IFS4102 (Digital Forensics) Assignment 2: Windows Forensics

Due Date: Saturday, 22 April 2023, 23:59 SGT

Introduction

In this assignment, you will again play the role of a Digital Forensic Investigator. Your ***second mission*** is to investigate a **Windows machine** seized from a suspect by analyzing its acquired **registry files**. As you are all well aware, Windows remains the most widely-used desktop OS, and its registry is a very useful source of evidence data. You may thus encounter the same forensics scenario in practice in the future. To solve the questions, you will need to use tools that have been covered in your labs, such as RegEdit and RegRipper.

Instructions and Deadline

This is an **individual** assignment. You MUST finish the assignment and report **independently**. Note that your report may be checked by the available anti-plagiarism service.

Please prepare your report in a self-contained **PDF file** by using your name and matric number as part of your file name. For example, Jack Lee with Matric No A001 should submit the filename JackLee-A001-A2.pdf. Your report should also contain your name, matric number, and email address on its first page.

Do upload your PDF file to Canvas' `Assignment-2` by **Saturday, 22 April 2023, 23:59 SGT**. There will be **no deadline extensions**, and there will be following **penalties for late submissions**:

- Late up to 5 hours: 10% penalty to your obtained marks.
- Later than 5 hours but no later than 1 day: Maximum possible marks are capped at 80%.
- Later than 1 day (*subject to approval only*): Maximum possible marks are capped at 60%.

Grading Scheme

By correctly answering all the questions asked in this assignment, you will get the possible **30 marks**. This assignment is worth **15%** of your final score.

As explained more below, in answering all the questions below, you will need to provide ***both*** **the relevant *full-path registry values* and their respective stored *data items***.

Good luck, and have fun with your second mission!

Forensics Scenario and Tasks

- You are given **a set of registry files** from the target Windows machine. Its zipped file, named `A2-registries.zip`, can be found in the `Assignments / Assignment-2` folder of Canvas' Files. The zip file's MD5 hash value is `c93674895d2a27f2aa667333460b5b89`. Please ensure the integrity of your downloaded file before you start analyzing it, such as by using `certutil`. Upon extracting the zip file, you should find the `SYSTEM` and `SOFTWARE` registry files of the machine, as well as 2 `NTUSER.DAT` files belonging to its 2 users.

- Your **task** is to analyze the state of the target machine by inspecting the given registry files, and then answering all the questions listed below. As briefly mentioned above, in answering each question below, you need to mention **both** the ***registry value*** holding the required piece of information (in **full "pathname"** format from its main registry key), **and** its respective stored ***data item***. For instance, in answering the question "What is the machine's Windows OS product ID?", you thus need to report the registry value `SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProductId`, together with its data `00260-60000-00000-AA378`.

  Given the assignment requirement, you are thus allowed to use an *automated* registry analysis tool in order to find out the required data items. Yet, you need to also mention the relevant registry values from which the data items are extracted, and therefore may need to *manually* verify them as well.

- **General hint:** To help you locate the relevant registry (sub-) keys and values, you can refer to some handy *Windows registry quick-find chart* cheat sheets, which were previously already uploaded into Canvas.

Challenge 1: Analyzing the SYSTEM Registry File of the Target Machine

Answer the following questions based on your analysis (**10 marks** in total, with **1 mark** carried by each question):

1. What are the current and default values of the *CurrentControlSet*?
2. What is the computer's name?
3. What are the processors' architecture *and* identifier/model? Also tell its number of processors.
4. What is the computer's Time Zone, which was entered during its installation?
5. When was the system's last shutdown time, both in hexadecimal format (as stored in the registry) and its corresponding human-readable time format (in UTC)?
6. Where is the computer's Windows system directory located?
7. Where is the computer's security event log is stored?
8. Where is the computer's system event log is stored?
9. What is the friendly name of previously-connected thumbdrive(s) from SanDisk (as its/their vendor)?
10. What were the computer's DHCP-based IP address and its network mask under the allocated `.local` DHCP domain?

Challenge 2: Analyzing the SOFTWARE Registry File of the Machine

Answer the following questions based on your analysis (**10 marks** in total, with **1 mark** carried by each question):

1. What is the product name of the installed Windows operating system?
2. Who is its registered owner? What is its registered organization?
3. When is its installation date, both in hexadecimal format (as stored in the registry) and its corresponding human-readable time format (in UTC)?
4. Who is the last logged-on user on the machine together with his/her User SID?
5. Based on the maintained profile list on the system, who are other users besides the recorded last logged-on user?
6. Who is the default user for logon information? What is the default domain name?
7. What are the web browsers installed on the computer according to the entries in the system's Start menu?
8. Where is the CCleaner program installed at? Give the full pathname of the executable (including the executable name).
9. What are the pathnames of programs that automatically get launched at machine boot time (startup)?
10. What are the machine's network cards?

Challenge 3: Analyzing the NTUSER.DAT Files of the Machine

Answer the following questions based on your analysis (**10 marks** in total):

[Important!] Please use the given `IEUser-NTUSER.DAT` file in answering **Questions 1–3**, and the `CFTT-NTUSER.DAT` file in answering **Questions 4–8**.

1. (1 mark) What were the URLs typed by the user on Internet Explorer?
2. (1 mark) What are the executables most recently executed using the Start $>$ Run command?
3. (1 mark) What are the installed Process Monitor's locations of log file and `dbghelp.dll`?

   [Please remember to use the `CFTT-NTUSER.DAT` *file for the remaining questions below!]*

4. (1 mark) What are an installed file archiver (zip utility) tool name and its recorded path?
5. (1 mark) What are the version no and executable pathname of the installed OneDrive?
6. (1 mark) What is Netscape Navigator's viewer for Word files of the user?
7. (1 mark) What is a Netscape Navigator's trusted external application for the user?

8. (2 marks) What are the user's most recently used/accessed Microsoft Word (.docx) files, and when were they opened respectively (in UTC)?

9. (1 mark) What is the user's *latest accessed* Microsoft Excel (.xlsx) file, and when was it opened (in UTC)?

Appendix: Note on RegRipper Seemingly Hanging when Importing SOFTWARE Registry File

This section provides some information regarding a potential issue with RegRipper when it is used to analyze the `SOFTWARE` registry file.

When using RegRipper to analyze the `SOFTWARE` registry file, RegRipper may seemingly hang after running the `btconfig` plugin. This is actually because the subsequent plugin, `clsid`, produces a lot of output that may take a long time to complete. As such, you may choose to disable the `clsid` plugin if it is taking too long.

To disable the `clsid` plugin, do perform the following steps:

1. Close RegRipper if you have it opened.
2. Open the file `plugins/software` in Notepad.
3. Comment out the line with `clsid`, so that it looks like the following:

```
...
bitbucket
btconfig
# clsid
cmd_shell
cmd_shell_tln
...
```

4. Save the file, and then close it.
5. Now you can import the `SOFTWARE` registry file as per normal.

— End of Assignment —