

Lab 5: Examining the Registry

What You Need for this lab

- Install Virtualbox : <https://www.virtualbox.org/wiki/Downloads>
- Install Kali 2021.4. : <https://old.kali.org/kali-images/kali-2021.4/>
 - Notes: Suggest You configure the disk size of Kali VM 80G because the size of each leakage cases image is 30G+
 - Add new virtual harddisk size 20 GB
- Tools RegRipper 3.0
- Download DD images
 - https://www.dropbox.com/s/u4axlx8eomgwfdc/cfreds_2015_data_leakage_pc.7z.001
 - https://www.dropbox.com/s/pyq50s2cri6yftf/cfreds_2015_data_leakage_pc.7z.002
 - https://www.dropbox.com/s/cxvzuiupmqc7l99/cfreds_2015_data_leakage_pc.7z.003

Step 1.

Unzipped the DD image

```
(duanhn@duanhn)-[~/lab5]
$ 7z x cfreds_2015_data_leakage_pc.7z.001
```

Verify the unzipped DD image

```
(duanhn@duanhn)-[~/lab5]
$ ls -lh
total 26G
-rw-r--r-- 1 duanhn duanhn 2.0G Jun  4 13:06 cfreds_2015_data_leakage_pc.7z.001
-rw-r--r-- 1 duanhn duanhn 2.0G Jun  4 13:12 cfreds_2015_data_leakage_pc.7z.002
-rw-r--r-- 1 duanhn duanhn 1.1G Jun  4 13:14 cfreds_2015_data_leakage_pc.7z.003
-rw-r--r-- 1 duanhn duanhn 20G Apr 21 2015 cfreds_2015_data_leakage_pc.dd

(duanhn@duanhn)-[~/lab5]
$
```

Verify the unzipped DD image with MD5

```
(duanhn@duanhn)-[~/lab5]
$ md5sum cfreds_2015_data_leakage_pc.dd
a49d1254c873808c58e6f1bcd60b5bde cfreds_2015_data_leakage_pc.dd
```

Step 2.

Exam partitions of the DD image using *fdisk*

```
(duanhn@duanhn)-[~/lab5]
$ fdisk -l cfreds_2015_data_leakage_pc.dd

Disk cfreds_2015_data_leakage_pc.dd: 20 GiB, 21474836480 bytes, 41943040 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: dos
Disk identifier: 0xf0265720

Device                                Boot  Start      End  Sectors  Size Id Type
cfreds_2015_data_leakage_pc.dd1 *        2048    206847    204800   100M  7 HPFS/N
cfreds_2015_data_leakage_pc.dd2          206848 41940991 41734144   19.9G  7 HPFS/N

(duanhn@duanhn)-[~/lab5]
$
```

List file/directory names of the system volume

```
(duanhn@duanhn)-[~/lab5]
$ fls -o 206848 cfreds_2015_data_leakage_pc.dd | head

d/d 486-144-5: Users
d/d 13797-144-1: Documents and Settings
d/d 389-144-6: ProgramData
d/d 273-144-6: Program Files (x86)
r/r 4-128-4: $AttrDef
r/r 8-128-2: $BadClus
r/r 8-128-1: $BadClus:$Bad
r/r 6-128-4: $Bitmap
r/r 7-128-1: $Boot
d/d 11-144-4: $Extend

(duanhn@duanhn)-[~/lab5]
$
```

If your VM doesn't support auto-mounting

Create a folder as the mount point

```
(duanhn@duanhn)-[~/lab5]
$ sudo mkdir /mnt/nist_dataleak_pc_dd2/
```

Mount partition 2 to the mounting point

```
(duanhn@duanhn)-[~/lab5]
$ sudo mount -o ro,loop,offset=1048576 cfreds_2015_data_leakage_pc.dd /mnt/nist_dataleak_pc_dd2
```

Copy HKEY_LOCAL_MACHINE (Hive) files to \lab

```
(duanhn@duanhn)-[/mnt/nist_dataleak_pc_dd2/Windows/System32/config]
$ cp SAM SYSTEM SOFTWARE SECURITY DEFAULT ~/lab5/hives/
```

Verify five files

```
(duanhn@duanhn)-[~/lab5/hives]
$ ls
DEFAULT  SAM  SECURITY  SOFTWARE  SYSTEM
```

Step 3.

Verify you have the dd image

```
(duanhn@duanhn)-[~/lab5]
$ ls -l cfreds_2015_data_leakage_pc.dd
-rw-r--r-- 1 duanhn duanhn 21474836480 Apr 21 2015 cfreds_2015_data_leakage_pc.dd
```

Compute MD5 and SHA1 of the DD image

```
(duanhn@duanhn)-[~/lab5]
$ md5sum cfreds_2015_data_leakage_pc.dd
a49d1254c873808c58e6f1bcd60b5bde cfreds_2015_data_leakage_pc.dd

(duanhn@duanhn)-[~/lab5]
$ sha1sum cfreds_2015_data_leakage_pc.dd
afe5c9ab487bd47a8a9856b1371c2384d44fd785 cfreds_2015_data_leakage_pc.dd

(duanhn@duanhn)-[~/lab5]
$
```

```
root@kali:~/lab# md5sum cfreds_2015_data_leakage_pc.dd
a49d1254c873808c58e6f1bcd60b5bde cfreds_2015_data_leakage_pc.dd
root@kali:~/lab# sha1sum cfreds_2015_data_leakage_pc.dd
afe5c9ab487bd47a8a9856b1371c2384d44fd785 cfreds_2015_data_leakage_pc.dd
root@kali:~/lab#
```

Item	Detailed Information
Filename	cfreds_2015_data_leakage_pc
MD5	A49D1254C873808C58E6F1BCD60B5BDE
SHA-1	AFE5C9AB487BD47A8A9856B1371C2384D44FD785
Imaging S/W	FTK Imager 3.4.0.1
Image Format	DD converted from VMDK (Some sectors were scrubbed ⁷)
Compression	Best (Smallest)
Bytes per Sector	512
Total Sectors	41,943,040
Total Size	20.00 GB (21,474,836,480 bytes)
Compressed Size	5.05 GB (5,427,795,228 bytes) ← compressed by 7zip

Show partitions of the image

```
(duanhn@duanhn)-[~/lab5]
$ fdisk -l cfreds_2015_data_leakage_pc.dd
Disk cfreds_2015_data_leakage_pc.dd: 20 GiB, 21474836480 bytes, 41943040 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: dos
Disk identifier: 0xf0265720

Device                                Boot  Start      End  Sectors  Size Id Type
cfreds_2015_data_leakage_pc.dd1 *      2048    206847   204800   100M  7 HPFS/NTFS/e
cfreds_2015_data_leakage_pc.dd2        206848 41940991 41734144  19.9G  7 HPFS/NTFS/e

(duanhn@duanhn)-[~/lab5]
$
```

Show partitions and unallocated space using *mmls*

```
(duanhn@duanhn)-[~/lab5]
$ mmls cfreds_2015_data_leakage_pc.dd
DOS Partition Table
Offset Sector: 0
Units are in 512-byte sectors

Shortcut Slot Layout Start      End          Length      Description
000:  Meta      0000000000  0000000000  0000000001  Primary Table (#0)
001:  _____ 0000000000  0000002047  0000002048  Unallocated
002:  000:000  0000002048  0000206847  0000204800  NTFS / exFAT (0x07)
003:  000:001  0000206848  0041940991  0041734144  NTFS / exFAT (0x07)
004:  _____ 0041940992  0041943039  0000002048  Unallocated

(duanhn@duanhn)-[~/lab5]
```

Display file system statistics and metadata information from a disk image (first partition)

```
(duanhn@duanhn)-[~/lab5]
$ fsstat -b 512 -o 2048 cfreds_2015_data_leakage_pc.dd
FILE SYSTEM INFORMATION
-----
File System Type: NTFS
Volume Serial Number: 4A180A15180A0125
OEM Name: NTFS
Volume Name: System Reserved
Version: Windows XP

METADATA INFORMATION
-----
First Cluster of MFT: 8533
First Cluster of MFT Mirror: 2
Size of MFT Entries: 1024 bytes
Size of Index Records: 4096 bytes
Range: 0 - 256
Root Directory: 5

CONTENT INFORMATION
-----
Sector Size: 512
Cluster Size: 4096
Total Cluster Range: 0 - 25598
```

List the second partition details

```
(duanhn@duanhn)-[~/lab5]
$ fsstat -b 512 -o 206848 cfreds_2015_data_leakage_pc.dd
FILE SYSTEM INFORMATION
-----
File System Type: NTFS
Volume Serial Number: C8CA0C8DCA0C7A48
OEM Name: NTFS
Version: Windows XP

METADATA INFORMATION
-----
First Cluster of MFT: 786432
First Cluster of MFT Mirror: 2
Size of MFT Entries: 1024 bytes
Size of Index Records: 4096 bytes
Range: 0 - 78080
Root Directory: 5

CONTENT INFORMATION
-----
Sector Size: 512
Cluster Size: 4096
Total Cluster Range: 0 - 5216766
Total Sector Range: 0 - 41734142

$AttrDef Attribute Values:
```

C8CA0C8DCA0C7A48

List all deleted .docx files in the whole partition?

```
(duanhn@duanhn)-[~/lab5]
$ fls -rdF -o 206848 cfreds_2015_data_leakage_pc.dd | grep .docx
r/- * 0:      Users/informant/AppData/Roaming/Microsoft/Templates/LiveContent/15
/Managed/Word Document Building Blocks/1033/TM02835270[[fn=Photo Sidebar (Annual R
eport Red and Black design)]] .docx
r/- * 0:      Users/informant/Desktop/~$signation_Letter_(Iaman_Informant) .docx

(duanhn@duanhn)-[~/lab5]
$
```

```
root@kali:~/lab# fls -rdF -o 206848 cfreds_2015_data_leakage_pc.dd | grep .docx
r/- * 0:      Users/informant/AppData/Roaming/Microsoft/Templates/LiveContent/15/Managed/Word
Document Building Blocks/1033/TM02835270[[fn=Photo Sidebar (Annual Report Red and Black de
sign)]] .docx
r/- * 0:      Users/informant/Desktop/~$signation_Letter_(Iaman_Informant) .docx
root@kali:~/lab#
```

Other useful parameters

- d display deleted entries only
- D directories only
- r recursively display directories
- l long format
- F Display file (all non-directory) entries only
- u Display undeleted entries only

Verify system information

```

(duanhn@duanhn)-[~/lab5/hives]
$ ls -l
total 60416
-rwxr-xr-x 1 duanhn duanhn 262144 Jun  4 14:00 DEFAULT
-rwxr-xr-x 1 duanhn duanhn 262144 Jun  4 14:00 SAM
-rwxr-xr-x 1 duanhn duanhn 262144 Jun  4 14:00 SECURITY
-rwxr-xr-x 1 duanhn duanhn 48496640 Jun  4 14:00 SOFTWARE
-rwxr-xr-x 1 duanhn duanhn 12582912 Jun  4 14:00 SYSTEM
(duanhn@duanhn)-[~/lab5/hives]

```

Verify Users' information

rip

```

(duanhn@duanhn)-[~/lab5/ntuser]
$ ls -l *.DAT
ls: cannot access '*.DAT': No such file or directory
-rwxr-xr-x 1 duanhn duanhn 524288 Jun  5 05:34 NTUSER_admin11.DAT
-rwxr-xr-x 1 duanhn duanhn 262144 Jun  5 05:34 NTUSER_Default.DAT
-rwxr-xr-x 1 duanhn duanhn 1048576 Jun  5 05:34 NTUSER_informant.DAT
-rwxr-xr-x 1 duanhn duanhn 524288 Jun  5 05:34 NTUSER_temporary.DAT
(duanhn@duanhn)-[~/lab5/ntuser]

```

What is the installed OS information in detail?

```

(duanhn@duanhn)-[~/lab5/ntuser]
$ ./rip.pl -r SOFTWARE -p winver
Launching winver v.20200525
winver v.20200525
(Software) Get Windows version & build info

ProductName           Windows 7 Ultimate
CSDVersion             Service Pack 1
BuildLab               7601.win7sp1_gdr.130828-1532
BuildLabEx             7601.18247.amd64fre.win7sp1_gdr.130828-1532
RegisteredOrganization
RegisteredOwner        informant
InstallDate            2015-03-22 14:34:26Z
(duanhn@duanhn)-[~/lab5/ntuser]
$

```

What is the computer name?


```
(duanhn@duanhn)-[~/lab5/ntuser]
$ ./rip.pl -l | grep -i name
- Check key/value names in a hive for leading null char
123. compname v.20090727 [System]
- Gets ComputerName and Hostname values from System hive
- Gets contents of PendingFileRenameOperations value
- Parse hive, check key/value names for RLO character

(duanhn@duanhn)-[~/lab5/ntuser]
$ ./rip.pl -r SYSTEM -p compname
Launching compname v.20090727
compname v.20090727
(System) Gets ComputerName and Hostname values from System hive

ComputerName      = INFORMANT-PC
TCP/IP Hostname   = informant-PC

(duanhn@duanhn)-[~/lab5/ntuser]
```

How many accounts does the system have?

Search for profiles

```
n: (duanhn@duanhn)-[~/lab5/ntuser]
$ ./rip.pl -l | grep -i profile
142. profilelist v.20200518 [Software]
- Get content of ProfileList key
166. profiler v.20200525 [NTUSER.DAT, System]
- Environment profiler information
```

```
(duanhn@duanhn)-[~/lab5/ntuser]
$ ./rip.pl -r SOFTWARE -p profilelist
Launching profilelist v.20200518
profilelist v.20200518
(Software) Get content of ProfileList key

Microsoft\Windows NT\CurrentVersion\ProfileList

Path      : %systemroot%\system32\config\systemprofile
SID       : S-1-5-18
LastWrite : 2009-07-14 04:53:25Z

Path      : C:\Windows\ServiceProfiles\LocalService
SID       : S-1-5-19
LastWrite : 2015-03-25 11:14:18Z

Path      : C:\Windows\ServiceProfiles\NetworkService
SID       : S-1-5-20
LastWrite : 2015-03-25 11:14:18Z

Path      : C:\Users\informant
SID       : S-1-5-21-2425377081-3129163575-2985601102-1000
LastWrite : 2015-03-25 15:30:57Z

Path      : C:\Users\admin11
SID       : S-1-5-21-2425377081-3129163575-2985601102-1001
LastWrite : 2015-03-22 15:57:41Z
```

Find and search for Security Accounts Manager (SAM) information


```
(duanhn@duanhn)-[~/lab5/ntuser]
$ ./rip.pl -r SAM -P samparse | grep -E "Username|Created|Date"
Launching samparse v.20220921
Username      : Administrator [500]
Account Created : Wed Mar 25 10:33:22 2015 Z
Last Login Date : Sun Nov 21 03:47:20 2010 Z
Pwd Reset Date  : Sun Nov 21 03:57:24 2010 Z
Pwd Fail Date   : Never
Username      : Guest [501]
Account Created : Wed Mar 25 10:33:22 2015 Z
Last Login Date : Never
Pwd Reset Date  : Never
Pwd Fail Date   : Never
Username      : informant [1000]
Account Created : Sun Mar 22 14:33:54 2015 Z
Last Login Date : Wed Mar 25 14:45:59 2015 Z
Pwd Reset Date  : Sun Mar 22 14:33:54 2015 Z
Pwd Fail Date   : Wed Mar 25 14:45:43 2015 Z
Username      : admin11 [1001]
Account Created : Sun Mar 22 15:51:54 2015 Z
Last Login Date : Sun Mar 22 15:57:02 2015 Z
Pwd Reset Date  : Sun Mar 22 15:52:10 2015 Z
Pwd Fail Date   : Sun Mar 22 15:53:02 2015 Z
Username      : ITechTeam [1002]
Account Created : Sun Mar 22 15:52:30 2015 Z
Last Login Date : Never
Pwd Reset Date  : Sun Mar 22 15:52:45 2015 Z
```

How many accounts does the system have?

6

When is the login time?

```
Username      : Administrator [500]
SID           : S-1-5-21-2425377081-3129163575-2985601102-500
Full Name     :
User Comment   : Built-in account for administering the computer/domain
Account Type   : Default Admin User
Account Created : Wed Mar 25 10:33:22 2015 Z
Name          :
Last Login Date : Sun Nov 21 03:47:20 2010 Z
Pwd Reset Date  : Sun Nov 21 03:57:24 2010 Z
Pwd Fail Date   : Never
```

```
Username      : Guest [501]
SID           : S-1-5-21-2425377081-3129163575-2985601102-501
Full Name     :
User Comment   : Built-in account for guest access to the computer/domain
Account Type   : Default Guest Acct
Account Created : Wed Mar 25 10:33:22 2015 Z
Name          :
Last Login Date : Never
Pwd Reset Date  : Never
Pwd Fail Date   : Never
```

```
Username      : informant [1000]
SID           : S-1-5-21-2425377081-3129163575-2985601102-1000
Full Name     : 
User Comment  : 
Account Type  : Default Admin User
Account Created : Sun Mar 22 14:33:54 2015 Z
Name         : 
Password Hint : IAMAN
Last Login Date : Wed Mar 25 14:45:59 2015 Z
Pwd Reset Date : Sun Mar 22 14:33:54 2015 Z
Pwd Fail Date  : Wed Mar 25 14:45:43 2015 Z
```

```
Username      : admin11 [1001]
SID           : S-1-5-21-2425377081-3129163575-2985601102-1001
Full Name     : admin11
User Comment  : 
Account Type  : Default Admin User
Account Created : Sun Mar 22 15:51:54 2015 Z
Name         : 
Last Login Date : Sun Mar 22 15:57:02 2015 Z
Pwd Reset Date : Sun Mar 22 15:52:10 2015 Z
Pwd Fail Date  : Sun Mar 22 15:53:02 2015 Z
```

```
Username      : ITechTeam [1002]
SID           : S-1-5-21-2425377081-3129163575-2985601102-1002
Full Name     : ITechTeam
User Comment  : 
Account Type  : Default Admin User
Account Created : Sun Mar 22 15:52:30 2015 Z
Name         : 
Last Login Date : Never
Pwd Reset Date : Sun Mar 22 15:52:45 2015 Z
Pwd Fail Date  : Sun Mar 22 15:53:02 2015 Z
Login Count   : 0
```

```
Username      : temporary [1003]
SID           : S-1-5-21-2425377081-3129163575-2985601102-1003
Full Name     : temporary
User Comment  : 
Account Type  : Custom Limited Acct
Account Created : Sun Mar 22 15:53:01 2015 Z
Name         : 
Last Login Date : Sun Mar 22 15:55:57 2015 Z
Pwd Reset Date : Sun Mar 22 15:53:11 2015 Z
Pwd Fail Date  : Sun Mar 22 15:56:37 2015 Z
Login Count   : 1
```

Who was the last user to logon into PC?

```
(duanhn@duanhn)-[~/lab5/ntuser]
$ ./rip.pl -r SOFTWARE -p lastloggedon
Launching lastloggedon v.20200517
lastloggedon v.20200517
(Software) Gets LastLoggedOn* values from LogonUI key

LastLoggedOn
Microsoft\Windows\CurrentVersion\Authentication\LogonUI
LastWrite: 2015-03-25 13:05:47Z

LastLoggedOnUser      = .\informant
LastLoggedOnSAMUser   = informant-PC\informant

(duanhn@duanhn)-[~/lab5/ntuser]
```

When was the last recorded shutdown date/time?

```
(duanhn@duanhn)-[~/lab5/ntuser]
$ ./rip.pl -r 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: 2015-03-25 15:31:05Z
ShutdownTime   : 2015-03-25 15:31:05Z
```

Explain the information of network interface(s) with an IP address assigned by DHCP.

```
(duanhn@duanhn)-[~/lab5/ntuser]
$ ./rip.pl -r SYSTEM -p nic2
Launching nic2 v.20200525
nic2 v.20200525
(System) Gets NIC info from System hive

Adapter: {846ee342-7039-11de-9d20-806e6f6e6963}
LastWrite Time: 2015-03-25 10:33:18Z

ControlSet001\Services\Tcpip\Parameters\Interfaces has no subkeys.
Adapter: {E2B9AEEC-B1F7-4778-A049-50D7F2DAB2DE}
LastWrite Time: 2015-03-25 15:24:51Z
UseZeroBroadcast          0
EnableDeadGWDetect        1
EnableDHCP                1
NameServer
Domain
RegistrationEnabled        1
RegisterAdapterName        0
DhcpIPAddress             10.11.11.129
DhcpSubnetMask             255.255.255.0
DhcpServer                 10.11.11.254
```

YOU MUST SUBMIT A FULL-SCREEN IMAGE FOR FULL CREDIT!

Save the document with the filename "**YOUR NAME Lab 5.pdf**", replacing "YOUR NAME" with your real name.

Email the image to the instructor as an attachment to an e-mail message. Send it to: **xxx@fe.edu.vn** with a subject line of "**Lab 5 From YOUR NAME**", replacing "YOUR NAME" with your real name.