

# 获取非易变数据

开机取证过程中，并不局限于易变信息。有时也需要收集一些重启后还存在的永久信息，例如，注册表键的内容和文件。因为调查员需要快速得到一些信息用于分析，或者是由于入侵者还登陆在系统上。这样的案子中，调查员可能让机器一直运行并在线，用于追踪攻击者（或僵尸网络），同时他也需要保存特定的信息，以防信息被修改或删除。

系统启动时，一些内容会被更改，例如，驱动器映射或者被映射的信息、启动的服务、安装的应用等。这些更改在启动后不会再存在，因而有必要记录在调查文档中。

## 1、注册表设置

一些注册表键值和设置会影响随后的取证分析与调查。虽然这些设置本身是非易变信息，他们还是会影响调查员的处理过程和决定，甚至会影响是否继续调查的决定。

### **ClearPageFileAtShutdown**

这个特殊的注册表值告诉操作系统关机时清除页交换文件。Windows 使用虚拟内存架构，一些进程使用的内存内容会被交换出去，位于交换文件中。系统关闭时，交换文件中的信息会在硬盘上保持不变，其中可能会有解密的密码、聊天会话信息和其他字符串信息，为调查提供重要的线索。然而，如果关机时清楚了交换文件，这些潜在的线索信息就很难再提取。

### **DisableLastAccess**

Windows 可以禁用文件最后访问时间的修改。这会提高系统性能，尤其是

对使用频繁的文件服务器。对普通的工作站或者类似的日常使用的台式机、笔记本不会有明显的性能提升。Windows 2003 中，将下列键值设为 1：

HKEY\_LOCAL\_MACHINE\System\CurrentControlSet\Control\FileSystem\Disablelastaccess。根据 Microsoft 的 Windows2003 性能调整指南文档，这个键值默认并不存在，必须由用户创建。

## 2、事件日志

这里采集的事件日志主要包括系统日志、服务器日志、数据库日志、防火墙日志等。

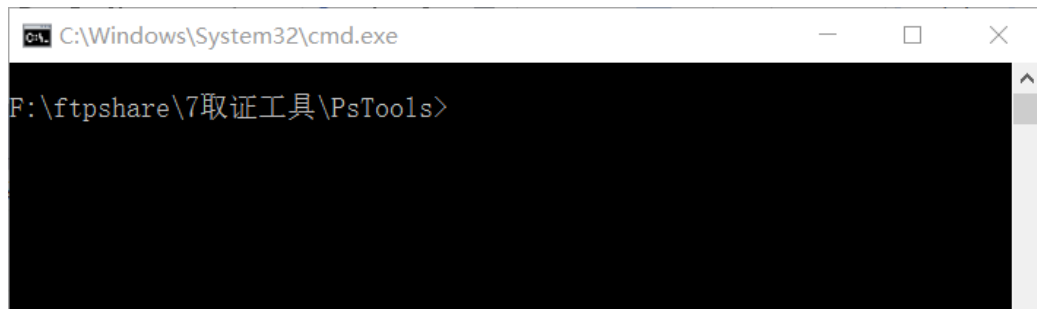
事件日志文件必然存在于文件系统中，而且其内容可能改变。事实上，根据审计策略的配置情况，事件日志会快速发生改变。

依赖于“对象”系统中审计策略的配置情况，以及在现场响应时的操作，调查人员的活动也可能记录在事件日志中。例如，如果调查员决定从远程来访问系统收集信息，那么如果设置了正确的审计策略，则远程登录的每次情况都会记录在安全事件日志中。如果由调查动作生成的日志足够多，则可能覆盖调查所需要的其他有价值的日志信息。Psloglist.exe 和 WDumpEvt 2.2 工具可以用来获取日志记录数据，或者直接将系统中的.evt 或.evtx 文件复制出来。

像服务器日志（如 IIS 日志、Apache 日志、Nginx 日志等）可以直接拷贝复制出来。

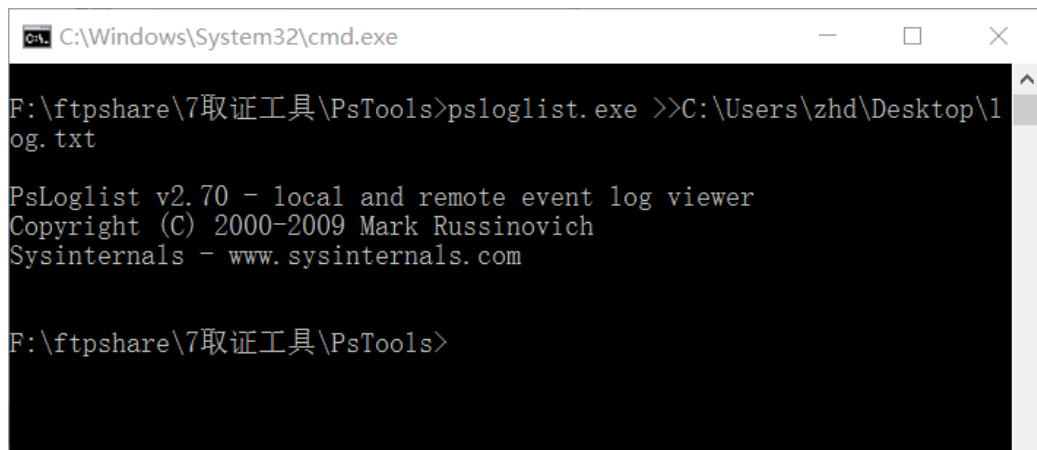
### 相获取系统日志实验

- 1、首先打开 cmd 命令窗口，切换至 Psloglist.exe 目录。



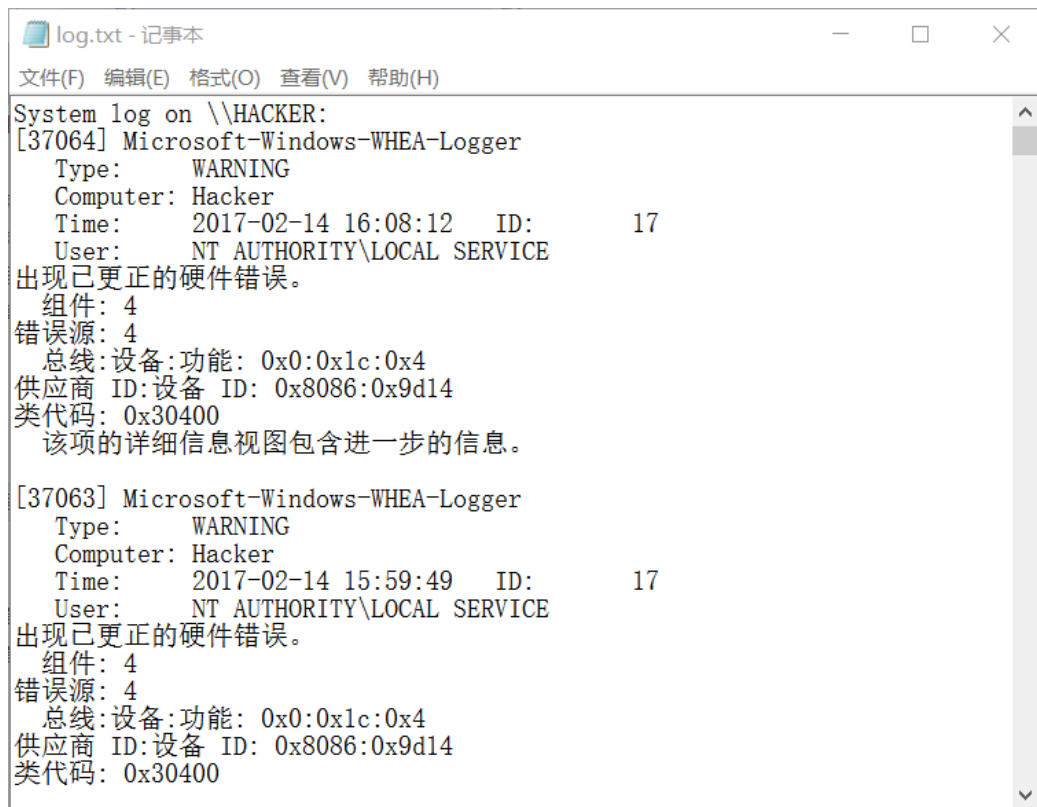
```
C:\Windows\System32\cmd.exe
F:\ftpshare\7取证工具\PsTools>
```

2、输入命令 `psloglist.exe >>C : \Users\zhd\Desktop\log.txt`。



```
C:\Windows\System32\cmd.exe
F:\ftpshare\7取证工具\PsTools>psloglist.exe >>C:\Users\zhd\Desktop\log.txt
PsLoglist v2.70 - local and remote event log viewer
Copyright (C) 2000-2009 Mark Russinovich
Sysinternals - www.sysinternals.com
F:\ftpshare\7取证工具\PsTools>
```

3、打开 `C : \Users\zhd\Desktop\log.txt` , 查看分析日志。



```
log.txt - 记事本
文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)
System log on \\HACKER:
[37064] Microsoft-Windows-WHEA-Logger
  Type:      WARNING
  Computer:  Hacker
  Time:      2017-02-14 16:08:12   ID:      17
  User:      NT AUTHORITY\LOCAL SERVICE
出现已更正的硬件错误。
  组件: 4
  错误源: 4
  总线:设备:功能: 0x0:0x1c:0x4
  供应商 ID:设备 ID: 0x8086:0x9d14
  类代码: 0x30400
  该项的详细信息视图包含进一步的信息。

[37063] Microsoft-Windows-WHEA-Logger
  Type:      WARNING
  Computer:  Hacker
  Time:      2017-02-14 15:59:49   ID:      17
  User:      NT AUTHORITY\LOCAL SERVICE
出现已更正的硬件错误。
  组件: 4
  错误源: 4
  总线:设备:功能: 0x0:0x1c:0x4
  供应商 ID:设备 ID: 0x8086:0x9d14
  类代码: 0x30400
```

### 3、元数据

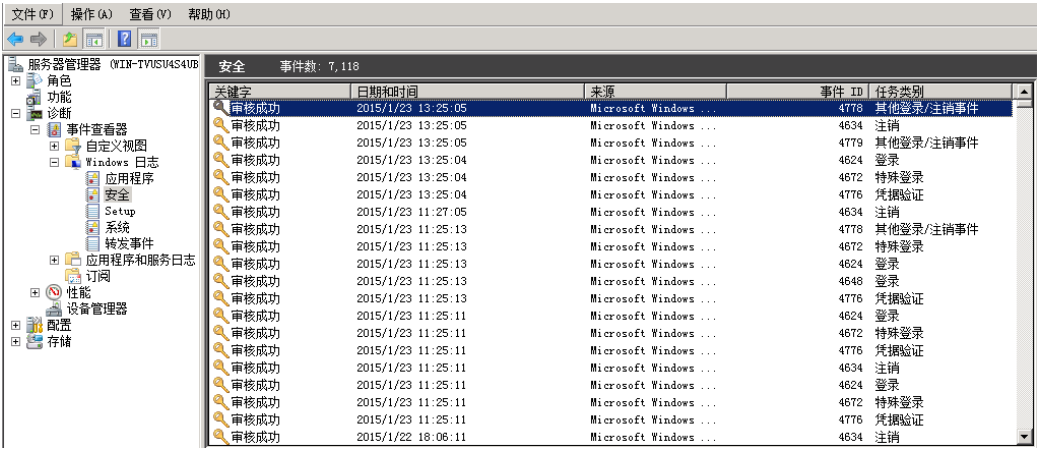
犯罪分子及有机可将自己的作案记录、联系人、通信方式、交易信息等存放在诸如记事本文件、Word 文件、Excel 文件、PPT 文件、音频文件、视频文件、图片文件等文件中，在数据采集时，不应忽视任何可疑文件。

### 4、脚印信息

攻击者在登陆网站后台或者获取 webshell 以及登陆服务器后，难免会留下一些记录，即为入侵的脚印信息。有经验的黑客会极力抹去自己的操作痕迹以躲避追查，那么是不是就没有办法找到他们的脚印呢？下面将由浅入深的了解一下如何收集脚印信息。

以模拟真实入侵的方法为主线，反向收集脚印信息：

当黑客获得服务器权限时，第一步便是登陆服务器，首先查看服务器登录日志：



The screenshot shows the Windows Event Viewer interface. The left pane displays the 'Security' log under 'Windows Logs'. The right pane shows a list of events. The table below represents the data visible in the event list.

时间戳	日期和时间	来源	事件 ID	任务类别
审核成功	2015/1/23 13:25:05	Microsoft Windows ...	4778	其他登录/注销事件
审核成功	2015/1/23 13:25:05	Microsoft Windows ...	4634	注销
审核成功	2015/1/23 13:25:05	Microsoft Windows ...	4779	其他登录/注销事件
审核成功	2015/1/23 13:25:04	Microsoft Windows ...	4624	登录
审核成功	2015/1/23 13:25:04	Microsoft Windows ...	4672	特殊登录
审核成功	2015/1/23 13:25:04	Microsoft Windows ...	4776	凭据验证
审核成功	2015/1/23 11:27:05	Microsoft Windows ...	4634	注销
审核成功	2015/1/23 11:25:13	Microsoft Windows ...	4778	其他登录/注销事件
审核成功	2015/1/23 11:25:13	Microsoft Windows ...	4672	特殊登录
审核成功	2015/1/23 11:25:13	Microsoft Windows ...	4624	登录
审核成功	2015/1/23 11:25:13	Microsoft Windows ...	4648	登录
审核成功	2015/1/23 11:25:13	Microsoft Windows ...	4776	凭据验证
审核成功	2015/1/23 11:25:11	Microsoft Windows ...	4624	登录
审核成功	2015/1/23 11:25:11	Microsoft Windows ...	4672	特殊登录
审核成功	2015/1/23 11:25:11	Microsoft Windows ...	4776	凭据验证
审核成功	2015/1/23 11:25:11	Microsoft Windows ...	4634	注销
审核成功	2015/1/23 11:25:11	Microsoft Windows ...	4624	登录
审核成功	2015/1/23 11:25:11	Microsoft Windows ...	4672	特殊登录
审核成功	2015/1/23 11:25:11	Microsoft Windows ...	4776	凭据验证
审核成功	2015/1/22 18:06:11	Microsoft Windows ...	4634	注销

查看有无异常登陆（异常时间，异常用户）

黑客登陆之后，可能会尝试删除从 WEB 入侵的记录，因此 web 服务日志将可能被删除或修改：

名称	修改日期	类型	大小
u_ex150106.log	2015/1/7 7:26	文本文档	305 KB
u_ex150107.log	2015/1/8 7:53	文本文档	315 KB
u_ex150108.log	2015/1/9 7:55	文本文档	2,474 KB
u_ex150109.log	2015/1/10 6:37	文本文档	58 KB
u_ex150110.log	2015/1/11 7:42	文本文档	36 KB
u_ex150111.log	2015/1/12 7:04	文本文档	26 KB
u_ex150112.log	2015/1/13 7:30	文本文档	54 KB
u_ex150113.log	2015/1/14 7:24	文本文档	34 KB
u_ex150114.log	2015/1/15 5:33	文本文档	20 KB
u_ex150115.log	2015/1/16 7:30	文本文档	33 KB
u_ex150116.log	2015/1/16 16:06	文本文档	62 KB
u_ex150119.log	2015/1/19 14:33	文本文档	6 KB
u_ex150120.log	2015/1/21 5:36	文本文档	1 KB
u_ex150121.log	2015/1/21 9:28	文本文档	18 KB
u_ex150122.log	2015/1/22 14:40	文本文档	39 KB

查看日志文件有无被修改或删除（异常修改时间，异常大小）

以 IIS 为例，如果 WEB 日志被删除，可以在系统日志中查找来自 W3SVC 的警告信息，或许可以找到一些线索。

攻击者在侵入系统之后，难免会留下一些痕迹，有经验的攻击者会刻意抹去这些痕迹，那么我们是不是就没办法了呢？我们可以通过一些软件来收集这一部分信息。

目前，国际上的主流产品有：

Forensic Toolkit：是一系列基于命令行的工具，可以帮助推断 Windows NT 文件系统中的访问行为。这些程序包括的命令有：AFind（根据最后访问时间给出文件列表，而这并不改变目录的访问时间）、HFind（扫描磁盘中有隐藏属性的文件）、SFind（扫描整个磁盘寻找隐藏的数据流）、FileStat（报告所有单独文件的属性）、NTLast（提供标准的 GUI 事件浏览器之外对每一个会话都记录了登录及登出时间，并且它能够指出登录是远程的还是本地的）。

The Coroner's Toolkit (TCT)：主要用来调查被“黑”的 Unix 主机，它提供了强大的调查能力，它的特点是可以对运行着的主机的活动进行分析，并捕

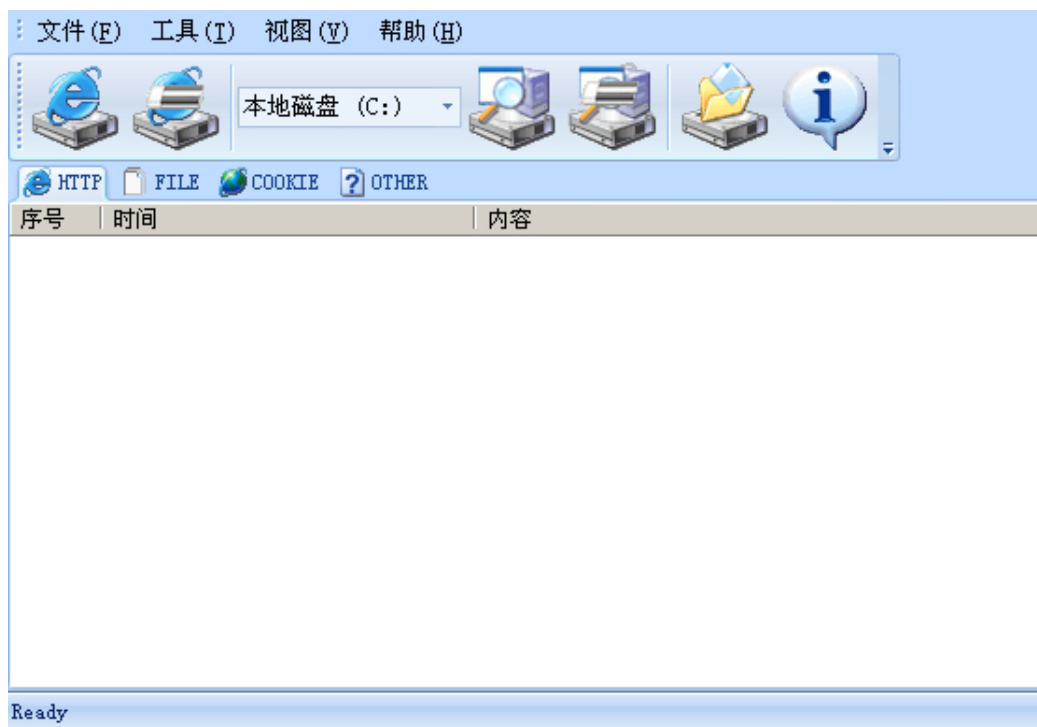
获目前的状态信息。其中的 grove-robber 可以收集大量的正在运行的进程、网络连接以及硬盘驱动器方面的信息。数据基本上以挥发性顺序收集,收集所有的数据是个很缓慢的过程,要花上几个小时的时间。TCT 还包括数据恢复和浏览工具 unrm&lazarus、获取 MAC 时间的工具 mactime。还包括一些小工具,如 ils(用来显示被删除的索引节点的原始资料)、icat(用于取得特定的索引节点对应的文件的内容)等等。

EnCase :自称是唯一一个完全集成的基于 Windows 界面的取证应用程序,其功能包括:数据浏览、搜索、磁盘浏览、数据预览、建立案例、建立证据文件、保存案例等。

ForensicX :主要运行于 Linux 环境,是一个以收集数据及分析数据为主要目的的工具。它与配套的硬件组成专门工作平台。它利用了 Linux 支持多种文件系统的特点,提供在不同的文件系统里自动装配映像等能力、能够发现分散空间里的数据、可以分析 Unix 系统是否含有木马程序。其中的 Webtrace 可以自动搜索互联网上的域名,为网络取证进行必要的收集工作,新版本具有识别隐藏文件的工具。

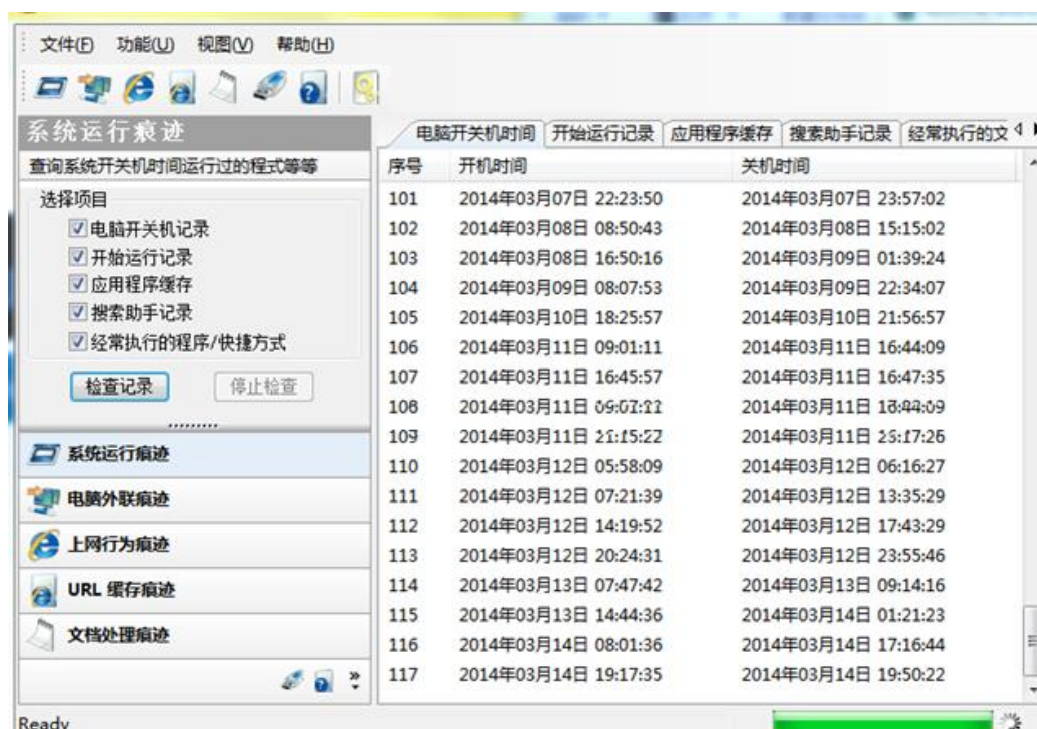
## **上网痕迹**

使用 UrlViewer 工具检查上网痕迹



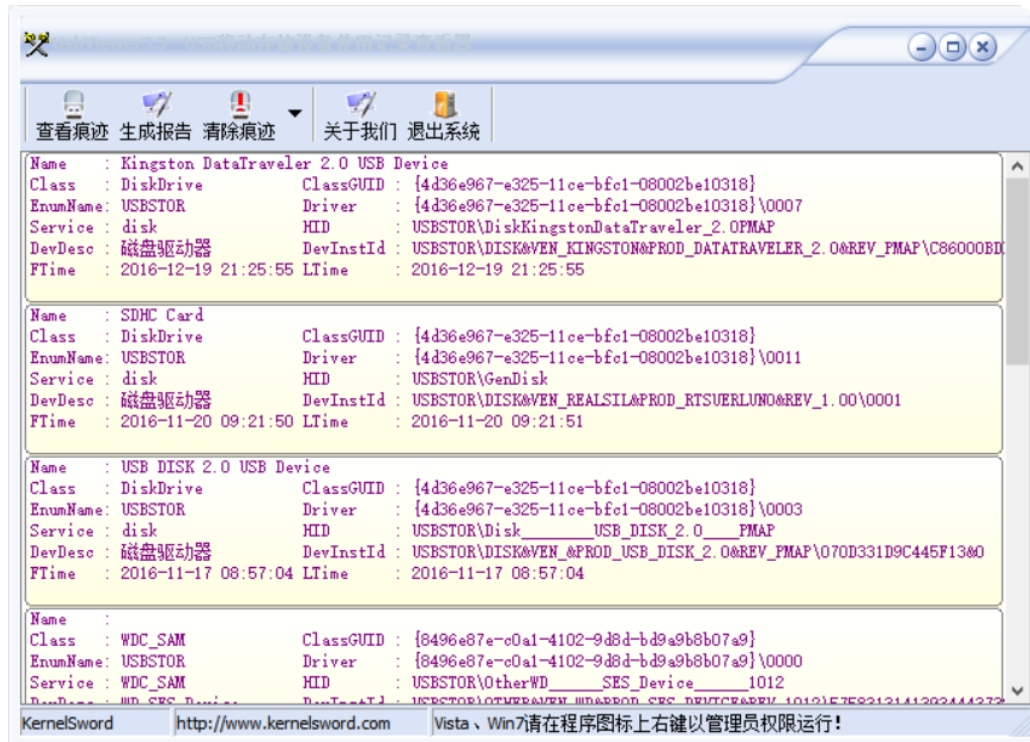
## 系统运行痕迹

使用 RG 涉密信息检查工具获取运行痕迹



## 外接设备痕迹

使用 UsbViewer 检测外接设备连接痕迹



## 系统账户

通过 net user 命令查看是否有多余账户

