基于 WinPE 系统的 U 盘取证①

The U Forensic Based on WinPE System

位晓晓　杨　英　文立强　(山东省轻工业学院 山东省计算中心 山东 济南 250014)

摘　要： 电子证据的特点，即对证据数据进行各种操作过程越频繁，越容易损坏证据，原始系统及介质越容易受到干扰和破坏，因此，设计一个对数据和系统影响尽可能少的工具就显得非常重要。论述了目前国内外的研究现状，简单介绍了 U 盘系统的制作过程，并在 U 盘系统的基础上，深入了解操作系统、文件结构、磁盘系统等基础知识，设计一个 U 盘信息采集软件。该软件的功能是实现基于电脑使用痕迹的硬盘信息和系统信息的快速提取。

关键词： 信息采集 电子证据 U 盘系统 计算机取证 电脑使用痕迹

近几年，由于利用计算机犯罪事件越来越多，针对计算机取证的研究越来越深入。作为计算机领域和法学领域的一门交叉科学，被用来解决大量的计算机犯罪和事故，包括网络入侵、盗用知识产权和网络欺骗等。计算机取证(computer forensics)正逐渐成为人们研究与关注的焦点[1]。

国外对取证技术的研究已有多年的历史，已开发出多种取证工具，比较流行的是镜像工具和专业的取证软件，当前国际上的数字证据取证工具有几款比较成熟的，如 Guidance Software 公司的 EnCase Professional，可以用于 Windows 系统下法庭数据收集和分析，可将系统的全部运行环境和数据生成一个映像文件，再对文件进行分析，从而发现犯罪证据；美国的 DIBS 产品，是一中数据镜像备份系统，可以确保单独复制的安全性和完整性；英国 Vogon 公司开发了基于 PC MAC 和 Unix 等系统的数据收集和分析系统，可以将计算机硬盘进行复制，生成物理镜像；COFEE(Computer Online Forensic Evidence Extractor)[2]是安装在优盘里的证据提取工具，可以快速地绕过 Windows 系统的所有安全措施；COFEE 可以解密系统密码，显示网络浏览的历史，对电脑系统进行深入搜索来获取证据，这无疑将大大提升警探的查案水平。

目前，国内相关行业针对高科技犯罪等方面的研究还处于起步阶段，同发达国家存在一定差距，大量计算机相关的犯罪行为缺乏有效的解决途径。当前法庭案例中出现的计算机证据都比较简单，多是文档、电子邮件、程序源代码等不需特殊工具就可以取得的信息。但随着技术的进步，计算机犯罪的水平也在不断提高，目前的计算机取证技术已不能满足打击计算机犯罪、保护网络与信息安全的要求，自主开发适合我国国情的、能够全面检查计算机与网络系统的计算机取证的工具与软件已经迫在眉睫。

1　概述

计算机取证技术主要分为静态取证和动态取证[3]。下面所说的取证技术主要是静态取证，在入侵事件已经发生后，对内存缓冲、硬盘以及其他形式的储存介质进行数据提取、分析、抽取有效数据以发现犯罪证据的过程。

事后取证技术包括从原始介质中的数据获取技术和数据分析技术。数据获取包括从内存里获取易灭失数据和从硬盘获取相对稳定数据，其获取顺序为先内存后硬盘。案件发生后，立即对目标机和网络设备进行检查并作好记录。

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数据分析技术，具体包括：

① 基金项目:山东省重大科技专项基金(2006GG1108097-25)
收稿时间:2009-01-16

文件属性分析、文件的数字摘要分析、日志分析，根据已经获得的文件或数据的用语、语法或编程风格，推断出其可能的作者的技术。

本课题目的是制作一个应用软件，能够对锁定电脑进行信息提取。主要实现对 E-mail 和 QQ 等即时通讯工具的信息提取。该软件可以用在网吧、家用电脑及公司电脑的调查取证上；可以配合企业管理员工，公司内部管理阶层对公司职员的电脑进行定期稽查，保护企业的知识产权；也可以实现公正性地调查取证，如律师事务所的调查审计。

自互联网诞生，E-mail 成为互联网上的一项重要服务，针对 E-mail 的研究始终没有中断过。针对邮件系统的计算机取证活动，国内外的研究技术重点多集中在邮件系统的监控上，通过对网络上 IP 包的分析来获取相关信息以及进行筛选。

即时通信(Instant Messaging)是近年来逐渐兴起的网络应用之一。面向大众娱乐聊天休闲的即时通信软件层出不穷，如 QQ，MSN，Yahoo Messenger 等等。它可以弥补传统通讯形式的不足，尤其是电子邮件及语音的不足，为用户提供实时有效的沟通手段。

国内外很多公司研发出了专门用于 IM 监控的软件[4]，对局域网的 IM 通信事件进行监控和分析。例如，MSN Sniffe，主要功能是嗅探局域网 MSN Messenger 聊天信息，也可以即时地在软件窗口查看监测到的聊天记录；DCI 针对 HTTP、E-mail(SMTP、POP3)、FTP、IM(MSN、Yahoo、ICQ)等协议进行监控，完整记录送出的档案、浏览网站的记录、聊天的内容。

2 设计模型

Windows 预安装环境 Windows PreInstallation Environment(WinPE)，又称微型操作系统。WinPE 不通过硬盘启动，它调用内存当作硬盘来启动[5]。

用 USBoot v1.68 或者 FLASHBOOT1.40 启动 U 盘制作工具，将 U 盘制作成 USB-HDD 的 DOS 启动型，按照工具的提示即可制作成功。

在进入 U 盘系统之前，首先修改一下 BIOS 设置。将 U 盘插入 USB 接口，启动电脑，在系统自检的界面上按 Del 键(视主板而定)进入 BIOS 设置，选择 BIOS FEATURES SETUP，将启动顺序(Boot Sequence)设为 USB-HDD(或 USB-ZIP)优先启动顺序。

本文的选题主要为用户提供一个基于 USB 接口的简单数据采集系统，其中用 PC 机作为 USB 的主控制端，完成数据处理和显示、系统控制等功能。

电脑在关机的状态下，插上 U 盘后启动电脑，修改 BIOS 设置，使电脑从 U 盘启动，这样能更加快速地启动电脑；进入 U 盘操作系统后，运行信息采集软件，进行信息搜集；搜集信息完毕，自动保存有效信息；拔下 U 盘，可以在另外的电脑终端或界面上显示系统所搜集到的信息，并且可以对所获取的信息进行分析处理，最后生成一个 html 文件报告，展示给操作人员。另外，系统可以实现用户选择性地定制软件功能，有目的的筛选所要搜集的信息。下图为信息采集原理图 1。

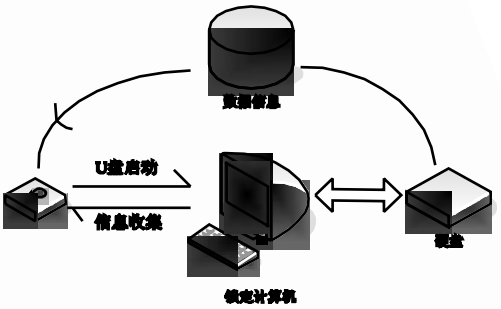

图 1 信息采集原理图

该工具能够实现：发现目标信息、提取目标信息、存储目标信息、分析目标信息。

3 信息搜索的设计

支持 FAT32，NTFS 文件系统，搜索类型支持逻辑搜索、物理搜索、已删除的文件。搜索源为本地硬盘。搜索字的编码方式支持 Big5，GB2312 或 Unicode，支持二次搜索，搜索报告自动产生。搜索功能包括关键词/文件名搜索、资源回收搜索、Hash 值搜索、可疑文件搜索、日志文件搜索、电子邮件搜索、即时通讯记录搜索。

3.1 获取信息

计算机取证其自身的特点导致取证的方式和来源不同。计算机证据的来源主要来自两个方面，一个是系统方面，另一个是网络方面[6]。其中，来自系统方面的证据包括：系统日志文件、备份介质、程序、脚本、进程、内存映象、交换区文件、临时文件、硬盘未分配的空间、系统缓冲区、打印机及其它设备的内

存。来自网络方面的证据有：防火墙日志、IDS 日志、其它网络工具所产生的记录和日志等[6]。

本文设计的软件获取的信息有：即时信息、邮箱使用痕迹、浏览器的历史记录、我的文档、我的收藏夹、回收站等内容。这些信息的物理存在构成了信息搜集的物质基础。

3.2 IE 浏览器使用痕迹

为了提高访问网页的速度，IE 浏览器会采用累积式加速的方法，将曾经访问的网页内容(包括图片以及 cookies 文件等)存放在电脑里。这个存放空间，就称它为 IE 缓存。IE 缓存提高了访问网站的速度，同时也为信息提取提供了来源。

Temporary Internet Files 是 Windows 中储存 Internet 临时文件的文件夹，具体的文件路径根据 Internet 选项中的设置而各不相同。

Cookies 是一种能够让网站服务器把少量数据储存到客户端的硬盘或内存，或是从客户端的硬盘读取数据的一种技术。当用户浏览某网站时，由 Web 服务器置于硬盘上的一个非常小的文本文件，它可以记录用户的 ID、密码、浏览过的网页、停留的时间等信息。

硬盘中的 Cookies 文件可以被 Web 浏览器读取，根据 Cookies 内容知道用户登录过什么网站，根据该文件，可链接该网站，进行跟踪调查。

3.3 邮箱使用信息

Office Outlook 是 Microsoft office 套装软件的组件之一，它对 Windows 自带的 Outlook express 的功能进行了扩充。Outlook 的功能有，收发电子邮件、管理联系人信息、记日记、安排日程、分配任务。

通常在某个网站注册了自己的电子邮箱后，要收发电子邮件，须登入该网站，进入电邮网页，输入帐户名和密码，然后进行电子邮件的相关操作。使用 Outlook Express，只要打开 Outlook Express 界面，Outlook Express 程序便自动与用户注册的网站电子邮箱服务器联机工作，收下用户的电子邮件。发信时，可以使用 Outlook Express 创建新邮件，通过网站服务器联机发送。(所有电子邮件可以脱机阅览)。Outlook Express 在接收电子邮件时，会自动把发信人的电邮地址存入“通讯簿”，供以后调用[9]。当用户点击网页中的电邮超链接时，会自动弹出写邮件界面，该新邮件已自动设置好了收信人的电邮地址和用户的电邮地址，用户只要写上内容，邮件即可发送。

Foxmail 信息的提取：首先要找到其安装目录，收件箱对应着 box 和 in.ind，发件箱对应着 out.box 和 out.ind，已发送邮箱对应着 sent. box 和 sent.ind，废件箱对应着 trash. box 和 trash. ind。

3.4 即时信息存放位置

即时通讯软件主要以 QQ 和 MSN 工具为例。针对 QQ 信息提取主要通过客户端获取，考虑软件的安装路径、加密技术和汉字编码转换等信息。聊天记录文件是正常登陆过 QQ 後生成的，用来记录 QQ 在这台机子上的所有聊天记录。对 QQ 的取证主要是获取它的聊天记录信息。

聊天记录文件采用了 Storage 结构化存储。其中消息内容都存储在每个号码下面的 Data 中，通过 Index 索引。对 QQ 聊天记录的获取主要是针对聊天记录信息、群消息、系统消息这三个数据库文件进行。

MSN 的聊天记录是以.xml 文件进行存储的，文件的名字为“用户昵称+帐号代码.xml”。这里的用户昵称是会话对方的昵称，内容包括聊天记录，还记录有用户接收到的文件信息，在“消息”一栏中记录着用回接收到的文件的名字和保存路径。在一个 XML 文件中，可能会有多个 Message Invitation、Invitation-Response 节点。XML 文档对象模型(XML DOM)提供了一个标准的方法来操作存储在 XML 文档中的信息，DOM 应用编程接口(API)用来作为应用程序和 XML 文档之间的桥梁。设计的 MSXML 解析器根据 XML 文档生成一个 DOM 树结构，它能够读 XML 文档并根据 XML 文档内容创建一个节点的逻辑结构，文档本身被认为是一个包含了所有其他节点的节点。通过 MSXML 解析器对逐个节点进行解析，得到所需的信息，例如聊天记录、时间、内容等。

3.5 黑客软件信息

病毒、木马、后门以及黑客程序也严重影响着信息的安全。这些程序感染计算机的一个共同特点是在注册表中写入信息，来达到如自动运行、破坏和传播等目的。举二例如下：

(1) 查找 NetSpy 黑客程序 HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run 下，在右边的窗口中寻找键"NetSpy"，如果存在，就说明已经装有 NetSpy 黑客程序；

(2) 查找 BO2000 的破坏 HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices 下若在右边窗口中如发现了“umgr32.exe”键值，则说明中了 BO2000。

病毒、木马、后门及黑客软件等的破坏，还需要专业人员对注册表比较熟悉才能判断是电脑否受到入侵。

另外，驱动器:\Documents and Settings\用户名\Favorites 为收藏夹的地址；驱动器:\Documents and Settings\用户名\My Documents 为我的文档的地址；驱动器:\RECYCLER 或者驱动器:\WINDOWS\RECYCLER 为回收站的路径。

4 结语

与光盘取证工具相比，采用 U 盘的优点是：U 盘读写比较方便，一般 CD/DVD 只能写入一次，U 盘可写入多次；U 盘启动电脑速度比光盘启动快，且噪音小；与 U 盘相比，光盘容易损坏，不利于数据读取和保存；U 盘体积小，比光盘更易于携带。

U 盘系统的优点有：U 盘系统制作简单；实现对计算机系统和文件的安全获取，Winpe 系统运行独立，能最小程度的减少对原始系统及原始介质的破坏和干扰。Windows 系统正常的关闭电脑的方式会导致系统向硬盘写入信息，这正是我们需要防止的；U 盘系统小，启动速度更快；能避开开机密码设置，使用方便。

该工具操作简单明了，可以用于公司内部管理阶层对公司职员的电脑进行定期稽查，保护企业的知识产权方面；也可以实现公正性地调查取证，如律师事务所的调查审计。

不足之处是：(1)若锁定电脑的主板不支持 USB 启动，则工具无法使用；(2)锁定电脑的 BIOS 设置了密码，需要对密码解密，延长操作时间；(3)由于 U 盘易于读写的特点，需要用户特别注意数据的保护，防止数据受到恶意篡改。这是工具亟待改善的地方。

参考文献

1 丁丽萍,王永吉.计算机取证的相关法律技术问题研究.软件学报, 2005,16(2):260－275.
2 巴斯光年.COFEE：微软官方警探专用反犯罪工具. 2008-05-01.http://news.mydrivers.com/1/105/105009.htm
3 Dixon PD. An overview of computer forensics. IEEE POTENTIALS, 2005,5(2):7－10.
4 Liu NQ, Wang ZS, Hao YJ, Qin K. Computer Forensics Research and Implementation Based on NTFS File Syestem. ISECS International Collo- quium on Computing, Communication,Control, and Management, 2008,8(2):519－523.
5 徐爱钧,万天军,李家绪.一种 U 盘数据采集系统的设计.长江大学学报(自科版), 2006,3(5):79－81.
6 赵小敏.基于日志的计算机取证技术的研究及系统设计与实现.杭州:浙江工业大学, 2002.