**7906ICT Digital Forensics**

**Tutorial 2.2 – Disk Forensics**

The aim of this tutorial is to give you some experience with the forensic process for disk images. We will cover some of the topics raised in the Lecture, but there are many more techniques you are open to explore. Please note that this tutorial is not a step by step guide. The expectations are that if you are not sure of how to do something, you should find out via internet search or by asking your tutor.

# Preliminaries

There are two options for doing the practical component of this tutorial. You can do this tutorial by logging into the Griffith Cyber Range which is an Internet isolated set of virtual machines that has been set up on the Griffith network. The other is to download and install the software on your local PC.

## Set Up Option 1 – Griffith Cyber Range

If you are not on a Griffith University campus need to VPN into the Griffith Network. Details of how to VPN into the Griffith Network can be found here: https://intranet.secure.griffith.edu.au/computing/remote-access/virtual-private-network. Go to the bottom of the page and find the instructions for your device.

Once you have set up your VPN to the Griffith network, you can use your browser to go to the following page: https://cyber.ict.griffith.edu.au/

The credentials for the Griffith Cyber Range Server are:

**Username: sXXXXXXX**

**Password: changeme**

sXXXXXXX is your Griffith username. When you log in for the first time change your password (which you will need to remember). To do this go to your username menu on the top right corner of the web page and select the Settings item. The Settings page will allow you to reset your password. Once you have reset the password, use your new password for subsequent logins. For this tutorial we will be using the SIFT workstation. Click on the SIFT link and you will be connected to a virtual machine running the SANS SIFT workstation Linux distribution.

When you have finished your tutorial simply close the browser tab with the connection to the virtual machine. Or press Shift-Ctrl-Alt to access the web menu and disconnect from the Griffith Cyber Range.

## Set Up Option 2 – Install on your local PC

The other option is to install the SIFT workstation on your local PC. Links to the virtual machine OVA file for download are found on the Learning@Griffith web site. **Note:** The SIFT workstation is a 15GB download. You will need to install VirtualBox and select File->Import Appliance to install the SIFT workstation Virtual machine. Start the Virtual Machine and log in.

The login credentials for the SIFT workstation are:

**Username: sansforensics**

**Password: forensics**

# Disk Forensics Scenario

The following is a well-known digital forensics training scenario.

On 09/20/04, a Dell CPi notebook computer, serial # VLQLW, was found abandoned along with a wireless PCMCIA card and an external homemade 802.11b antennae. It is suspected that this computer was used for hacking purposes, although cannot be tied to a hacking suspect, Greg Schardt. Schardt also goes by the online nickname of “Mr. Evil” and some of his associates have said that he would park his vehicle within range of Wireless Access Points (like Starbucks and other T-Mobile Hotspots) where he would then intercept internet traffic, attempting to get credit card numbers, usernames & passwords.

Find any hacking software, evidence of their use, and any data that might have been generated. Attempt to tie the computer to the suspect, Greg Schardt.

A DD image (in seven parts: 1, 2, 3, 4, 5, 6, 7, 8, and notes) and a EnCase image (second part) of the abandoned computer have already been made.

# Evidence

Assuming that the correct evidence has been identified and collected, the next step is to download the disk image onto the SIFT workstation virtual machine.

1. If you are using the Griffith Cyber Range, your virtual machines are isolated from the Internet but you can download the evidence for this tutorial from [http://forensic-tutorials.griffith.internal](http://forensic-tutorials.griffith.internal/) in the *tutorial2.2* directory. If you are using your own local SIFT workstation you can download the evidence from the link provided in the

Learning@Griffith page for this tutorial. It is a 2.5Gb download.

**Answer:**

Answer

1. Create a directory in the /cases directory called schardt and unzip the file here.

**Answer:**

Answer

1. Concatenate the DD image files into one file using the cat command.

**Answer:**

Answer

1. What is the image hash?

**Answer:**

Answer

sansforensics@siftworkstation: ~

$ mv '/home/sansforensics/Downloads/Tutorial2.2.zip' /home/sansforensics/Desktop/cases/

sansforensics@siftworkstation: ~

$ mkdir schardt

sansforensics@siftworkstation: ~

$ cd /home/sansforensics/Desktop/cases/

sansforensics@siftworkstation: ~/Desktop/cases

$ mkdir schardt

sansforensics@siftworkstation: ~/Desktop/cases

$ mv '/home/sansforensics/Desktop/cases/Tutorial2.2.zip' '/home/sansforensics/Desktop/cases/schardt'

sansforensics@siftworkstation: ~/Desktop/cases

$ cd schardt/

sansforensics@siftworkstation: ~/Desktop/cases/schardt

$ unzip schardt

unzip: cannot find or open schardt, schardt.zip or schardt.ZIP.

sansforensics@siftworkstation: ~/Desktop/cases/schardt

$ unzip schardt.zip

unzip: cannot find or open schardt.zip, schardt.zip.zip or schardt.zip.ZIP.

sansforensics@siftworkstation: ~/Desktop/cases/schardt

$ unzip Tutorial2.2.zip

Archive: Tutorial2.2.zip

inflating: 4Dell Latitude CPi.E01

inflating: 4Dell Latitude CPi.E02

inflating: SCHARDT.001

inflating: SCHARDT.002

inflating: SCHARDT.003

inflating: SCHARDT.004

inflating: SCHARDT.005

inflating: SCHARDT.006

inflating: SCHARDT.007

inflating: SCHARDT.008

inflating: SCHARDT.LOG

sansforensics@siftworkstation: ~/Desktop/cases/schardt

$ cat SCHARDT.001 SCHARDT.002 SCHARDT.003 SCHARDT.004 SCHARDT.005 SCHARDT.006 SCHARDT.007 SCHARDT.008 > schardt.dd

sansforensics@siftworkstation: ~/Desktop/cases/schardt

$ img\_stat schardt.dd

IMAGE FILE INFORMATION

--------------------------------------------

Image Type: raw

Size in bytes: 4871301120

Sector size: 512

sansforensics@siftworkstation: ~/Desktop/cases/schardt

$ ls -al

total 12658180

drwxr-xr-x 2 sansforensics sansforensics 4096 Aug 28 13:23 .

drwxrwxr-x 3 sansforensics root 4096 Aug 28 13:13 ..

-rw-r--r-- 1 sansforensics sansforensics 671094597 Jul 3 2019 '4Dell Latitude CPi.E01'

-rw-r--r-- 1 sansforensics sansforensics 419384951 Jul 3 2019 '4Dell Latitude CPi.E02'

-rw-r--r-- 1 sansforensics sansforensics 666238976 Jul 3 2019 SCHARDT.001

-rw-r--r-- 1 sansforensics sansforensics 666238976 Jul 3 2019 SCHARDT.002

-rw-r--r-- 1 sansforensics sansforensics 666238976 Jul 3 2019 SCHARDT.003

-rw-r--r-- 1 sansforensics sansforensics 666238976 Jul 3 2019 SCHARDT.004

-rw-r--r-- 1 sansforensics sansforensics 666238976 Jul 3 2019 SCHARDT.005

-rw-r--r-- 1 sansforensics sansforensics 666238976 Jul 3 2019 SCHARDT.006

-rw-r--r-- 1 sansforensics sansforensics 666238976 Jul 3 2019 SCHARDT.007

-rw-r--r-- 1 sansforensics sansforensics 207628288 Jul 3 2019 SCHARDT.008

-rw-r--r-- 1 sansforensics sansforensics 4871301120 Aug 28 13:23 schardt.dd

-rw-r--r-- 1 sansforensics sansforensics 4608 Jul 3 2019 SCHARDT.LOG

-rw-r--r-- 1 sansforensics sansforensics 2128823960 Aug 28 13:07 Tutorial2.2.zip

sansforensics@siftworkstation: ~/Desktop/cases/schardt

$ ssdeep schardt.dd

ssdeep,1.1--blocksize:hash:hash,filename

25165824:XQmR1vitjs+Uhu7dKCkh7PATsEMUtxC01b:NRd+FydMx1b,"/cases/schardt/schardt.dd"

sansforensics@siftworkstation: ~/Desktop/cases/schardt

$ md5sum schardt.dd

aee4fcd9301c03b3b054623ca261959a schardt.dd

sansforensics@siftworkstation: ~/Desktop/cases/schardt

# Examination

At this stage of the investigation you should examine the disk image. This will help you access the image in the analysis phase of the investigation.

1. Use Sleuth kit to examine the image file format status.

**Answer:**

sansforensics@siftworkstation: ~/Desktop/cases/schardt

$ img\_stat schardt.dd

IMAGE FILE INFORMATION

--------------------------------------------

Image Type: raw

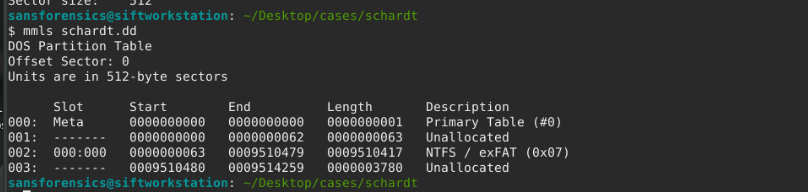
Size in bytes: 4871301120

Sector size: 512

sansforensics@siftworkstation: ~/Desktop/cases/schardt

1. Which Sleuth kit command will display the layout of the disk? Use it to identify partitions and unallocated space.

**Answer:**

****

sansforensics@siftworkstation: ~/Desktop/cases/schardt

$ mmls schardt.dd

DOS Partition Table

Offset Sector: 0

Units are in 512-byte sectors

Slot Start End Length Description

000: Meta 0000000000 0000000000 0000000001 Primary Table (#0)

001: ------- 0000000000 0000000062 0000000063 Unallocated

002: 000:000 0000000063 0009510479 0009510417 NTFS / exFAT (0x07)

003: ------- 0009510480 0009514259 0000003780 Unallocated

sansforensics@siftworkstation: ~/Desktop/cases/schardt

1. Display the detailed file system status using fsstat.

**Answer:**

sansforensics@siftworkstation: ~/Desktop/cases/schardt

$ fsstat -o 63 schardt.dd

FILE SYSTEM INFORMATION

--------------------------------------------

File System Type: NTFS

Volume Serial Number: B26CB1CE6CB18D9B

OEM Name: NTFS

Version: Windows XP

METADATA INFORMATION

--------------------------------------------

First Cluster of MFT: 2097152

First Cluster of MFT Mirror: 4755208

Size of MFT Entries: 1024 bytes

Size of Index Records: 4096 bytes

Range: 0 - 12305

Root Directory: 5

CONTENT INFORMATION

--------------------------------------------

Sector Size: 512

Cluster Size: 512

Total Cluster Range: 0 - 9510415

Total Sector Range: 0 - 9510415

$AttrDef Attribute Values:

$STANDARD\_INFORMATION (16) Size: 48-72 Flags: Resident

$ATTRIBUTE\_LIST (32) Size: No Limit Flags: Non-resident

$FILE\_NAME (48) Size: 68-578 Flags: Resident,Index

$OBJECT\_ID (64) Size: 0-256 Flags: Resident

$SECURITY\_DESCRIPTOR (80) Size: No Limit Flags: Non-resident

$VOLUME\_NAME (96) Size: 2-256 Flags: Resident

$VOLUME\_INFORMATION (112) Size: 12-12 Flags: Resident

$DATA (128) Size: No Limit Flags:

$INDEX\_ROOT (144) Size: No Limit Flags: Resident

$INDEX\_ALLOCATION (160) Size: No Limit Flags: Non-resident

$BITMAP (176) Size: No Limit Flags: Non-resident

$REPARSE\_POINT (192) Size: 0-16384 Flags: Non-resident

$EA\_INFORMATION (208) Size: 8-8 Flags: Resident

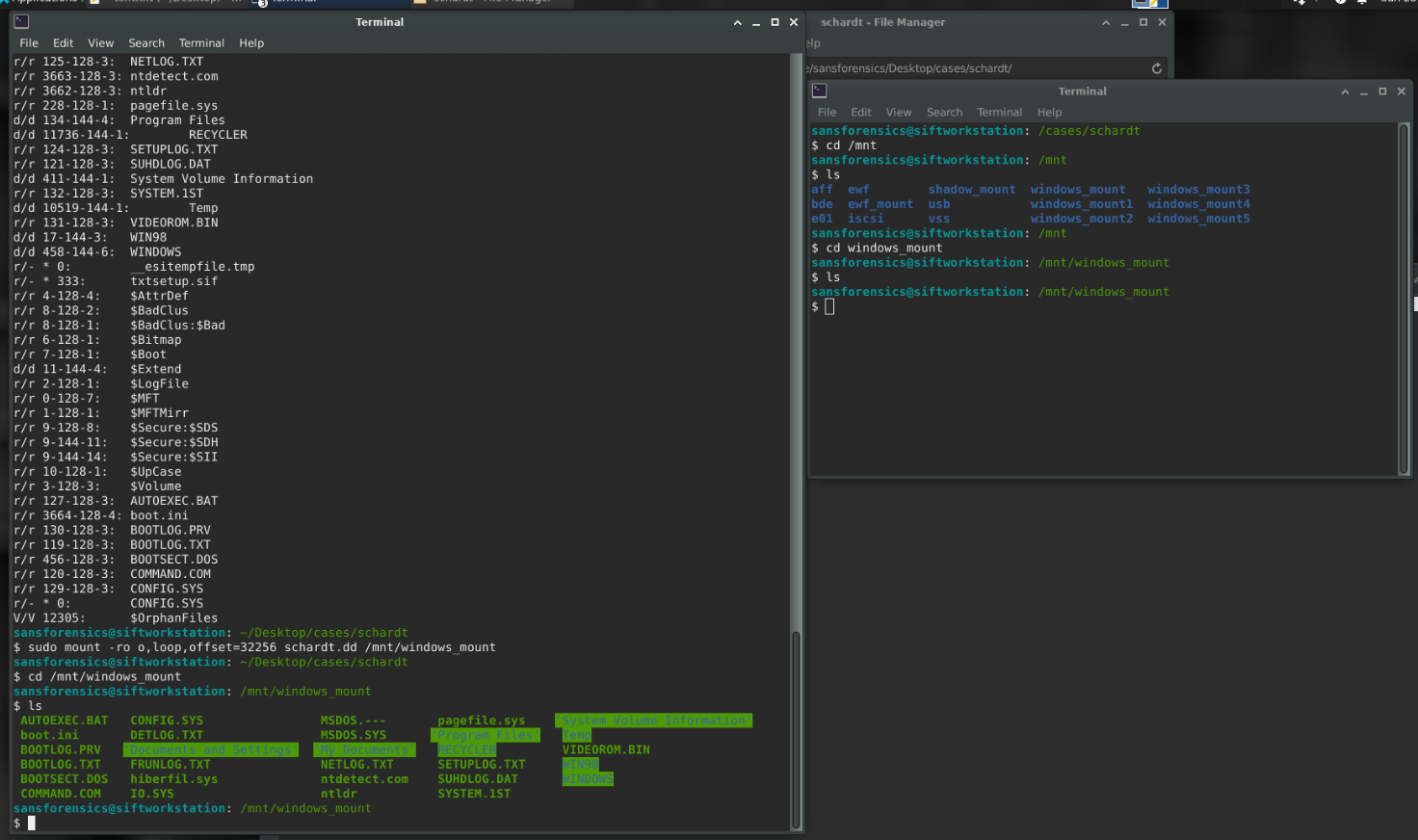
$EA (224) Size: 0-65536 Flags:

$LOGGED\_UTILITY\_STREAM (256) Size: 0-65536 Flags: Non-resident

sansforensics@siftworkstation: ~/Desktop/cases/schardt

1. Mount the dd image so you can access it as a disk to the /mnt/windows\_mount mount point. Note you may need to identify the offset when the partition begins. It is also good practice to mount the disk read only.

**Answer:**



sansforensics@siftworkstation: ~/Desktop/cases/schardt

$ sudo mount -ro o,loop,offset=32256 schardt.dd /mnt/windows\_mount

sansforensics@siftworkstation: ~/Desktop/cases/schardt

$ cd /mnt/windows\_mount

sansforensics@siftworkstation: /mnt/windows\_mount

$ ls

AUTOEXEC.BAT CONFIG.SYS MSDOS.--- pagefile.sys 'System Volume Information'

boot.ini DETLOG.TXT MSDOS.SYS 'Program Files' Temp

BOOTLOG.PRV 'Documents and Settings' 'My Documents' RECYCLER VIDEOROM.BIN

BOOTLOG.TXT FRUNLOG.TXT NETLOG.TXT SETUPLOG.TXT WIN98

BOOTSECT.DOS hiberfil.sys ntdetect.com SUHDLOG.DAT WINDOWS

COMMAND.COM IO.SYS ntldr SYSTEM.1ST

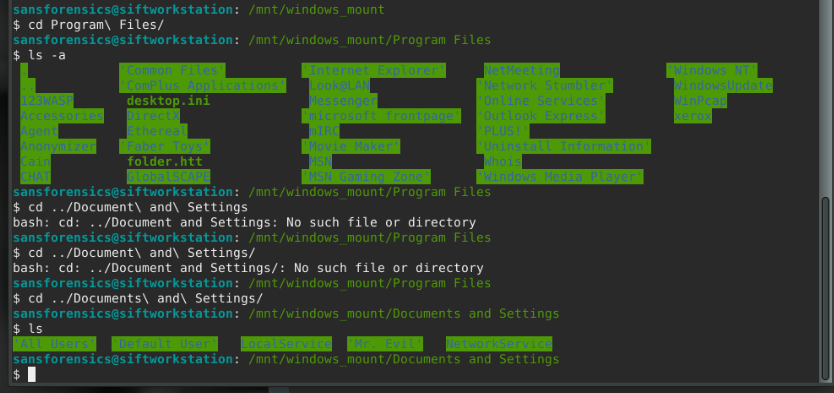
sansforensics@siftworkstation: /mnt/windows\_mount

# Analysis

Most of the analysis in this tutorial will use RegRipper and its plugins. We will use this tool to examine the registry in the image and find the evidence we need for the Schardt case.

1. Run the rip.pl command line tool and list the available plugins.

**Answer:**



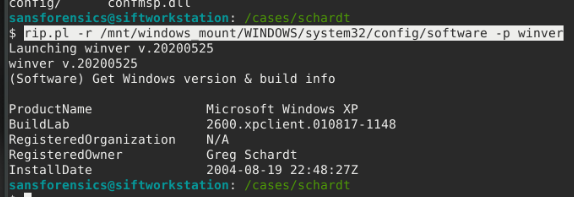
rip.pl -l

Use these plugins and other tools you learnt from last week to find answers for the following:

1. What operating system was used on the computer?

**Answer:**

rip.pl -r /mnt/windows\_mount/WINDOWS/system32/config/software -p winver



sansforensics@siftworkstation: /cases/schardt

$ rip.pl -r /mnt/windows\_mount/WINDOWS/system32/config/software -p winver

Launching winver v.20200525

winver v.20200525

(Software) Get Windows version & build info

ProductName Microsoft Windows XP

BuildLab 2600.xpclient.010817-1148

RegisteredOrganization N/A

RegisteredOwner Greg Schardt

InstallDate 2004-08-19 22:48:27Z

sansforensics@siftworkstation: /cases/schardt

1. When was the install date?

**Answer:**

2004-08-19 22:48:27Z

1. What is the time zone settings?

**Answer:**

sansforensics@siftworkstation: /cases/schardt

$ rip.pl -l | grep zone

230. timezone v.20200518 [System]

sansforensics@siftworkstation: /cases/schardt

$ rip.pl -r /mnt/windows\_mount/WINDOWS/system32/config/system -p timezone

Launching timezone v.20200518

timezone v.20200518

(System) Get TimeZoneInformation key contents

TimeZoneInformation key

ControlSet001\Control\TimeZoneInformation

LastWrite Time 2004-08-19 17:20:02Z

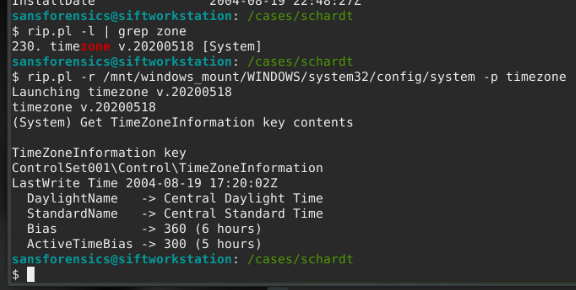
DaylightName -> Central Daylight Time

StandardName -> Central Standard Time

Bias -> 360 (6 hours)

ActiveTimeBias -> 300 (5 hours)

sansforensics@siftworkstation: /cases/schardt



1. Who is the registered owner?

**Answer:**

$ rip.pl -r /mnt/windows\_mount/WINDOWS/system32/config/software -p winver

…………………………

RegisteredOwner Greg Schardt

1. What is the computer hostname?

**Answer:**

sansforensics@siftworkstation: /cases/schardt

$ rip.pl -l | grep -C 5 ostname

243. termcert v.20200526 [System]

- Gets Terminal Server certificate

244. compname v.20090727 [System]

- Gets ComputerName and Hostname values from System hive

245. lxss\_tln v.20140723 [NTUSER.DAT]

- Gets WSL config.

sansforensics@siftworkstation: /cases/schardt

$ rip.pl -r /mnt/windows\_mount/WINDOWS/system32/config/system -p compname

Launching compname v.20090727

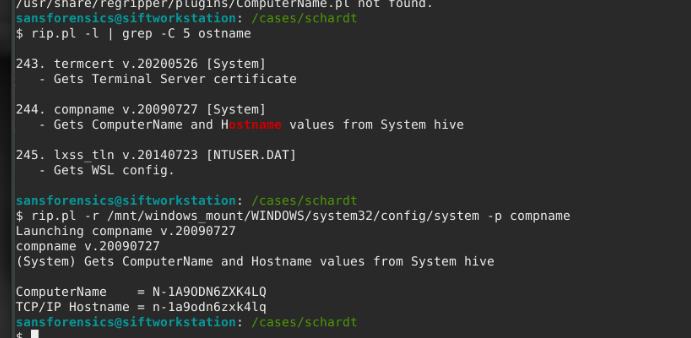
compname v.20090727

(System) Gets ComputerName and Hostname values from System hive

ComputerName = N-1A9ODN6ZXK4LQ

TCP/IP Hostname = n-1a9odn6zxk4lq

sansforensics@siftworkstation: /cases/schardt



1. When was the last recorded computer shutdown date/time?

**Answer:**

sansforensics@siftworkstation: /cases/schardt

$ rip.pl -l | grep shut

23. shutdown v.20200518 [System]

sansforensics@siftworkstation: /cases/schardt

$ rip.pl -r /mnt/windows\_mount/WINDOWS/system32/config/system -p shutdown

Launching shutdown v.20200518

shutdown v.20200518

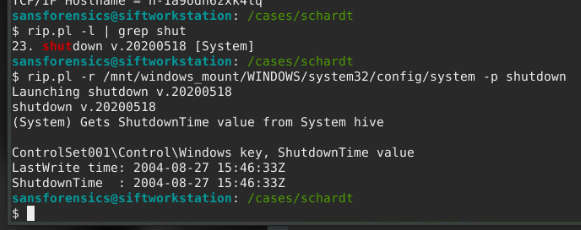
(System) Gets ShutdownTime value from System hive

ControlSet001\Control\Windows key, ShutdownTime value

LastWrite time: 2004-08-27 15:46:33Z

ShutdownTime : 2004-08-27 15:46:33Z

sansforensics@siftworkstation: /cases/schardt



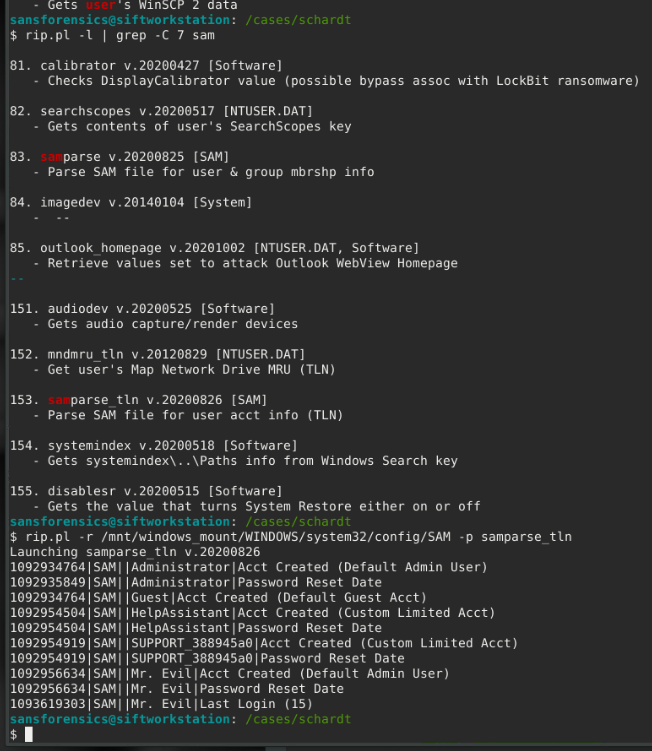
1. How many accounts are recorded (total number)?

**Answer:**

5

rip.pl -l | grep -C 7 sam

rip.pl -r /mnt/windows\_mount/WINDOWS/system32/config/SAM -p samparse\_tln



sansforensics@siftworkstation: /cases/schardt

$ rip.pl -r /mnt/windows\_mount/WINDOWS/system32/config/SAM -p samparse | grep Username

Launching samparse v.20200825

Username : Administrator [500]

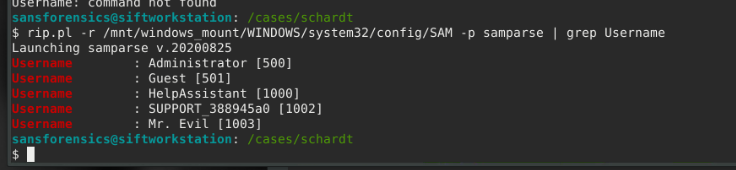
Username : Guest [501]

Username : HelpAssistant [1000]

Username : SUPPORT\_388945a0 [1002]

Username : Mr. Evil [1003]

sansforensics@siftworkstation: /cases/schardt

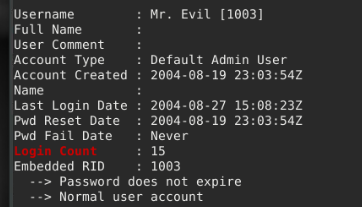


1. What is the account name of the user who mostly uses the computer?

**Answer:**

Mr. Evil

rip.pl -r /mnt/windows\_mount/WINDOWS/system32/config/SAM -p samparse | grep -C 9 "Login Count"

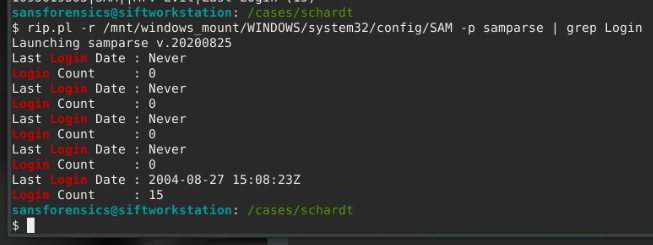


1. Who was the last user to logon to the computer?

**Answer:**

Mr. Evil

rip.pl -r /mnt/windows\_mount/WINDOWS/system32/config/SAM -p samparse | grep Login



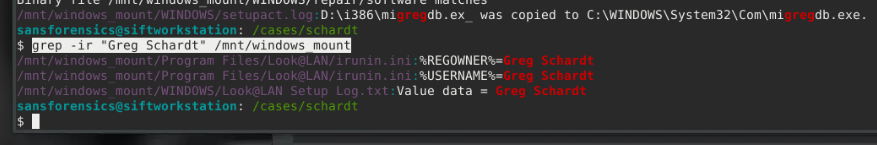
1. A search for the name of “Greg Schardt” reveals multiple hits. One of these proves that Greg Schardt is Mr. Evil and is also the administrator of this computer. What file is it? What software program does this file relate to?

**Answer:**

Proof in Q10

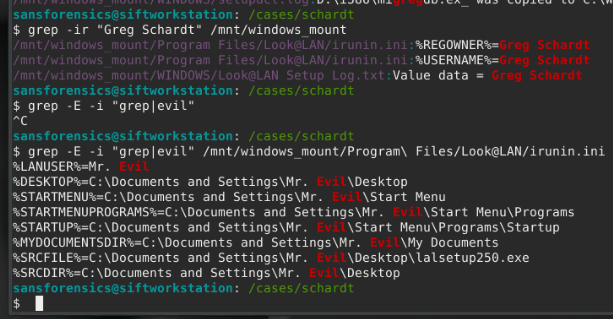
Proof in Q18 as well

grep -ir "Greg Schardt" /mnt/windows\_mount



grep -ir "Greg Schardt" /mnt/windows\_mount

grep -E -i "grep|evil"



1. Find 6 installed programs that may be used for hacking.

**Answer:**

sansforensics@siftworkstation: /cases/schardt

$ cd /mnt/windows\_mount/Program\ Files

sansforensics@siftworkstation: /mnt/windows\_mount/Program Files

$ ls

123WASP CHAT Ethereal Look@LAN MSN 'Outlook Express' 'Windows NT'

Accessories 'Common Files' 'Faber Toys' Messenger 'MSN Gaming Zone' 'PLUS!' WindowsUpdate

Agent 'ComPlus Applications' folder.htt 'microsoft frontpage' NetMeeting 'Uninstall Information' WinPcap

Anonymizer desktop.ini GlobalSCAPE mIRC 'Network Stumbler' Whois xerox

Cain DirectX 'Internet Explorer' 'Movie Maker' 'Online Services' 'Windows Media Player'

1. How many executable files are in the recycle bin?

**Answer:**

cd /mnt/windows\_mount/RECYCLER

ls

cd S-1-5-21-2000478354-688789844-1708537768-1003/

sansforensics@siftworkstation: /mnt/windows\_mount/RECYCLER/S-1-5-21-2000478354-688789844-1708537768-1003

$ ls -al

total 12107

drwxrwxrwx 1 root root 4096 Aug 27 2004 .

drwxrwxrwx 1 root root 0 Aug 25 2004 ..

-rwxrwxrwx 1 root root 2160043 Aug 25 2004 Dc1.exe

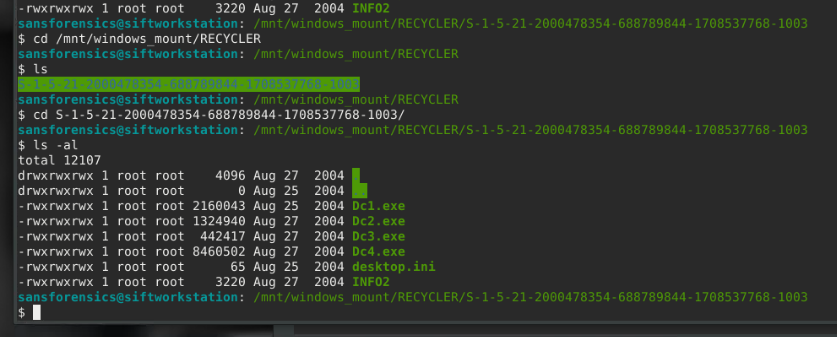
-rwxrwxrwx 1 root root 1324940 Aug 27 2004 Dc2.exe

-rwxrwxrwx 1 root root 442417 Aug 27 2004 Dc3.exe

-rwxrwxrwx 1 root root 8460502 Aug 27 2004 Dc4.exe

-rwxrwxrwx 1 root root 65 Aug 25 2004 desktop.ini

-rwxrwxrwx 1 root root 3220 Aug 27 2004 INFO2



cat INFO2

1. Are these files really deleted?

**Answer:**

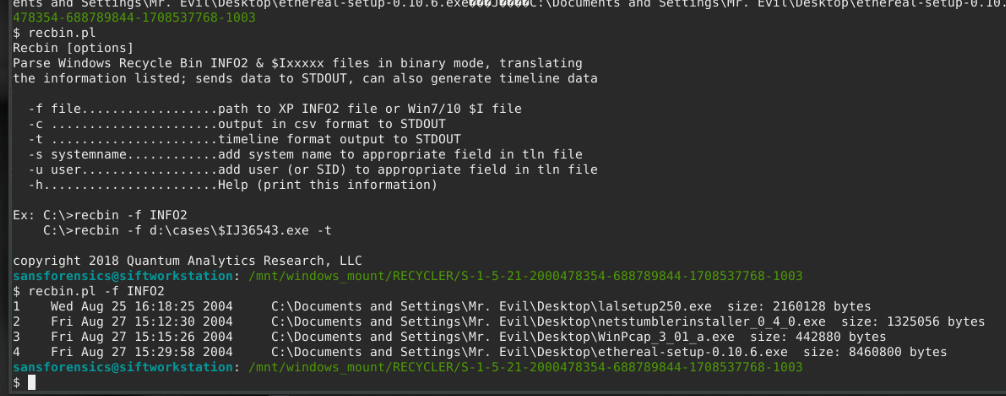
They are not deleted they are just deallocated, having their block index marked as free.

This is the case even when permanently deleted

1. What are the details of the original files found in the recycle bin?

**Answer:**

recbin.pl

recbin.pl -f INFO2

# Tutorial Quiz

You have now completed the exercises for this tutorial. You can now attempt the quiz for this tutorial.