Introduction to Windows Registry

Introduction

In this practical you will use RegRipper and AcessData FTK Imager to gather critical information from the Windows Registry

By the end of this lab you will be able to

- Use RegRipper and FTK Imager to gather forensic information from suspect's Windows Registry files

Task 1: Introduction to Windows Registry

Use the FTK Imager to locate and extract the following registry files from the Mantooth image (the image is available in the Week 4 section of the FORFUN moodle page), along with their path information:

- SAM
- SECURITY
- SOFTWARE
- SYSTEM

All of the above are located in the Mantooth.E01/Partition 1/MANTOOTH [NTFS]/[root]/Windows/System32/config folder

Use the RegRipper tool to extract the following information from the **SYSTEM** and Software registry files; the RegRipper tool can be downloaded from the following link: https://github.com/keydet89/RegRipper3.0/archive/refs/heads/master.zip

Please ask your lab tutor if you have any difficulties with the RegRipper software.

1. What is the name of the computer?

WESMANTOOTH-PC

2. The time zone name

Mountain Standard Time

3. IDE hard drive name

Maxtor 6E020L0 ATA Device

4. What is the IP address of the computer? When did the computer get it? And what is the IP address of its DHCP server?

IP address is 192.168.1.106 it was obtained on sat jul 14 17:40:19 2007
The IP address of the DHCP server is 192.168.1.1

5. What is the setting for prefetch?

EnablePrefetcher=3

6. Determine the start type of the truecrypt service

Start= system start

7. What is the serial number for the "Canon PowerShot SD500" device; when was it connected to the computer?

Serial number: 6&ac461f8&0&3
Sat Jul 14 17:56:41 2007

8. List 5 portable devices that were connected to the computer, along with their serial numbers.

iPod (S/N: 000A270014B302AB&0), Drive SM_USB20 (S/N: AA14012714842&0), Cruzer Mini (SNDK3066A40516400406&0), Sony DSC (S/N: 6&382957cd&0), TD2SMART G3 (S/N: 23090525338296&0)

9. What is the default web browser?

IEEXPLORE.EXE

10. Which user logged on the system last? When did the log on happen?

.\Wes Mantooth @ Tue Feb 12 19:12:14 2008

11. List down the network cards that were used by the system

Realtek RTL8139/810x Family Fast Ethernet NIC [Tue Feb 27 19:21:27 2007]
Linksys Wireless-G USB Network Adapter [Tue Feb 12 18:14:42 2008]

12. What is the profile name of the wireless network that the system was connected to?

Frankenwave2

13. List 3 removable devices that were connected to the computer, along with last write time, serial number and assigned drive letter if possible

```
Device: DISK&VEN_FLASH&PROD_DRIVE_SM_USB20&REV_1000
LastWrite : Tue Mar  6 15:37:28 2007 (UTC)
SN       : 6&6B8C30&0&AA14012714842&0
Drive     : VistaImage (E:)

Device    : DISK&VEN_SANDISK&PROD_CRUZER_MINI&REV_0.1
LastWrite : Fri Mar  9 01:07:02 2007 (UTC)
SN       : SNDK3066A40516400406&0
Drive     : Vista_Image (F:)

Device    : DISK&VEN_SANDISK&PROD_CRUZER_MINI&REV_0.1
LastWrite : Sat Jul  7 20:33:13 2007 (UTC)
SN       : SNDK4DB2A41B47901706&0
Drive     : MANTOOTH (E:)
```

14. List 5 software that were installed on the system along with the timestamp

WebEx: Wed Oct 10 10:12:40 2007 (UTC)
FileZilla (remove only): Sun Jun 24 00:23:53 2007 (UTC)
Microsoft Office Standard Edition 2003 v.11.0.5614.0: Tue Apr 17 23:25:28 2007 (UTC)
RTC Client API v1.2 v.1.2.0000: Tue Apr 17 21:43:27 2007 (UTC)
AccessData DNA 3 Worker v.3.3:Tue Apr 17 19:58:46 2007 (UTC)

15. List the registered organisation, install date, product ID, product name and registered owner of the Windows Operating System

RegisteredOwner : Wes Mantooth
RegisteredOrganization : Volturi Enterprises
ProductId : 89580-378-0753292-71704
ProductName : Windows Vista (TM) Ultimate
InstallDate : Tue Feb 27 19:22:03 2007 (UTC)

16. List all the user profiles that were created on the system

```
Path     : C:\Users\Wes Mantooth
SID      : S-1-5-21-3166329-3263506726-1320359247-1000
LastWrite : Tue Feb 12 20:13:25 2008 (UTC)
LoadTime  : Thu Jan  1 00:00:00 1970 (UTC)

Path     : C:\Users\Dracula
SID      : S-1-5-21-3166329-3263506726-1320359247-1002
LastWrite : Fri Mar 23 00:31:49 2007 (UTC)
LoadTime  : Thu Jan  1 00:00:00 1970 (UTC)
```

Use the RegRipper tool to extract the following information from the **SAM** registry file;

17. Note down the following information for each user reported within the SAM file: username, account type, account created, password hint, last login date, password reset date, password fail date, and login count.

```
Username       : Administrator [500]
Account Type    : Default Admin User
Account Created : Tue Feb 27 18:29:26 2007 Z
Last Login Date : Thu Nov  2 13:02:01 2006 Z
Pwd Reset Date  : Thu Nov  2 13:08:15 2006 Z
Pwd Fail Date   : Never
Login Count     : 1

Username       : Guest [501]
Account Type    : Default Guest Acct
Last Login Date : Never
Pwd Reset Date  : Never
Pwd Fail Date   : Never
Login Count     : 0

Username       : Wes Mantooth [1000]
Account Type    : Default Admin User
Account Created : Tue Feb 27 18:29:10 2007 Z
Password Hint   : in your face
Last Login Date : Tue Feb 12 19:12:08 2008 Z
Pwd Reset Date  : Tue Feb 27 18:29:13 2007 Z
Pwd Fail Date   : Tue Feb 12 20:13:16 2008 Z
Login Count     : 96

Username       : Dracula [1002]
Full Name      : Count Dracula
Account Type    : Custom Limited Acct
Account Created : Tue Mar  6 01:25:43 2007 Z
Last Login Date : Mon Apr  2 00:30:58 2007 Z
Pwd Reset Date  : Mon Apr  2 00:30:39 2007 Z
Pwd Fail Date   : Tue Feb 12 20:13:17 2008 Z
Login Count     : 3

Username       : Laurent [1003]
Full Name      : Laurent
```

Account Type : Custom Limited Acct
Account Created : Tue Feb 12 00:13:36 2008 Z
Last Login Date : Never
Pwd Reset Date : Never
Pwd Fail Date : Never
Login Count : 0

18. Based upon the answer from the previous question, which user will you investigate further and why?

Wes Mantooth as the user is the most active user, an admin user, and also the user who used the system last.

Use the FTK Imager to locate and extract the following registry files from the Mantooth image, along with their path information:

- Wes Mantooth's NTUSER.dat
- Dracula's NTUSER.dat

Wes Mantooth's NTUSER.dat is *located in the Mantooth.E01/Partition 1 /MANTOOTH [NTFS]/[root]/Users/Wes Mantooth folder*

Dracula's NTUSER.dat is *located in the Mantooth.E01/Partition 1 /MANTOOTH [NTFS]/[root]/Users/Dracula folder*

Use the RegRipper tool to extract the following information from the **Wes Mantooth's NTUSER.dat**

registry file;

19. What are the most recent PDFs opened by Mantooth?

C/Users/Wes Mantooth/Desktop/order851797-2007-04-12-13-17-02 (1).pdf
/C/Users/Wes Mantooth/AppData/Local/Microsoft/Windows/Temporary Internet Files/Content.IE5/E8L9BFMS/order851797-2007-04-12-13-17-02.pdf

20. Name three recent files being opened via Paint

File1 -> C:\Users\Wes Mantooth\Documents\Scripts\nationaltall.bmp
File2 -> C:\Users\Wes Mantooth\Documents\Scripts\prescription.gif
File3 -> C:\Users\Wes Mantooth\Documents\Scripts\nationaltal.gif

21. List 5 MRU applications by Mantooth

NOTEPAD.EXE
SnagIt32.exe
FTK Imager.exe
aim6.exe
WinMail.exe
Sat Jul 14 17:56:41 2007

22. Find the file path for file ATM_THEFTS1.ppt

E:\Business Ideas\ATM_THEFTS1.ppt

23. Based upon the answer from the previous question, what would you do as an investigator?

Search for the E drive which is highly likely an external drive

24. Find the start page of the Internet Explorer

http://www.google.com

25. What is the Download Directory for the Internet Explorer?

C:\Users\Wes Mantooth\Desktop\Latest True Crypt

26. List 5 links that are stored in the IE favorites

Microsoft Websites
MSN Websites
Wes's Favs
Windows Live
Yahoo!
My Yahoo!.url
Yahoo!.url

27. List the files that were opened by Media Player from F drive

F:\Sounds and Video\pf3.wav
F:\Sounds and Video\wizoz18d.wav

28. Based upon the answer from the previous question, what would you do as an investigator?

Search for the F drive which is highly likely an external drive

29. Name the two recent used PowerPoint files, along with their file path

File1 -> E:\Business Ideas\ATM_THEFTS1.ppt
File2 -> C:\Users\Wes Mantooth\Desktop\ATM_THEFTS1.ppt

30. Find 5 items from Recent used documents that you would like to investigate further, along with your justifications

Johns Stuff (\\TRAINING-KEN): this is a network share.
Bitlocker Command.txt.txt: this is related to encryption
C money plates.doc: sounds interesting
Super Secret Stuff.zip: again sounds interesting
russ_4_ящеркой.doc: a document created in Russian?

31. List 5 programs that were opened via the Windows RUN application

cmd
mspaint
notepad
regedt32
calc
www.google.com

32. List 5 URLs that were typed into the Internet Explorer

url1 -> http://www.tucows.com/
url2 -> http://www.tigerdirect.com/
url3 -> http://www.newegg.com/
url4 -> http://www.altavista.com/
url5 -> http://www.mamma.com/
url6 -> http://www.google.com/
url7 -> http://www.goole.com/
url8 -> http://www.youtube.com/

33. List the email addresses that could be used by Mantooth

mantooth2007@aol.com
dollarhyde86@comcast.net
molarman420@hotmail.com

34. Find the password for the WinVNC program

c2706283b4a6cb8e

35. Find Mantooth's Yahoo Messenger's user name

Incisorman420

36. Find details of Mantooth's default printers

Epson Stylus Photo RX420 (M),winspool,LPT1: