Linux 环境下的计算机取证工具介绍

Introduction to Computer Forensic Tools Based on Linux

殷联甫 （嘉兴学院信息工程学院 314001）

摘要：本文主要介绍 Linux 环境下的三个主要计算机取证工具 Sleuthkit、Autopsy 和 SMART for Linux 及其使用方法。
关键词：计算机取证 计算机取证工具 Linux 操作系统

1 引言

计算机取证作为计算机安全领域的一个新的热点正引起人们的普遍关注。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。

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。

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，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。

计算机取证过程中要用到很多工具，目前可用的取证工具也比较多，根据取证工具的功能，主要可以将取证工具分为三大类：第一类是实时响应工具，第二类是取证复制工具，第三类是取证分析工具。近年来 Linux 系统的发展势头非常迅猛，用户日益增多，了解 Linux 环境下的计算机取证工具具有非常重要的意义。目前 Linux 环境下的取证工具也有不少，有兴趣的读者可参阅网址 http://www.opensourceforensics.org/tools/unix.html。本文主要介绍 Linux 环境下的三个主要取证工具：Sleuthkit、Autopsy 和 SMART for Linux。

2 Sleuthkit

2.1 下载及安装

Sleuthkit 由一系列命令行取证工具组成，由 Brian Carrier 编写，维护网站是 http://www.sleuthkit.org。该工具的部分设计思想基于由 Dan Farmer 和 Wietse Venema 编写的 The Coroner's Toolkit（TCT），Sleuthkit 同时增加了对 FAT 和 NTFS 文件系统的支持。

现在假设我们已经从 http://www.sleuthkit.org 网站下载 Sleuthkit 工具的源代码到/root 目录中，下面的命令给出了 Sleuthkit 工具的编译过程：

```
# tar xzvf sleuthkit-1.66.tar.gz
# cd sleuthkit-1.66
# make
```

如果编译过程出现问题的话，可以参阅 INSTALL 文档。编译结束后，你可以看到所有 sleuthkit 命令都在 sleuthkit-1.66/bin 目录中，而每个命令的使用说明都在 sleuthkit-1.66/man 目录中。

Sleuthkit 工具由四部分组成，每一部分对应文件系统的一个层次：

（1）文件系统层工具：fsstat（命令以 fs（file system，文件系统）开头）

（2）文件名称层工具：fls，ffind（命令以 f（file，文件）开头）

（3）数据层工具：dcalc，dcat，dls，dstat（命令以 d（data，数据）开头）

（4）i 节点层工具：icat，ils，ifind，istat（命令以 i（inode，i 节点）开头）

2.2 主要命令的使用

（1）fsstat 和 fls

fsstat 命令主要列出在一个设备或一个分区映像

上的文件系统的相关信息。看下面的例子(假设你的当前目录是 /root/sleuthkit-1.66/bin):

./ fsstat /root/able2/able2.part2.dd

在上面的命令中,able2.part2.dd 是名为 able2 的分区的映像文件,由 dd 命令生成。

fls 命令主要列出包含在一个文件系统中的文件名和目录,该命令有许多可选项。看下面的例子:

./ fls - f linux-ext2 - Frd /root/ able2/able2.part2.dd

在上面的命令中,选项"- f linux-ext2"表示 fls 命令的运行对象是 ext2 文件系统,"-F"表示仅显示文件名,"-r"表示目录按降序排列,"-d"表示显示被删除文件名。

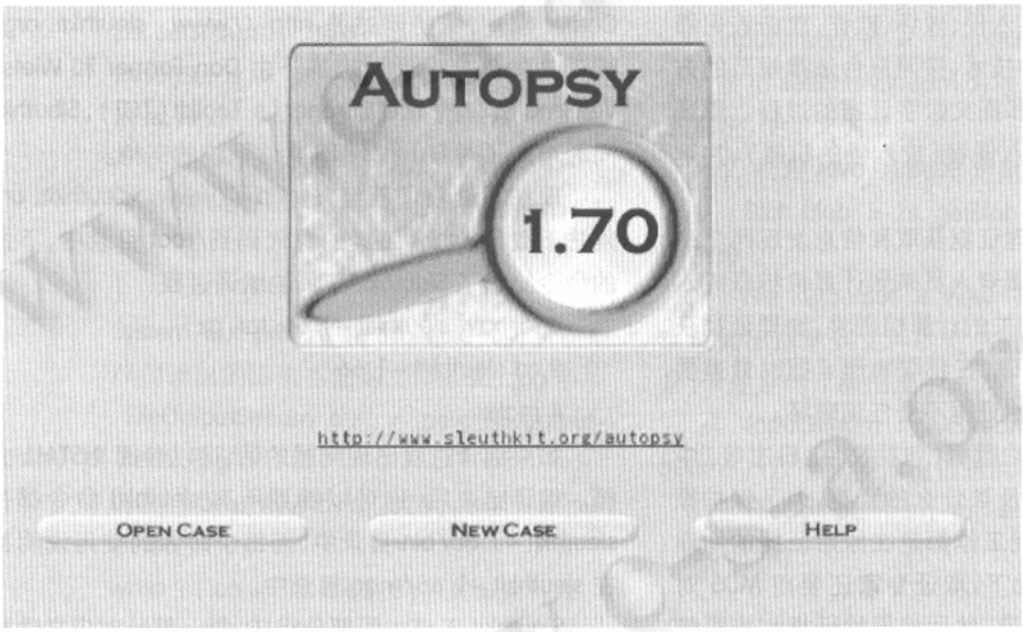

图 1　Autopsy 启动画面

(2) istat 和 icat

istat 命令的功能与 fsstat 相近。fsstat 命令的运行对象是一个文件系统,而 istat? 命令的运行对象是一个 i 节点。看下面的例子:

./ istat -f linux-ext2 /root/able2/able2.part2.dd 2139 | less

在上面的命令中,istat 读出在一个 ext2(-f linux-ext2)分区(/root/able2/able2.part2.dd)上的 i 节点号为 2139 的 i 节点的相关信息。

icat 命令的主要功能是读出与一个 i 节点相关的所有数据块中的数据。看下面的例子:

./ icat - f linux-ext2 /root/able2/able2.part2.dd 2139 > /root/lrkn.tgz.2139

在上面的命令中,icat 读出 ext2(- f linux-ext2)分区(able2.part2.dd)中与 i 节点 2139 相关的所有数据块中的数据。

3 Autopsy

3.1 下载及安装

Autopsy 由 Brian Carrier 编写,下载网址是 http://www.sleuthkit.org。在正式下载及安装 Autopsy 之前,我们必须做以下几项工作:

(1) 建立一个用于存放 Autopsy 运行结果的工作目录(该目录也叫"证据保管箱"):

mkdir /root/autopsy_evid

(2) 在安装 Autopsy 之前必须先安装 sleuthkit,并记下 sleuthkit 的安装路径,因为在安装 Autopsy 时要输入 sleuthkit 的安装路径。

下面开始安装 Autopsy(假设源文件 autopsy-1.75.tar.gz 已下载到 root 目录中):

tar xzvf autopsy-1.75.tar.gz

cd autopsy-1.75

make

在安装过程中,安装程序需要寻找一些文件,同时提示你输入 sleuthkit 的安装路径。当安装程序提示你输入你的 NSRL 数据库的位置时,请直接按回车键(除非你已经安装了 NSRL 数据库)。最后,输入"证据保管箱"的路径(/root/autopsy_evid)。

3.2 Autopsy 的使用

安装结束后,我们必须在 X Windows 环境下使用该工具。在终端上输入:

```
# ./autopsy
```

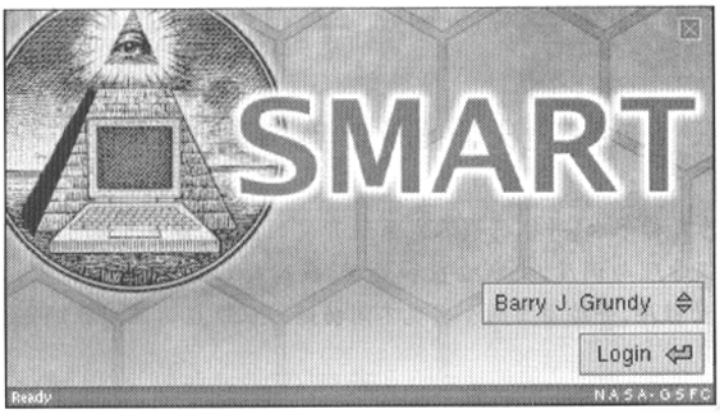

图 2　SMART 的启动登录画面

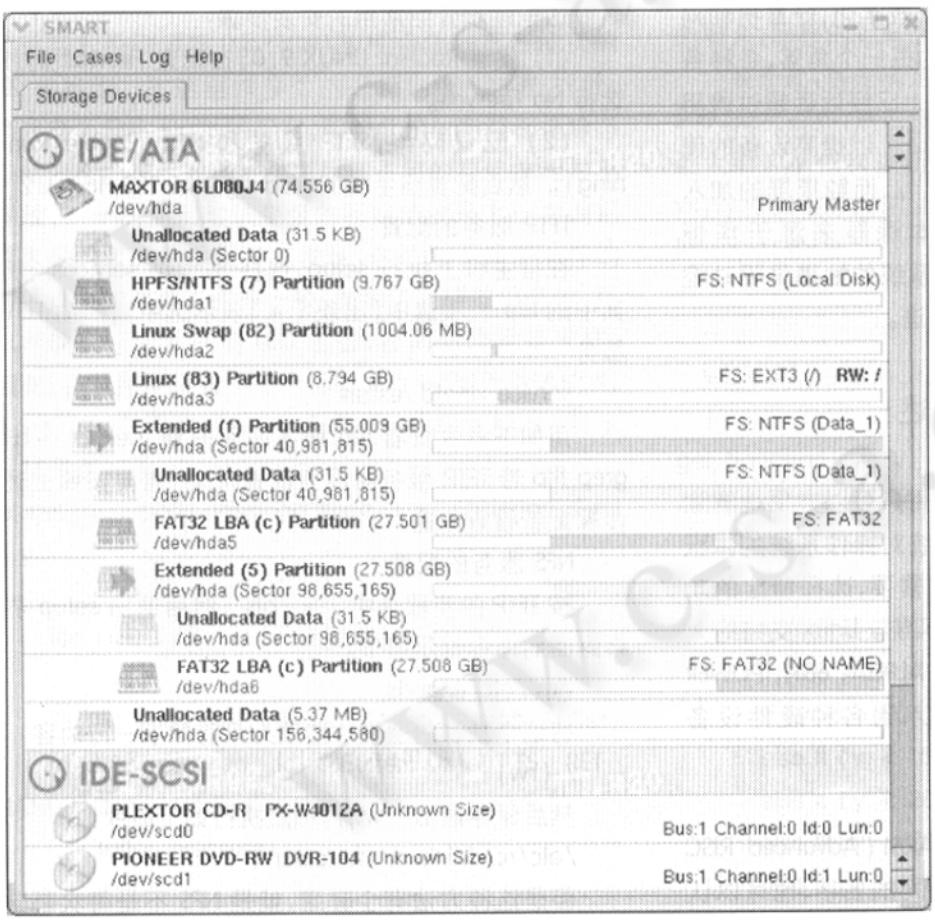

图 3　SMART 的初始画面

```
= = = = = = = = = = = = = = = = = = = = =
Autopsy Forensic Browser
http://www.sleuthkit.org/autopsy/
ver 1.75
= = = = = = = = = = = = = = = = = = = = =
Evidence Locker: /root/autopsy_evid/
Start Time: Sun Aug 17 16:13:56 2003
Remote Host: localhost
Local Port: 9999
Open an HTML browser on the remote host and paste this URL in it:
http://localhost:9999/
309825290725069710 42/autopsy
Keep this process running and use <ctrl-c> to exit
```

注意：当 Autopsy 开始运行后，你不能关闭终端，因为 Autopsy 进程是作为终端的一个子进程在运行的，如果关闭终端的话，Autopsy 进程也将终止运行。现在你必须打开浏览器，同时将上面显示的 URL 复制到浏览器窗口，此时开始显示下面的 Autopsy HTML 界面如图 1。

单击“New Case”，开始使用 Autopsy。

4　SMART for Linux

SMART 是一个由 ASR Data 开发，基于 Linux 的商业化的计算机取证工具，网址是 http://www.asrdata.com/SMART。SMART 的启动登录画面如图 2 所示。

参考文献

1 B. Grundy. The Law Enforcement and Forensic Examiner Introduction to Linux: A Beginner's Guide. 2004. http://www.linux-forensics.com/linuxintro-LEFE-2.0.5.pdf.

2 殷联甫，计算机取证工具分析，计算机系统应用，2005.8.