Extract the information present in RAM with the help of volatility Framework.

Introduction:

Objective of the project

This project aims to use the Volatility framework to analyze the RAM runtime state of a device and retrieve data from it. The project aims to show the use of memory forensics to retrieve critical information from a computer's volatile memory, including processes, open files, network connections, and more.

Description of the project

Memory forensics is a way for getting and reviewing data from the vulnerable memory of a computer. An open-source tool for memory forensics research is the Volatility framework. It offers a collection of plugins that enable forensic detectives to glean details from a memory dump about the operating system and active processes.

The following measures will be taken in the project

Apply an appropriate memory acquisition tool to the target device to obtain a memory dump from it. Analyze the memory dump and retrieve the necessary data using the Volatility framework. Examine the information that was extracted to find any possible security risks or criminal activity.

Scope of project

The project's goal is to use the Volatility framework to show the use of memory forensics. The task involves gathering knowledge about the system's execution state from a memory dump from a target device. The information gathered from the memory dump will be reviewed to find any possible security threats or malicious actions.

The project does not entail hacking into any computer systems or investigating live systems. The project will be restricted to looking at a device's memory dump that has been given for forensic analysis only. The Volatility framework or any of its plugins won't be modified or reverse-engineered as part of this effort.

Analysis Report:

System snapshots

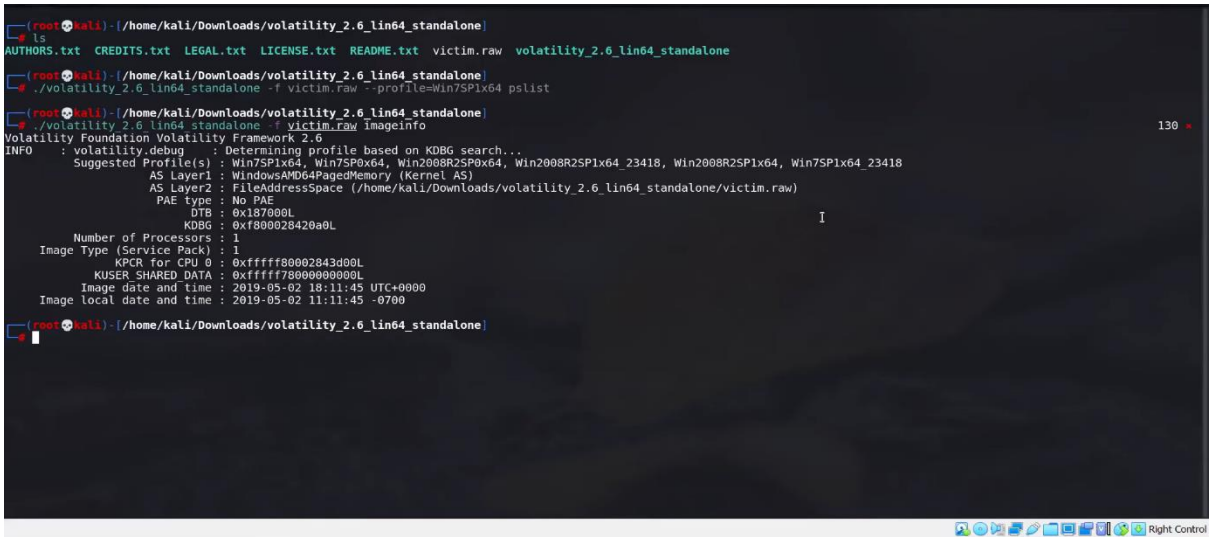

Figure 1

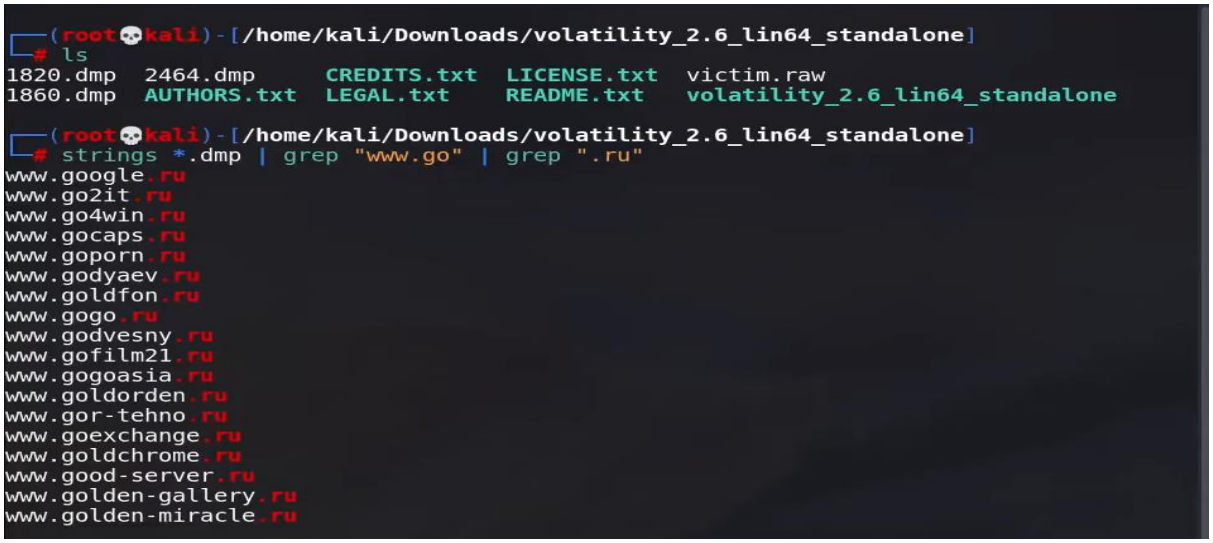

Figure 2

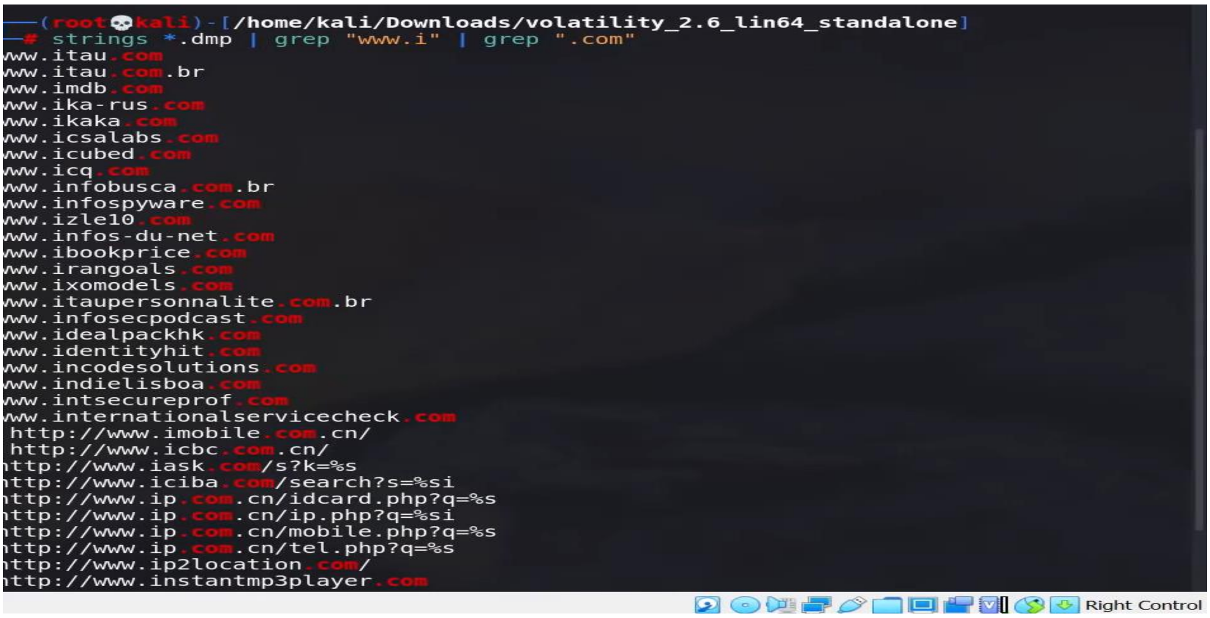

Figure 3

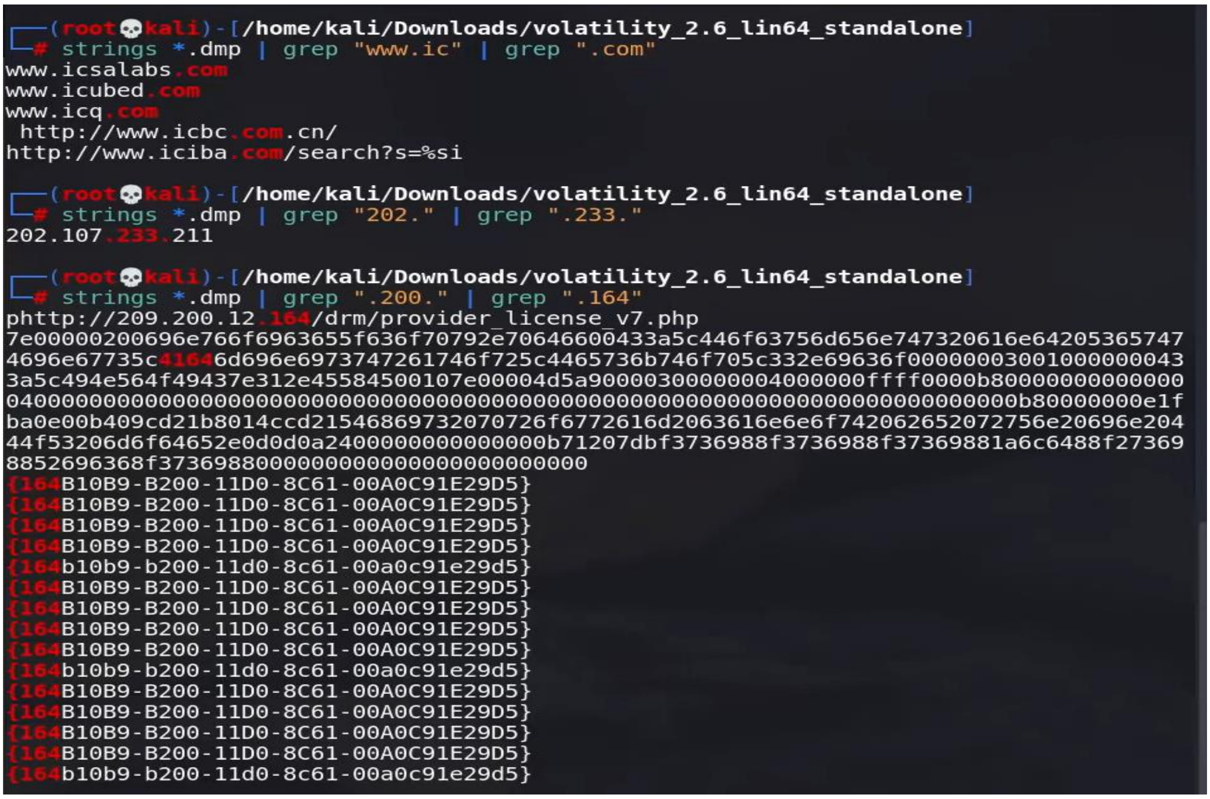

Figure 4

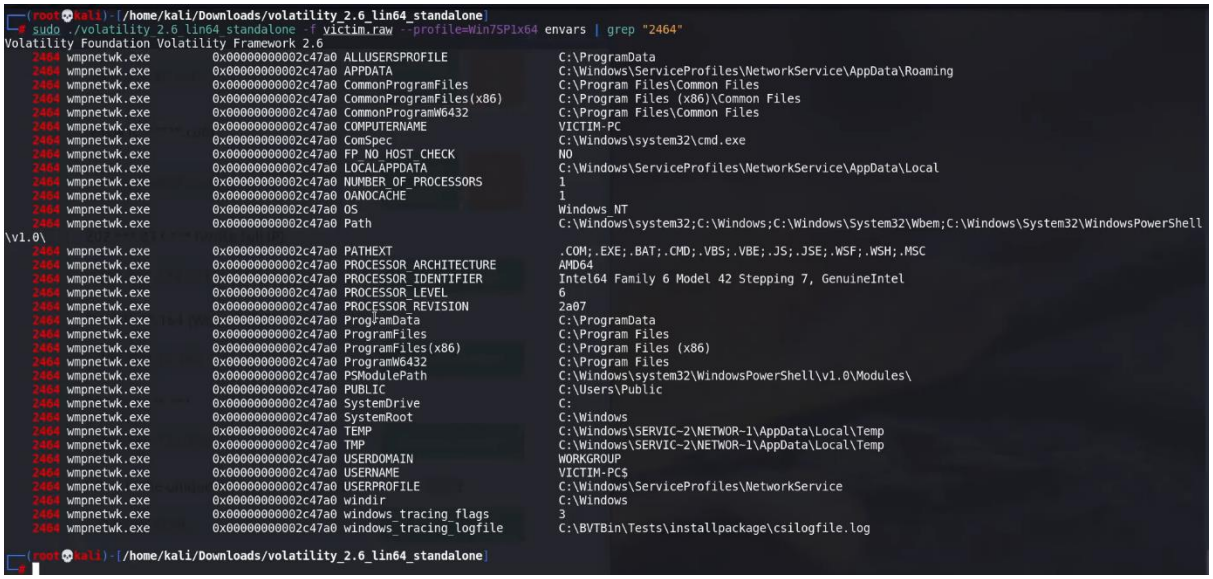
┌──(root💀kali)-[/home/kali/Downloads/volatility_2.6_lin64_standalone]
└─# sudo ./volatility_2.6_lin64_standalone -f victim.raw --profile=Win7SP1x64 envars | grep "2464"
Volatility Foundation Volatility Framework 2.6
2464 wmpnetwk.exe 0x00000000002c47a0 ALLUSERSPROFILE C:\ProgramData
2464 wmpnetwk.exe 0x00000000002c47a0 APPDATA C:\Windows\ServiceProfiles\NetworkService\AppData\Roaming
2464 wmpnetwk.exe 0x00000000002c47a0 CommonProgramFiles C:\Program Files\Common Files
2464 wmpnetwk.exe 0x00000000002c47a0 CommonProgramFiles(x86) C:\Program Files (x86)\Common Files
2464 wmpnetwk.exe 0x00000000002c47a0 CommonProgramW6432 C:\Program Files\Common Files
2464 wmpnetwk.exe 0x00000000002c47a0 COMPUTERNAME VICTIM-PC
2464 wmpnetwk.exe 0x00000000002c47a0 ComSpec C:\Windows\system32\cmd.exe
2464 wmpnetwk.exe 0x00000000002c47a0 FP_NO_HOST_CHECK NO
2464 wmpnetwk.exe 0x00000000002c47a0 LOCALAPPDATA C:\Windows\ServiceProfiles\NetworkService\AppData\Local
2464 wmpnetwk.exe 0x00000000002c47a0 NUMBER_OF_PROCESSORS 1
2464 wmpnetwk.exe 0x00000000002c47a0 OANOCACHE 1
2464 wmpnetwk.exe 0x00000000002c47a0 OS Windows_NT
2464 wmpnetwk.exe 0x00000000002c47a0 Path C:\Windows\system32;C:\Windows;C:\Windows\System32\Wbem;C:\Windows\System32\WindowsPowerShell
\v1.0\
2464 wmpnetwk.exe 0x00000000002c47a0 PATHEXT .COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC
2464 wmpnetwk.exe 0x00000000002c47a0 PROCESSOR_ARCHITECTURE AMD64
2464 wmpnetwk.exe 0x00000000002c47a0 PROCESSOR_IDENTIFIER Intel64 Family 6 Model 42 Stepping 7, GenuineIntel
2464 wmpnetwk.exe 0x00000000002c47a0 PROCESSOR_LEVEL 6
2464 wmpnetwk.exe 0x00000000002c47a0 PROCESSOR_REVISION 2a07
2464 wmpnetwk.exe 0x00000000002c47a0 ProgramData C:\ProgramData
2464 wmpnetwk.exe 0x00000000002c47a0 ProgramFiles C:\Program Files
2464 wmpnetwk.exe 0x00000000002c47a0 ProgramFiles(x86) C:\Program Files (x86)
2464 wmpnetwk.exe 0x00000000002c47a0 ProgramW6432 C:\Program Files
2464 wmpnetwk.exe 0x00000000002c47a0 PSModulePath C:\Windows\system32\WindowsPowerShell\v1.0\Modules\
2464 wmpnetwk.exe 0x00000000002c47a0 PUBLIC C:\Users\Public
2464 wmpnetwk.exe 0x00000000002c47a0 SystemDrive C:
2464 wmpnetwk.exe 0x00000000002c47a0 SystemRoot C:\Windows
2464 wmpnetwk.exe 0x00000000002c47a0 TEMP C:\Windows\SERVIC~2\NETWOR~1\AppData\Local\Temp
2464 wmpnetwk.exe 0x00000000002c47a0 TMP C:\Windows\SERVIC~2\NETWOR~1\AppData\Local\Temp
2464 wmpnetwk.exe 0x00000000002c47a0 USERDOMAIN WORKGROUP
2464 wmpnetwk.exe 0x00000000002c47a0 USERNAME VICTIM-PC$
2464 wmpnetwk.exe 0x00000000002c47a0 USERPROFILE C:\Windows\ServiceProfiles\NetworkService
2464 wmpnetwk.exe 0x00000000002c47a0 windir C:\Windows
2464 wmpnetwk.exe 0x00000000002c47a0 windows_tracing_flags 3
2464 wmpnetwk.exe 0x00000000002c47a0 windows_tracing_logfile C:\BVTBin\Tests\installpackage\csilogfile.log
┌──(root💀kali)-[/home/kali/Downloads/volatility_2.6_lin64_standalone]
└─#

Figure 5