用户可以方便地管理大量的电子证据和查看所有的相关文件,包括"已删除"的文件、文件碎片和未分配的磁盘空间。

(2) Encase 企业版解决方案。Encase 企业版解决方案(Encase Enterprise Edition,简称 EEE)是世界上第一个可以有效执行远程企业紧急事件响应(Response)、审计(Audit)和发现(Discovery)任务的解决方案。计算机紧急事件响应工作组(CERT)和计算机调查员可以利用 EEE 即时通过局域网或广域网识别、预览、获取和分析远程的电子媒介。

(3) FastBloc IDE 工具。FastBloc IDE 是目前市场上最先进的阻止硬盘写数据的工具。FastBloc IDE 有以下特性:通过 IDE 信道相连,无需 SCSI 控制器卡或 SCSI 驱动器;与内置 CD-ROM 驱动器的高度和宽度相同,可以快速连到一台取证计算机上;体积小,便于携带和使用。

4.2 SafeBack

SafeBack 是颇具历史意义的电子证据保护工具,它是世界上惟一的处理电子证据的工业标准。它的主要用途是保护计算机硬盘驱动器上的电子证据,也可以用来复制计算机硬盘驱动器上的所有存储区域。

SafeBack 对硬盘驱动器的大小和存储能力没有限制。它可以对硬盘驱动器上的分区创建镜像备份,也可以对整个物理硬盘(可能包含多个分区和/或操作系统)创建镜像备份。SafeBack 创建的备份映像文件可以被写到任何可写的磁存储设备上,包括 SCSI 磁带设备。SafeBack 可以保护已备份或已拷贝的硬盘上的所有数据,包括未激活或"已

删除"的数据。

4.3 NetMonitor

NetMonitor 网络信息监控与取证系统是针对 Internet 开发的网络内容监控系统，它能够记录网络上的全部底层报文，监控流经网络的全部信息流，提供 WWW、TELNET、FTP、POP3 和 UDP 等应用的重组，可根据用户特定需求实现对其他应用的分析和重组，是网络管理员监测黑客攻击、维护网络运行安全的有力助手。

NetMonitor 网络信息监控与取证系统采用系统前台监测数据、后台分析数据等技术手段。前台系统负责监测 IP 协议数据包，可以根据特定配置截取网上数据流，并以文件的形式记录下来。后台系统则以指定形式和设定的过滤规则来分析、组合前台系统所记录的数据包，形成可直接查看的原始数据流和取证文件。

NetMonitor 网络信息监控与取证系统还提供远程管理能力，用户可在远程启动、关闭前台监测系统和后台数据分析系统，并观看监测数据和取证文件。

4.4 TCT

TCT 是 Earthlink 网络的 Dan Farmer 和 IBM 公司的 Wietse Venema 研究员为了协助计算机取证而设计的软件包，适用的操作系统包括 Solaris、FreeBSD、Linux 等。它有 4 个主要组成部分：grave－robber、unrm&lazarus、mactime 和一组小工具（ils、icat、pcat、file 等）[2]。

grave－robber：信息收集，主要用来收集索引节点的信息；

unrm&lazarus：恢复被删除的文件，包括隐藏文件；

mactime：读取并且报告系统中所有文件的 MAC（Modification /Access /Change，简称 MAC）时间；

ils：显示被删除的索引节点的原始资料；

icat：取得特定的索引节点对应文件的内容。

5 一个完整的计算机取证实例

为了使大家对计算机取证过程有一个感性的认识，下面给出一个完整的计算机取证的实例，该实例是华盛顿大学计算机安全服务小组资深专家 Dave Dittrich 对被入侵的计算机系统进行取证的全过程。取证过程分为以下几个步骤[1]：

5.1 冻结现场

Dave Dittrich 在有充分的证据表明计算机系统已经受到入侵时，马上切断系统电源。正常情况下，Unix 系统是用 shutdown 命令来关机的，但当计算机系统受到入侵后，计算机系统会受入侵程序的欺骗，在 shutdown 过程中删除某些文件，从而销毁入侵证据。因此，为了保护现场，必须马上切断系统电源。

但是，马上切断系统电源可能会丢失以下信息：没有写盘的数据缓冲区中的数据、进程空间的数据、内核空间的数据以及交换空间的数据等等。作为补救措施，在切断系统电源之前可通过以下操作来获取尽可能多的证据：

last，w，who

获取当前登录的用户以及以前登录过的用户的详细信息。

ls －lat

获取 /dev 目录、根目录和某些怀疑目录中的文件的详细信息。

ps aux，ps elf

获取当前系统中所有进程的详细信息。

lsof

获取当前所有打开的文件句柄的详细信息，从中可以发现某些后门、嗅探器等等。

5.2 保存证据

切断系统电源以后，Dave Dittrich 马上拆下被入侵计算机上的原始硬盘，然后在另一台机器上（该机器上安装的操作系统版本必须与被入侵计算机上的完全相同，而且原始硬盘只能以只读方式安装在该机器上）对原始硬盘进行物理拷贝（Unix 系统中进行物理拷贝的实用程序是 dd），用 MD5 对原始硬盘上的数据做摘要，然后保存好原始硬盘和摘要信息[1][2]。

5.3 取证分析

Dave Dittrich 将物理拷贝的磁盘以只读方式安装在取证分析机上。首先他用标准 Unix 工具进行分析，当他在检查 /etc /passwd 文件时发现了几个可疑的帐户：帐户"y"使用了 home 目录 /tmp，另一个帐户"x"使用根文件系统，因此，他决定对这二个帐户中的文件进行检查：

```
# ls －lat /mnt/tmp
total 156
drwxrwxrwt 6 root root 1024 May 1 04:03 .
－r－－r－－r－－ 1 root gdm 11 Apr 29 14:17
.X0－lock
drwxrwxrwt 2 root gdm 1024 Apr 29 14:17 .X11
－unix
drwxrwxrwt 2 xfs xfs 1024 Apr 29 14:17 .font
－unix
drwxr－xr－x 25 y root 1024 Apr 28 23:47 ..
drwx－－－－－－ 2 user1 user1 1024 Apr 26
17:36 kfm－cache－500
－rw－rw－r－－ 1 user1 user1 12288 Apr 26
16:37 psdevtab
```

```
drwxrwxrwt 2 root root 1024 Apr 21 11:12 .
ICE-unix
-rwx------ 1 root root 138520 Apr 20
20:15 .fileMFpmnk
```

他发现上面最老的那个文件(指文件 fileMFpmnk)有点异常,至少看起来不太熟悉,非常值得怀疑。因此,他接下来开始分析嵌在该程序中的字符串:

```
# strings - /mnt/tmp/.fileMFpmnk
...
ftpd
:aAvdlLiop:P:qQr:sSt:T:u:wWX
bad value for -u
option -%c requires an argument
unknown option -%c ignored
...
VirtualFTP Connect to: %s [%s]banner
logfile
email
/var/log/xferlog
connection refused (server shut down) from
%s
%s FTP server shut down -- please try a-
gain later.
%s FTP server (%s) ready.
%s FTP server ready.
FTP server ready.
...
FTP LOGIN REFUSED (already logged in as
%s) FROM %s, %s
Already logged in.
/etc/ftphosts
FTP LOGIN REFUSED (name in %s) FROM %
s, %s
anonymous
FTP LOGIN REFUSED (anonymous ftp denied
on default server) FROM %s, %s
FTP LOGIN REFUSED (ftp in denied - uid)
FROM %s, %s
/etc/ftpusers
...
...
```

上面的字符串说明这可能是一个 FTP 服务器,名为 ftpd 或 in.ftpd,……。

通过一系列分析 Dave Dittrich 最后得到了黑客安装 rootkit 的证据,并且找到了被安装的黑客工具。为了了解更详细的信息,Dave Dittrich 接下来用 TCT 工具进行分析。他使用 mactime 工具对系统中所有文件按 MAC 时间进行排序,并且使用 unrm 恢复出所有被删除的文件。随后,他开始从大量的数据中寻找入侵线索。最后,Dave Dittrich 将所有的发现汇总起来形成了最终的分析报告[1][2]。

5.4 提交分析报告

在这份报告中,Dave Dittrich 根据一些敏感文件被修改的时间确认了入侵者首次成功进入系统的时间以及以后每次登录的时间和进行的操作。从恢复出来的日志文件中,他找到了入侵者登录时使用的 IP 地址以及以后入侵者编译和安装黑客软件的证据。

6 计算机取证尚存在的问题及发展趋势

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。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满足要求,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,能识别可疑活动,保存现场记录,并且可以回放整个犯罪过程。这种方法能迅速生成计算机证据,减少调查时间,同时对取证人员的要求也可以降低。

另外,利用无线局域网和手机、PDA、传真等无线终端设备进行计算机犯罪的案件逐年上升,如何在无线环境中进行取证分析也是今后的研究方向。同时,结合人工智能、机器学习、神经网络和数据挖掘等技术开发新的取证工具或软件,使取证工具能有效地挖掘出潜在的信息,也是计算机取证今后的研究方向之一。

参考文献

1 Dittrich D. Basic steps in forensic analysis of Unix systems.2003。
http://www.staff.washington.edu/dittrich/misc/forensics/

2 王玲、钱华林,计算机取证技术及其发展趋势,软件学报,2003,14(9):1635~1644。

3 钱桂琼、杨泽民、许榕生,计算机取证的研究与设计,计算机工程,2002,28(6):56~58。

4 赵小敏、陈庆章,计算机取证的研究现状及趋势,网络安全技术与应用,2003,9:32~35。

5 何明,计算机安全学的新焦点—计算机取证,计算机系统应用,2002,7:42~43。