# 计算机反取证技术研究

## Research on Computer Anti – Forensics

殷联甫 （嘉兴学院信息工程学院 314001）

**摘要**：在计算机取证日益受到人们重视和关注的今天，人们对反取证技术的研究相对较少。本文主要介绍目前常见的反取证技术和工具，并给出几个实现反取证的具体实例。

**关键词**：计算机取证 计算机反取证 计算机安全 计算机犯罪

## 1 引言

在计算机犯罪日益猖獗的今天，计算机取证正日益受到人们的关注和重视。计算机取证就是对计算机犯罪的证据进行获取、保存、分析和出示，它实际上是一个扫描计算机系统以及重建入侵事件的过程。与计算机取证研究相比，人们对反取证技术的研究相对较少。对于计算机取证人员来说，研究反取证技术意义非常重大，一方面可以了解入侵者有哪些常用手段用来掩盖甚至擦除入侵痕迹；另一方面可以在了解这些手段的基础上，开发出更加有效、实用的计算机取证工具，从而加大对计算机犯罪的打击力度，保证信息系统的安全性。

计算机反取证就是删除或者隐藏入侵证据使取证工作无效。目前的计算机反取证技术主要有数据擦除、数据隐藏等。数据擦除是最有效的反取证方法，它是指清除所有可能的证据（包括索引节点、目录文件和数据块中的原始数据等），原始数据不存在了，取证工作自然无法进行。数据隐藏是指入侵者将暂时还不能被删除的文件伪装成其他类型或者将它们隐藏在图形或音乐文件中，也有人将数据文件隐藏在磁盘上的 Slack 空间、交换空间或者未分配空间中，这类技术统称为数据隐藏[5][7]。

## 2 数据擦除

数据擦除是阻止取证调查人员获取、分析犯罪证据的最有效的方法，一般情况下是用一些毫无意义的、随机产生的‘0’、‘1’字符串序列来覆盖介质上面的数据，使取证调查人员无法获取有用的信息。目前最极端的数据擦除工具是 Data Security Inc. 开发的基于硬件的 degaussers 工具，该工具可以彻底擦除计算机硬盘上的所有电磁信息。其它用软件实现的数据擦除工具既有商业软件包，也有开放源代码的自由软件，其中最有名的是基于 UNIX 系统的数据擦除工具 The Defiler's Toolkit，The Defiler's Toolkit 提供两个工具来彻底清除 UNIX 类系统中的文件内容[1][2]。

### 2.1 Necrofile 的使用

该工具列出并清除在指定时间范围内被删除文件的 i 节点的内容，同时清除与这些 i 节点相关的数据块的内容。这样取证调查人员便无法获得文件系统的任何证据，取证工作自然无法正常进行。

当调用 Necrofile 程序运行时，Necrofile 程序首先检查 i 节点表中每个 i 节点的状态，对于每个“脏（dirty）”i 节点予以特别的关注，将每个符合清除条件的“脏（dirty）”i 节点的内容清空，然后再写回到 i 节点表中。下面是使用 Necrofile 工具清除被删除文件 i 节点内容的一个例子：

（1）第一步：用 TCT 工具包中的 ils 工具在指定分区上查找被删除的 i 节点

```
# ./ils /dev/hda6
class|host|device|start_time
ils|XXX|/dev/hda6|1026771982
st_ino|st_alloc|st_uid|st_gid|st_mtime|st_atime|st_
ctime|st_dtime|st_mode|\
st_nlink|st_size|st_block0|st_block1
12|f|0|0|1026771841|1026771796|1026771958|
1026771958|100644|0|86|545|0
```

```
13|f|0|0|1026771842|1026771796|1026771958|
1026771958|100644|0|86|546|0
.
.
.
#
```

(2) 第二步:用 Necrofile 工具定位并清除被删除 i 节点的内容

```
#./necrofile -v -v -v -v /dev/hda6
Scrubbing device: /dev/hda6
12 = m: 0x3d334d4d a: 0x3d334d4d c: 0x3d334d4f
d: 0x3d334d4f
13 = m: 0x3d334d4d a: 0x3d334d4d c: 0x3d334d4f
d: 0x3d334d4f
.
.
.
#
```

(3) 第三步:验证被删除 i 节点的内容已被清空

```
#./ils /dev/hda6
class|host|device|start_time
ils|XXX|/dev/hda6|1026772140
st_ino|st_alloc|st_uid|st_gid|st_mtime|st_atime|st_
ctime|st_dtime|st_mode|\
st_nlink|st_size|st_block0|st_block1
#
```

在上面的例子中,"ils"是 TCT 工具包中的一个工具,主要功能是查找并列出指定分区上所有被删除的 i 节点的内容。Necrofile 工具定位并覆盖由 ils 查找到的所有 i 节点,将其内容全部清空,这样 ils 再也无法找到这些被删除的 i 节点。i 节点的内容被清除以后,接下来的工作是要清除文件目录项的内容。

### 2.2 Klismafile 的使用

该工具完成的主要功能是清除被删除文件的目录项的内容。下面是使用该工具清除被删除文件目录项内容的一个例子:

(1) 第一步:用 fls 工具列出指定分区上所有被删除的文件目录项

```
#./fls -d /dev/hda6 2
? * 0: a
? * 0: b
.
.
.
#
```

(2) 第二步:用 Klismafile 工具清除所有被删除文件目录项的内容

```
#./klismafile -v /mnt
Scrubbing device: /dev/hda6
cleansing /
-> a
-> b
.
.
.
Total files found: 29
Directories checked: 1
Dirents removed : 26
#
```

(3) 第三步:验证被删除文件目录项的内容已被清空

```
#./fls -d /dev/hda6 2
#
```

在上面的例子中,"fls"是 TCT-UTILS 软件包中的一个工具,主要功能是检查目录文件,列出被删除文件目录项的内容。本例中先用 fls 工具列出根目录下所有被删除文件的目录项,然后用 Klismafile 工具清除所有被删除文件目录项的内容,最后 fls 再也无法看到文件目录项的内容。

## 3 数据隐藏

数据隐藏主要是阻止调查取证人员在取证分析阶段对获取的数据进行有效的分析。目前实现数据隐藏的常用方法主要有以下几种。

### 3.1 实现数据隐藏的几种常用方法[2][8]

(1) 数据加密。数据加密是用一定的加密算法对数据进行加密,使明文变为密文。但这种方法不是十分有效,因为有经验的调查取证人员往往能够感觉到数据已被加密,并能对加密的数据进行有效的解密。

(2) 更改文件的扩展名。在 Windows 系统中,更改文件的扩展名是一种最简单的数据隐藏方法。例

如,某人不想让别人看到其 Word 文档里的内容,并且不想使其成为对自己不利的证据,那么他可以将文件的扩展名从. doc 改为. jpg。这样的话,无论是 Internet Exploer 还是图标外观,都显示该文件为一个 JPEG 图片。对于经验不足的调查取证人员,可能永远也不会想到该文件其实是一个文档,即使你双击该图标,Windows 也会试图使用默认的 JPEG 文件的浏览器来打开它。

(3) 隐写术。隐写术的意思是"隐藏在普通的视觉之下"。Steganography(隐写术)这个单词是由希腊词语里的"Covered writing"转化而来的,是指有隐藏特性的数据。密码隐写术或信息伪装夹带技术是使用一些其他的非加密数据对目标进行隐藏,我们把这种非加密的数据称为"载体"。载体通常是一个多媒体文件,可能是声音文件也可能是图像文件。

伪装夹带技术通常通过两种方法对数据进行保护:第一种是使数据不可见,隐藏它的所有痕迹;第二种是对数据进行加密,其过程不仅仅是对数据进行隐藏。如果隐藏的文件被发现,那仍需要对其进行解密才能使用。伪装夹带技术会给取证调查带来很大的麻烦。但幸运的是它的使用受到时间因素的限制,因而没有得到广泛的使用。如果你想要"伪装夹带"一个文件,那你一次只能对一个文件进行操作。许多事件中包含成百上千个文件,嫌疑人不可能有时间来找到那么多合适的载体并伪装夹带所有的文件。

目前已有一些商业的隐写术应用软件,数字水印就是其中的一种,它主要是将数据隐藏到位图中。

(4) 改变系统环境。系统环境改变之后,系统会给出假的关于数据内容和活动的信息。

### 3.2 实现数据隐藏的具体实例[1]

目前在 UNIX 系统中使用最广泛的取证分析工具是由 Dan Farmer 和 Wietse Venema 开发的 The Coronor's" Toolkit,即 TCT 工具包。尽管 TCT 工具包的功能非常强大,但 TCT 工具包存在一个致命的缺陷,该缺陷源于它在实现时有两个致命的错误:一个错误是认为数据块不能分配给根 i 节点之前的任意 i 节点;另一个错误是没有考虑到坏块 i 节点。这样使得 TCT 工具无法检查入侵者隐藏在磁盘的某个特定区域上面的数据。Runefs 就是一个利用 TCT 工具包的缺陷而在 UNIX 环境下开发成功的数据隐藏工具。

下面是一个使用 runefs 工具包建立、使用隐藏空间的具体实例:

(1) 第一步.建立隐藏空间

```
# df -k /dev/hda6
Filesystem 1k-blocks Used Available Use% Mounted on
/dev/hda6 1011928 20 960504 1% /mnt
# ./bin/mkrune -v /dev/hda6
+++ bb_blk +++
        bb_blk->start = 33275
        bb_blk->end = 65535
        bb_blk->group = 1
        bb_blk->size = 32261
+++
rune size: 126M
# df -k /dev/hda6
Filesystem 1k-blocks Used Available Use% Mounted on
/dev/hda6 1011928 129196 831328 14% /mnt
# e2fsck -f /dev/hda6
e2fsck 1.26 (3-Feb-2002)
Pass 1: Checking inodes, blocks, and sizes
Pass 2: Checking directory structure
Pass 3: Checking directory connectivity
Pass 4: Checking reference counts
Pass 5: Checking group summary information
/dev/hda6: 11/128768 files (0.0% non-contiguous), 36349/257032 blocks
#
```

上面的操作演示了如何在磁盘上分配 126M 的隐藏空间、该隐藏空间如何被内核注册。

(2) 第二步:使用隐藏空间

```
# cat readme.tools | ./bin/runewr /dev/hda6
# ./bin/runerd /dev/hda6 > f
# diff f readme.tools
#
```

上面演示了如何在隐藏空间中读写数据。

(3) 第三步:验证 TCT 工具无法看到隐藏空间

```
# ./icat /dev/hda6 1
/icat: invalid inode number: 1
```

#

## 4 Linux 环境下常见的计算机反取证工具介绍[6]

(1) srm(http://srm.sourceforge.net/)

srm 是 rm 命令的改进,它在删除文件时能将文件内容全部清空。

(2) wipe(http://wipe.sourceforge.net/)

wipe 工具能有效地将硬盘表面的信息彻底清除,使调查取证人员无法从硬盘上恢复任何信息。

(3) grind(http://prp0.prp.physik.tudarmstadt.de/~mrose/grind/)

grind 工具用一些随机数来覆盖文件的内容,使调查取证人员无法从硬盘上获取有价值的信息。

## 5 Windows 环境下常见的计算机反取证工具介绍[6]

(1) Diskzapper(http://diskzapper.com/)

Diskzapper Dangerous 在机器启动过程中能自动删除硬盘上的所有信息,无须人工干预。Diskzapper Extreme 首先生成一串随机数,然后用生成的随机数覆盖硬盘上每个扇区的内容。

(2) StealthDisk(http://invisicom.com/products/stealthdisk/)

StealthDisk 能隐藏计算机上所有的文件和文件夹,同时能删除所有在线 Internet 访问记录。

(3) SecureIT2000(http://www.cypherix.co.uk/prods.htm)

SecureIT2000 是一个基于 Blowfish 算法的 448 位强数据加密工具,能对所有的文件和文件夹进行加密。

(4) Cloak(http://www.insightconcepts.com/products/cloak/)

Cloak 是一个有效的隐写术应用软件,它能对文件进行加密并将其隐藏在位图文件中。

(5) Invisible Secrets(http://www.neobytesolutions.com/invisiblesecrets/index.html)

Invisible Secrets 是一个数据隐藏工具,能将一些重要数据隐藏在 5 种不同类型的文件中,这 5 种文件包括:.JPEG、.PNG、.BMP、.HTML 和.WAV。

## 6 结束语

计算机反取证就是删除或者隐藏入侵证据使取证工作无效。目前的计算机反取证技术主要有数据擦除、数据隐藏、数据加密等。对于计算机取证人员来说,研究计算机反取证技术意义非常重大,一方面可以了解入侵者有哪些常用手段用来掩盖甚至擦除入侵痕迹;另一方面可以在了解这些手段的基础上,开发出更加有效、实用的计算机取证工具,从而加大对计算机犯罪的打击力度,保证信息系统的安全性。

## 参考文献


1 Defeating Forensics Analysis on Unix. http://www.phrack.org/show.php?p=59&a=6. 2004.

2 Forensics and Anti-Forensics Tools. http://www.giac.org/practicals/GSEC/Taref-Alkari-GSEC.pdf. 2004.

3 Anti-forensics. http://www.aversion.net/presentations/HTCIA-02/anti-forensics.ppt. 2004.

4 The Art of Defiling. http://www.blackhat.com/presentations/bh-asia-03/bh-asia-03-grugq/bh-asia-03-grugq.pdf. 2004

5 Forensics and Anti-Forensics Computing. http://www.fukt.bth.se/~uncle/papers/forensics200212.pdf. 2005.

6 Anti-Forensics Tools. http://www.networkintrusion.co.uk/foranti.htm. 2005.

7 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。

8 [美]Warren G. Kruse II, Jay G. Heiser 著,段海新等译. 计算机取证:应急响应精要. 人民邮电出版社,2003。