计算机取证的工具体系

陈祖义[1, 2]，龚俭[1]，徐晓琴[1]

（1.东南大学计算机系 江苏省计算机网络技术重点实验室 南京 210096；
2.空军第一航空学院 信阳 464000）

摘要：计算机取证调查成功与否在很大程度上取决于收集、保存和处理证据的取证工具。本文具体介绍了计算机取证所需的工具集，对相关的工具进行了比较，重点阐述了数据获取工具，介绍了取证工具的国内外发展现况，最后指出了取证工具的发展趋势。

关键词：计算机犯罪 电子证据 计算机取证 取证工具

the Tool Set of Computer Forensics

Chen Zuyi[1, 2], Gong Jian[1], Xu Xiaoqin[1]

（1.Department of Computer Science & Engineering, Southeast University, Key Lab of Computer Network Technology Jiangsu Province, Nanjing, 210096；2.the First Aviation College of the Air Force, Xinyang 464000）

【Abstract】 the success of the investigation of computer crime depends largely on the tools which collect, preserve and deal with the evidence. This paper introduces the state-of-art of computer forensics toolkits with the evidence collecting tools being emphasized. These tools are compared, and their development trends are prospected.

【key words】Computer crime，Digital evidence，Computer forensics，Forensics tools

1．引言

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[1]。由于计算机取证科学是一门综合性的学科，涉及到磁盘分析、加解密、图形和音频文件的分析、日志信息挖掘、数据库技术、媒体介质的物理分析等，如果没有合适的取证工具，依赖人工实现就会大大降低取证的速度和取证结果的可靠性。随着大容量磁盘和动态证据信息的出现，手工取证也是不可行的。所以计算机取证工作需要一些相应的工具软件和外围设备来支持。在计算机取证过程中最重要的是要学会运用一些软件工具。这些工具既包括操作系统中已经存在的一些命令行工具，还包括专门开发的工具软件和取证工具包。调查取证成功与否在很大程度上取决于调查人员是否熟练掌握了足够的、合适的、高效的取证工具。

2．取证工具的选用

取证工具通常按照调查取证的流程来分类（见图 1），其中数据获取和分析工具是计算机取证工具包中最基本、最重要的工具。在选用现有的系统命令和工具软件作为取证工具之前，首先要验证所选用的工具能否满足要求，即需要准确地核实工具的用途；判定它的输出是否可信；以及确定如何操作这个工具。这种验证对于确保计算机系统内部信息的正确提取十分重要。

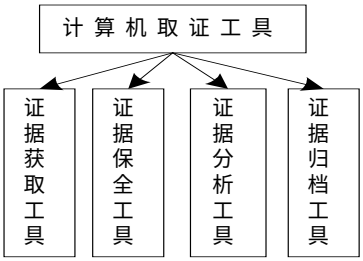

图 1 计 算 机 取 证 工 具 设 计 模 型

计算机取证有业余和专业的之分，业余的取证可以找到犯罪的根源和动机，以确保同样的事情不再发生。它是系统管理和应急响应的延伸。取证的目的不同，对取证所使用的工具要求也会不一样。

3．证据获取工具

数字证据主要来自两个方面，一个是主

作者简介：陈祖义（1974～），男，硕士生，研究方向为网络安全；龚俭，教授，博导，研究方向为网络安全，网络管理；徐晓琴，硕士生

机系统方面的，另一个是网络方面的。证据获取工具就是用来从这些证据源中得到准确的数据。计算机取证的重要原则是，在不对原有证物进行任何改动或损坏的前提下获取证据，否则证据将不被法庭接受[2]。为了能有效地分析证据，首先必须安全地、全面地获取证据，以保证证据信息的完整性和安全性。证据获取工具的体系结构如图 2 所示。

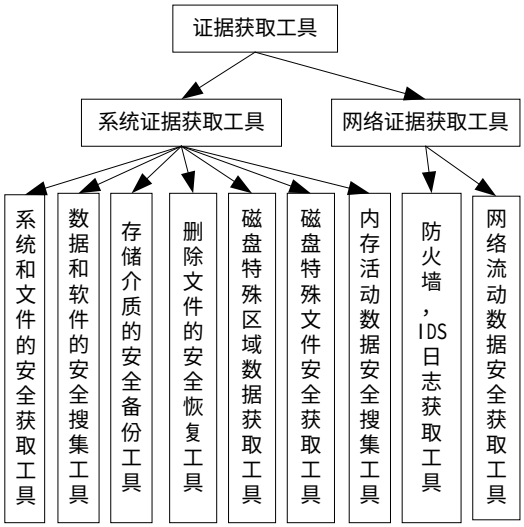

图2　证据获取工具的体系结构

3.1 计算机系统和文件的基本信息获取工具

保护现场是计算机调查取证工作中很重要的一步，通常需要根据受害系统的性质和安全管理的政策规定来决定是让可疑计算机继续运行，还是立即拔掉电源，或者进行正常的关机过程。在互联网入侵案件中，如果未对计算机取得一个映像之前切断网络或关机，就有毁掉所有可能的证据的危险。表一列出了常用的工具。

表一　计算机系统和文件的基本信息的获取工具

工具	作用
Last	列出用户注册和注销系统的基本信息
W	列出系统中活动用户的基本信息
Who	列出系统中正登录的用户基本信息
Lastcomm	列出系统中最近执行的shell命令
Ls	列出系统的文件、目录信息
Lsof	列出最近被系统打开的文件
Ps	列出系统中当前运行的进程
Find	列出某时间后被修改过的文件和目录

3.2 磁盘映像工具

在分析证物时最好使用原始证物的精确拷贝。取证意义上的备份必须是对原始驱动器每一个比特的精确克隆。因为一般的备份程序只能对单个的文件系统作备份，它无法捕获闲散空间、未分配区域以及 Swap 文件。只有逐位拷贝才能建立整个驱动器的映像，才可以确保得到所有可能需要的数据，例如已被删除或隐藏的文件。获得精确备份的最好方法是应用磁盘映像工具。一个适用的磁盘映像工具应该能够：进行位流复制或者是对磁盘或分区做映像；在映像时不改变原始磁盘的内容；既可以访问 IDE 磁盘也可访问 SCSI 磁盘；校验磁盘映像文件；记录 I/O 错误；提供全面的文档；有很快的映像速度；提供压缩能力等特性[3]。表二是常用的磁盘映像工具的比较。

表二　常用的磁盘映像工具比较

性质 / 工具	映像文件校验方式	可映像的介质	磁盘接口	复制的方式
Safe Back Version 3.0	CRC checksum	Hard drive, tape，removable media	IDE	Sector-by-sector
SnapBack DataArrest	MD5 checksum	Hard drive, tape，removable media	SCSI	Sector-by-sector
Linux “dd” Version 7.0	MD5 checksum	Hard drive, tape，removable media	SCSI IDE	Sector-by- sector file-by-file
DIBS PERU	DIVA	Optical media	SCSI IDE	Sector-by sector

3.3 磁盘擦除工具和反删除工具

把映像文件存放到分析机的存储介质之前，必须确保分析机器的存储介质里没有包含任何残留数据，因为这些残留数据可能对取证造成干扰。只是简单地删除或格式化存储介质是不够的，有一些专门程序可以系统地对存储介质的每一个扇区的数据进行清除，比如 NTI 公司的 DiskScrub 工具 [4]。计算机犯罪往往在入侵后将自己残留在受害方系统中的“痕迹”擦除掉，取证人员就必须把这些被删除的关键信息恢复出来。TCT 是一套用于恢复已被删除 UNIX 文件的工具，包括从比特流重新构造一系列连贯数据的工具和在 UNIX 环境下从文件系统中创建这样一个比特流的工具。Unrm 也是这

样一个 Unix 工具，它能产生一个单独的对象，包括文件系统未分配空间中所有的数据。可以使用 lazarus 工具系统地分析整个被创建的对象，判断其中是否有特殊的文件或二进制文件。该工具的分析效果非常好，从中可以得到很多细节信息 [5]。Higher Ground Software Inc. 的软件 Hard Drive Mechanic 也可用于从被删除的、被格式化的和已被重新分区的硬盘中获取数据。

3.4 磁盘特殊区域数据获取工具

磁盘的特殊区域也就是指在通常情况下无法访问到的区域。通常包括：未分配磁盘空间和文件的 slack 空间。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，同样文件的 slack 空间也可能包含先前文件遗留下来的信息。所以这些磁盘特殊区域很可能是证据的隐藏之地。NTI 公司的 GetFree 工具可以捕获磁盘未分配空间数据[4]，该公司的工具 GetSlack 可自动搜集磁盘文件系统中的 slack 文件碎片并将其写入一个统一的文件中[4]。

3.5 磁盘特殊文件获取工具

在调查取证中有一些比较容易忽视的特殊文件，但这些文件对证据的发现又很有帮助，可能隐藏有要寻找的证据，这些特殊文件一般包括：Swap 文件、缓存文件、临时文件和页面文件等。在 Windows 操作系统下的 windows swap(page)file，大概有 20-200M 的容量，记录着字符处理、Email 消息、Internet 浏览行为、数据库事务处理以及几乎其它任何有关 windows 会话工作的信息。NTI 公司的 GetSwap 工具可以用来获取静态的交换文件和页面文件的内容[4]。Cain V2.5 for NT/2000/XP 可以读取缓存文件、临时文件，比如 IE 缓存和 COOKIE 等，从而可以破解屏保密码、PWL 密码、共享密码、缓存口令、远程共享口令、SMB 口令等。

3.6 网络信息获取工具

上面讲到的一些取证工具都是基于一种静态的观点，即事件发生后对目标系统数据的静态获取。但随着计算机犯罪技术手段的不断提高，这种静态的获取有时无法满足要求，必须开发和使用动态的网络信息获取工具。网络信息获取工具用来在网络信道监测和获取特定的可成为证据的信息，这样可以发现对基于主机系统来说不易发现的犯罪证据。网络信息获取工具可以与 IDS、Honeypot、Honeynet 紧密结合，实时获取数据。整个获取过程将更加具有系统性、智能性和灵活性[6]。常用的网络信息获取工具有 windump、iris、tcpdump、ngrep、snort、sniffit、dsniff、grave-robber 等。还有一些获取本地网络状态信息的工具：netstat、route、arp 等。Fport 运行在 windows 平台上，可以识别系统中哪个应用软件在与别的计算机通信或在监听别的计算机。

4．证据保全工具

取证工作的第二个基本原则是要证明所获得的证据和原有的数据是完全相同的。在普通的案件取证中，证明所收集到的证物没有被修改过是一件非常困难的事情，也是很重要的事情，电子证据更是如此。需要证明的是取证人员在取证调查过程中没有造成任何对原始证物的改变；或者如果存在对证物的改变，也是由于计算机的本质特征造成的，并且这种改变对证物在取证上没有任何的影响。在取证过程中可采用保护证物的方法，如证物监督链，它可以使法院确信取证过程中原始证物没有发生任何改变，并且由证物推测出的结论也是可信的[7]。在电子证据取证过程中，为了保全证据通常使用数据签名和数字时间戳技术。

时间和数字签名都是很重要的证明数据有效性的内容。数字签名用于验证传送对象的完整性以及传送者的身份，但是数字签名没有提供对数字签名时间的见证，因此还需要数字时间戳服务。这种服务通过对数字对象进行登记，来提供注册后特定事物存在于特定的日期和时间的证据。时间戳服务对收集和保存数字证据非常有用，它提供了无可争辩的公正性来证明数字证据在特定的日期和时间里是存在的，并且在从该时刻到出庭这段时间里没有被修改过[7]。

除了要对被调查机器的硬盘的映像文件和关机前被保存下来的所有信息做时间标记以外，还有很多对象同样需要做时间标记。比如说：在收集证据过程中得到的证据，

其中包括日志文件、嗅探器的输出结果和入侵检测系统的输出结果；在可疑机器上得到的调查结果，其中包括所有文件的清单和它们的被访问时间；调查人员每天记录的副本等。在美国，目前提供时间戳服务的公司有 Surety 和 DigiStamp

证物的完整性验证和数字时间戳都是通过计算哈希值来实现的。这些哈希值的对象可以是单个的文件，也可以是整张软盘或整个硬盘。在完成哈希值计算并将其记录下来之后才可以开始证物的分析工作。现在较常用的两种哈希算法分别是 SHA 和 MD5。如果可能的话，应该尽量计算整个驱动器以及所有单个文件的哈希值。

表三　常用的数字证据保全工具

工具	性质
Md5sum	用 MD5 算法对给定的数据计算 MD5 校验和
CRCMd5	可以对给定的数据计算 CRC 和 MD5 校验和
DiskSig	验证映像文件拷贝精确性的 CRC 哈希工具
DiskSig pro	验证映像文件拷贝精确性的 CRC 或 MD5 哈希工具
Seized	保证用户无法对正在被调查的计算机或系统进行操作

5．证据分析工具

证据分析是计算机取证的核心和关键，其内容包括分析计算机的类型，采用的操作系统类型，是否有隐藏的分区，有无可疑外设，有无远程控制和木马程序及当前计算机系统的网络环境等等。通过将收集的程序、数据和备份与当前运行的程序数据进行对比，从中发现篡改痕迹。

分析工作的第一步通常是分析可疑硬盘的分区表，因为分区表内容不仅是提交给法院的一个重要条目，而且它还将决定在分析时需要使用什么工具。New Technology 公司的 Ptable 工具可以用来分析硬盘驱动器的分区情况[4]。

在检查分区表之后要浏览文件系统的目录树，这样可以对所分析的系统产生一个大致的了解。New Technology 公司的 FileList 工具是一个磁盘目录工具，可以将系统里的文件按照上次使用的时间顺序进行排列，让分析人员可以建立用户在该系统上的行为时间表[4]。

取证人员可以使用十六进制编辑器 UltraEdit32 和 winhex 等工具或一种取证程序来检查磁盘的主引导记录和引导扇区。如果使用的十六进制编辑器或其他取证程序具备搜索功能时，可用它搜索与案件有关的词汇、术语。搜索关键词是分析工作很重要的一步。New Technology 公司的 Filter_we 可以对磁盘数据根据所给的关键词进行模糊搜索。

在完成关键词搜索的工作后，应该找回那些已经被删除的文件。通过手动检查每一个扇区来查找已被删除的文件的方法已不再适用，可以采用前面介绍的反删除工具进行恢复。

NTI 公司的软件系统 Net Threat Analyzer[4]使用人工智能中的模式识别技术，分析 slack 磁盘空间、未分配磁盘空间、自由空间中所包含的信息，研究 Swap 文件、缓存文件、临时文件及网络流动数据，从而发现系统中曾发生过的 EMAIL 交流，Internet 浏览及文件上传下载等活动，提取出与生物、化学、核武器等恐怖袭击、炸弹制造及性犯罪等相关的内容。NTI 公司的 IPFilter 可以动态获取 swap 文件进行分析。Ethereal 能在 unix 和 windows 系统中运行，能捕捉通过网络的流量并进行分析，能重构诸如上网和访问网络文件等行为[7]。

计算机取证人员经常需要使用文件浏览器来打开各种格式的文件。Quick View Plus 是一款优秀的文件浏览器，它可以识别计算机里的超过 200 种文件类型，像 PC 、UNIX 以及一些 Macintosh 格式的文件几乎可以立即进行浏览，它也可用于浏览各种电子邮件文件格式，例如.msg。

很多案例都需要对大量的图片进行查阅，以此来查找与指控相关的东西。取证人员可以使用工具 ThusmbsPlus[8]，它只需要选择一个驱动器或目录，就会自动显示被选驱动器或目录中的所有图片文件并自动进行分析判断有没有信息隐藏。

在取证调查过程中正确并快速地识别反常文件是非常必要的，比如那些有着与他们真实数据类型不相符扩展名的文件。Guidance Software 公司的 Encase 取证工具

包称这一功能为文件特征识别及分析，它提供自动更新功能，并可以将试图隐藏的数据文件以列表的形式列出来。EnCase 中的分析工具包括关键字查找，hash 值分析，文件数字摘要分析等。在整个过程中，利用 EnCase 的报告函数能方便地将证据及调查结果进行归档[9]。

6．证据归档工具

在计算机取证的最后阶段，也是最终目的，应该是整理取证分析的结果供法庭作为诉讼证据。主要对涉及计算机犯罪的时间、地点、直接证据信息、系统环境信息、取证过程、以及取证专家对电子证据的分析结果和评估报告等进行归档处理。尤其值得注意的是，在处理电子证据的过程中，为保证证据的可信度，必须对各个步骤的情况进行归档以使证据经得起法庭的质询[11]。

计算机证据要同其他证据相互印证、相互联系起来综合分析。证据归档工具比较典型的是 NTI 公司的软件 NTI-DOC，它可用于自动记录电子数据产生的时间、日期及文件属性。还有 Guidance Software 公司的 Encase[9]工具，它可以对调查结果采用 html 或文本方式显示，并可打印出来。

7．结论

我国的计算机犯罪防范研究主要集中于计算机犯罪的特点、预防对策及其给社会带来的影响方面。在技术上还缺乏自主知识产权的计算机取证工具。

因为目前取证工具缺乏统一的标准和规范，所以制定取证工具的评价标准，取证机构和从业人员的资质审核办法以及取证工作的操作规范是非常必要的 [10]。

随着取证领域的不断扩大，取证工具应向着专业化和自动化的方向发展，未来的取证工具的开发应该结合人工智能、机器学习、神经网络和数据挖掘技术等，具有更多的信息分析和自动证据发现的功能，以代替大部分的人工操作[11]。

现在大量的移动设备如便携式计算机、掌上电脑、手机都可能成为犯罪的目标。如何在无线环境中进行取证和分析也是今后的一个重要研究课题。

给证物加上时间戳，这样可以证明证物在某一特定时刻是确实存在的。数据时间戳是一种非常实用的技术，虽然目前调查工作中使用它不是很普遍，但在未来的取证工作中，数字时间戳必将成为一种有效的证物鉴定方法[11]。

计算机取证技术的发展要进一步与信息安全技术的发展相结合，例如在网络协议设计过程中考虑到未来取证的需要，为潜在的取证活动保留充足信息。

计算机取证软件的效用倾向于同时拥有收集及分析数据的功能。但是没有哪个产品可以做所有的事情，因此，拥有更多的工具就更有可能发现那些藏于暗处而对案件有所帮助的信息。

参考文献

1.许榕生，吴海燕，刘宝旭. 计算机取证概述 计算机工程与应用 2001.21

2.NTI,Computer Evidence Processing Steps: http://www.forensics-intl.com/evidguid.html

3.Madihah Mohd. Saudi，an overview of disk imaging tool in computer forensics：http://www.sans.org/rr/papers/27/643.pdf

4. Data Capture Tool ：http://www.forensics-intl.com

5.Dan Farmer,Wietse Venema http://www.fish.com/tct

6.Stephen Barish.Windows Forensics:a case study: http://www.securityfocus.com/infocus/1653

7.Kruse,W.G. and Heiser,J.G.(2001) Computer Forensic.Incident Response Essentials, Addison-Wesley,Boston.

8.http://www.acerious.com

9.Guidance Software,Inc. http://www.encase.com/

10.王玲,钱华林：计算机取证技术及其发展趋势 软件学报 Vol.14,No. 9

11.Vacca,J.R.(2002) Computer Forensics:Computer Crime Scene Investigations,Charles River Media,Inc.,Hingham, Massachuetts.