Introduction to Windows Registry

Introduction

In this practical you will use RegRipper and AccessData 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 3 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?

2. The time zone name

3. IDE hard drive name

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?

5. What is the setting for prefetch?

6. Determine the start type of the truecrypt service

7. When was the last shutdown time of the computer?

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

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

10. What is the default web browser?

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

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

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

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

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

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

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.

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

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?

20. Name three recent files being opened via Paint

21. List 5 MRU applications by Mantooth

22. Find the file path for file ATM_THEFTS1.ppt

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

24. Find the start page of the Internet Explorer

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

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

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

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

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

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

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

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

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

34. Find the password for the WinVNC program

35. Find Mantooth's Yahoo Messenger's username

36. Find details of Mantooth's default printers