Intro to Memory Forensics

TABLE OF CONTENTS

Directory Structure

1. PerfLogs

It is the folder created to keep Windows performance logs. It is found as an empty folder because the logging option is turned off by default.

2. ProgramData

The ProgramData folder is located as a hidden folder under the root of the disk where the Windows operating system is installed. The "Hidden Items" option must be activated under the "View" menu first to be able to see the folder. There are data belonging to the programs installed in the system, independent from the user accounts in this folder.

3. Program Files

All the programs installed in the system are located under the "Program Files" folder in a Windows operating system installed as 32-bit. In Windows operating systems installed as 64-bit, only 64-bit programs are installed under this folder.

Directory Structure

4. Program Files (x86)
This folder is only available on Windows operating systems installed as "64-bit". There are programs installed on the system as "32-bit" under this folder. Programs installed as "64-bit" are stored in another folder named “Program Files” with a similar name.

5. Users
The Users folder contains the personal folder of each user who has logged on to the system at least once. Folders and documents such as desktop folder, downloaded files, and documents are stored under this folder that belongs to each user on the system.

6. Windows
The Windows folder is where the entire operating system is installed. It has its own structure and it contains many systemic information in a certain order. For example, the database where users' passwords are kept is located under this folder.

Windows Process Management

A process is a program under execution in an active program. Processes are the units of commands/programs running on the operating system. Mainly the processes are examined during the live Windows host review. Examination and analysis of memory essentially actually mean the analysis of processes. Each process has its own identification number in the Windows environment which is called "Process ID" (PID) and they are logged in each process operation.

Windows Process Management

Process Tree

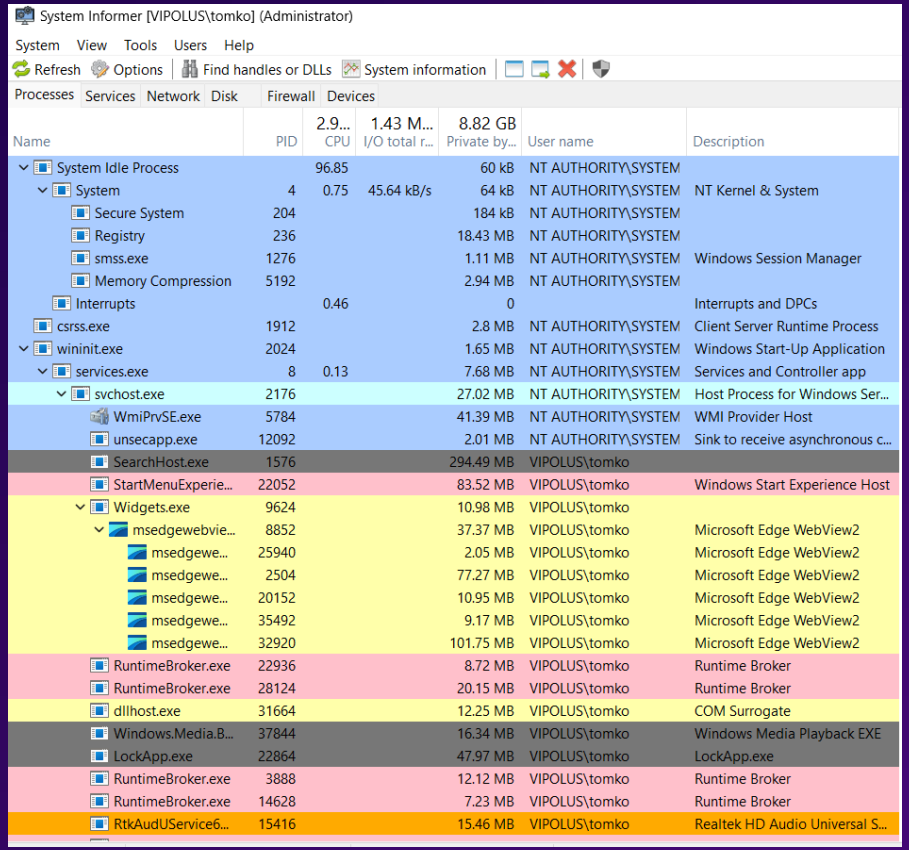
Running a program is a process. From this process, another process can be created. There is a parent-child relationship between the two processes.

Process: A process is a program under execution in an active program.

Parent Process: In computing, a parent process is a process that has created one or more child processes.

Child Process: A child process in computing is a process created by another process (the parent process). A parent process may have multiple child processes, but a child process only one parent process.

Windows Process Management



Windows Process Management

wininit.exe

The “wininit.exe” process is known as the “Windows Initilization Process”. It is responsible for starting the Service Control Manager (services.exe), Local Security Authority process (lsass.exe), and Local Session Manager (lsm.exe). It is located under the “C:\Windows\System32” folder. It is created during system boot. It is the process that works with the privileges of the most authorized user (NT AUTHORITY\SYSTEM) on the system.

services.exe

The “services.exe” is the process responsible for starting and stopping services. “Svchost.exe”, “dllhost.exe”, “taskhost.exe”, and “spoolsv.exe” are child processes of the “Services.exe” process. It is located under the “C:\Windows\System32” folder. It is the process that works with the privileges of the most authorized user (NT AUTHORITY\SYSTEM) on the system. There should only be 1 "services.exe" process at a time in the process tree under normal conditions. If there are multiple "services.exe" processes or if there is a process with a similar name, it should be investigated further as it may be a process that belongs to a malicious activity.

Windows Process Management

svchost.exe

“Svchost.exe” is a generic host process name for services that run from dynamic-link libraries. Because DLL files are non-executable files, they are run with svchost for triggering the services of the operating system. “svchost.exe” is responsible for the usage and management of multi-dll services for the optimization of system sources. All DLL-based services share the same svchost process. Every svchost process occurs with executing unique services. It's parent process is “services.exe”. And "Services.exe" is the child process of "wininit.exe".

Windows Process Management

lsass.exe

The “lsass.exe” (Local Security Authority Subsystem Service) is the process responsible for critical security operations such as confirming or rejecting users' passwords during login in the Windows operating system. In addition, this process works actively during the password changes of users. This process is critically important as it contains the user passwords in the system. The attacker gaining access to the system can obtain the user's password by leveraging this process. There is a free tool called “mimikatz” developed by “Benjamin Delpy” and users' passwords can be obtained from the "lsass.exe" process with the help of the “Mimikatz” tool. It can be accessed at the following address:

Mimikatz: https://blog.gentilkiwi.com/mimikatz “lsass.exe” is located under the “C:\Windows\System32” folder. It is the process that works with the privileges of the most authorized user (NT AUTHORITY\SYSTEM) on the system.

Windows Process Management

winlogon.exe

The “Winlogon.exe” is the process that performs the login and logout operations of the users in the Windows operating system. It is the process that works with the privileges of the most authorized user (NT AUTHORITY\SYSTEM) on the system. “Winlogon.exe” is located under the “C:\Windows\System32” folder.

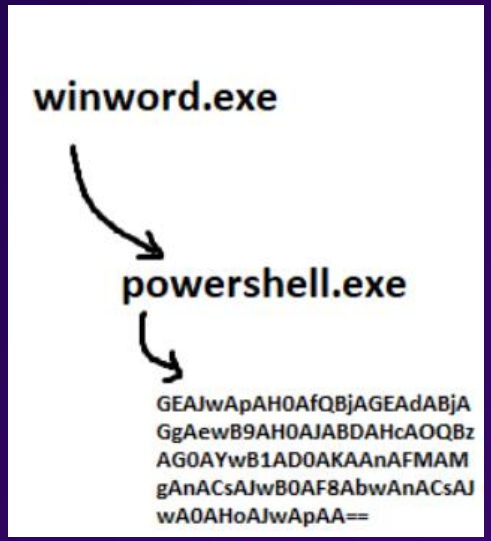
explorer.exe

The “Explorer.exe” process is the parent process of almost every process that has a graphical user interface (GUI) in the Windows operating system and opens as a window. For example, this process kicks in when Windows explorer is started. Under normal circumstances, one "explorer.exe" process is expected. “Explorer.exe” is located under the “C:\Windows\” folder. This process runs with the privileges of the user who is currently logged in to the system.

Windows Process Management

Winword.exe

Winword.exe is the executable file name for Microsoft Word which is used when Word is launched.



Event Logs

Event Logs are logs collected through the Windows operating system. There are various types of logs in these logs. Application logs, security logs and system logs can be given as examples. Event logs are a very important resource to understand whether many processes on the system have taken place and to have a grasp of the details. SOC analysts often make use of event logs when detecting the presence and activity of threats on the system. For example, some event logs are as follows:

Powershell activities
Deleting event logs
Starting and stopping services
Creating a new scheduled task
RDP activity
Changing user privileges
Failed login activities

Event Logs

Application
It provides log records related to the applications in the system. For example, you can find errors received by an antivirus application running on the system.

System
It is the area where the logs created by the basic components of the operating system are located. For example, logs for a driver loads and unloads operations can be found here.

Security
Records regarding authentication and security are kept here.

Extra:
ConsoleHost_history.txt

Path:
C:\Users\<User>\AppData\Roaming\Microsoft\Windows\PowerShell\PSReadLine\ConsoleHost_history.txt

Volatility Framework

```
git clone https://github.com/volatilityfoundation/volatility3.git
cd volatility3
python3 setup.py install
python3 vol.py —h
```

Volatility Framework

Common Usage:
Python3 vol.py –f <imagepath> <plugin>

Plugin Example:

windows.cmdline.CmdLine -> Lists process command line arguments.
windows.dumpfiles.DumpFiles -> Dumps cached file contents from Windows memory samples.
windows.filescan.FileScan-> Scans for file objects present in a particular windows memory image.
windows.netscan.NetScan-> Scans for network objects present in a particular windows memory image.
windows.pslist.PsList-> Lists the processes present in a particular windows memory image.
windows.pstree.PsTree-> Plugin for listing processes in a tree based on their parent process ID.

Useful material:

letsdefend.io
cyberdefenders.org
hackthebox.com/sherlocks

Volatility Challenges:
https://github.com/stuxnet999/MemLabs

Thank you for your attention!