

## **Intro to Cyber Forensics Lab Grading Sheet**

**Project: Lab #7 – Memory Forensics**

**Member Name: VINUSHA GOUD POTTOLLA**

**Member Name: OLUWATOYOSI KEHINDE**

**Member Name: BOINAPELLY AKSHITH RAO**

**Member Name: AMANI PONMAN**

**Member Name: YADLAPALLI IAKSHMIDAR**

### **Executive Summary / 4 points**

+ ✓ -

- ☐ ☐ ☐ Executive summary is brief and focused to the point of the project
- ☐ ☐ ☐ The summary clearly illustrates the objectives of the laboratory exercise

### **Apparatus / 4 points**

- ☐ ☐ ☐ The apparatus are clearly illustrated and documented

### **Procedures / 12 points**

- ☐ ☐ ☐ Adequate information provided to allow re-creation of work
- ☐ ☐ ☐ Consistent level of coverage throughout the project – nothing overly detailed or omitted

### **Problem Solving / 5 points**

- ☐ ☐ ☐ All problems identified
- ☐ ☐ ☐ Alternative solutions identified
- ☐ ☐ ☐ Solutions attempted listed
- ☐ ☐ ☐ Final solution detailed (what fixed the problem and why?)

### **Conclusions & Recommendations / 5 points**

- ☐ ☐ ☐ Tie back to the learning objectives identified in the executive summary - critical
- ☐ ☐ ☐ Conclusions stated in a logical fashion
- ☐ ☐ ☐ Conclusions are viable based on the procedures and results
- ☐ ☐ ☐ Recommendations practical & relevant

### **Format & Grammar / 5 points**

- ☐ ☐ ☐ Table of Contents present
- ☐ ☐ ☐ Report written in past tense
- ☐ ☐ ☐ Proper voice (no I's, We's, Our's or The group)
- ☐ ☐ ☐ Paper easy to read (fonts, spacing, etc.)
- ☐ ☐ ☐ Proper credit given to sources in bibliography (APA style)
- ☐ ☐ ☐ Paper is cohesive and consistent in tone

**Spelling & grammar errors: minus one half point for each, up to a max deduction of 5 points – at that**

**time, paper is returned for correction and re-submission with a one letter grade penalty.**

**Final Score \_\_\_\_\_ / 35**

## **Contents**

<b>1</b>	<b>Executive Summary</b>	<b>3</b>
<b>2</b>	<b>Apparatus</b>	<b>4</b>
<b>3</b>	<b>Procedures</b>	<b>5</b>
	<b>3.1 Time log</b>	
	<b>3.2 Procedure</b>	<b>5</b>
	<b>3.3 Figures</b>	<b>6</b>
<b>4</b>	<b>Problem Solving and Troubleshooting</b>	<b>27</b>
<b>5</b>	<b>Conclusion and Recommendations</b>	<b>32</b>
<b>6</b>	<b>References</b>	<b>13</b>

## **1.Executive summary**

The exercise's main goal was to familiarize participants with the procedures involved in acquiring volatile memory and analysing it using forensic techniques and tools. Being vigilant and adhering to all rules and procedures was necessary to ensure that the data was safe, undamaged, and intact both throughout acquisition and processing. Group 1 carried out this experiment on December 6, 2024, with a focus on collaboration and rigorous adherence to forensic criteria.

During the memory acquisition phase, DumpIt a dependable tool for volatile memory capture with minimal interference—was used. For integrity preservation, the obtained memory dump was safely moved to a forensic workstation. The major tool for analysing the contents of the memory dump file was the Volatility 3 software, which supported Python 3.13.10.

Setting up the proper operating system profile, looking at running and stopped processes, researching parent-child relationships, and spotting malicious or hidden activity were the main phases. Every one of these procedures offered a thorough analysis of the memory condition at the time of collection, which gave forensic investigators useful information.

Throughout the exercise, controlled procedures were used to guarantee that the data was safe and undisturbed. The entire exercise clearly emphasizes that a systematic and organized approach to memory forensics would produce reliable and repeatable results.

## 2. Apparatus

ITEM/PART	MODEL NUMBER	VERSION	USAGE
Memory Acquisition Tool	DumpIt	Latest	To acquire memory from the system.
Analysis Tool	Volatility	3	Forensic analysis of the acquired memory.
Python Interpreter	N/A	3.13.10	Dependency for running Volatility.

Table 1: The Hardware and Software used for the lab exercise.

### 3. Procedures

#### 3.1. Time-Log

#	DATE	Time(24htr)	ACTION TAKEN / INVESTIGATION LEAD
1	December 02,2024	19:20	Opened the existing Windows Virtual Machine
2	December 02,2024	19:26	Downloaded Dumplit.exe and took the memory dump
3	December 02,2024	19:40	Analyzed evilprofessor.vmem using volatility
4	December 02,2024	19:58	Results were summarized

Table 2: Time log of the actions taken during investigation

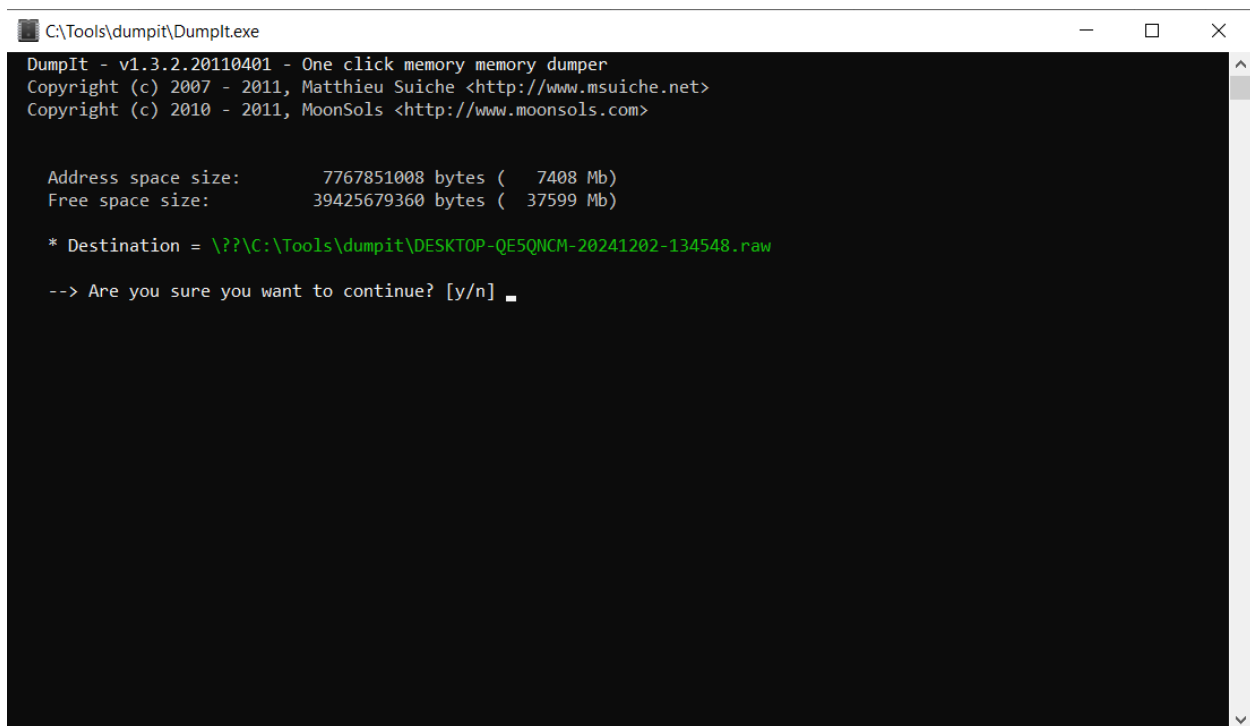
### 3.2. Procedure

The Group 1 team completed two lab components on December 6, 2024, including memory acquisition and processing. To dump volatile memory, the first section (Memory Acquisition Lab) runs DumpIt.exe with administrator rights. The raw file dump was safely moved to a forensic workstation for analysis after the memory dump file was successfully created.

Volatility 3, which requires Python 3.13.10, was used to examine the memory dump file (evil professor.vmem) on the forensic workstation for the second section, the Memory Analysis Lab. The windows.info. Info plugin was used to identify the proper OS profile before the study began. This was followed using a variety of plugins to investigate live processes, parent-child relationships, and potential malicious or concealed behaviour.

### 3.3 Figures

#### Memory Acquisition Lab



```
C:\Tools\dumpit\DumpIt.exe
DumpIt - v1.3.2.20110401 - One click memory memory dumper
Copyright (c) 2007 - 2011, Matthieu Suiche <http://www.msuiche.net>
Copyright (c) 2010 - 2011, MoonSols <http://www.moonsols.com>

Address space size:      7767851008 bytes ( 7408 Mb)
Free space size:        39425679360 bytes ( 37599 Mb)

* Destination = \\?\C:\Tools\dumpit\DESKTOP-QE5QNCM-20241202-134548.raw

--> Are you sure you want to continue? [y/n] _
```

*Fig 1: Asking for permissions to get the memory*

```
C:\Tools\dumpit\DumpIt.exe
DumpIt - v1.3.2.20110401 - One click memory memory dumper
Copyright (c) 2007 - 2011, Matthieu Suiche <http://www.msuiche.net>
Copyright (c) 2010 - 2011, MoonSols <http://www.moonsols.com>

Address space size:      7767851008 bytes ( 7408 Mb)
Free space size:        39425679360 bytes ( 37599 Mb)

* Destination = \??\C:\Tools\dumpit\DESKTOP-QE5QNCM-20241202-134548.raw

--> Are you sure you want to continue? [y/n] y
+ Processing... Success.
```

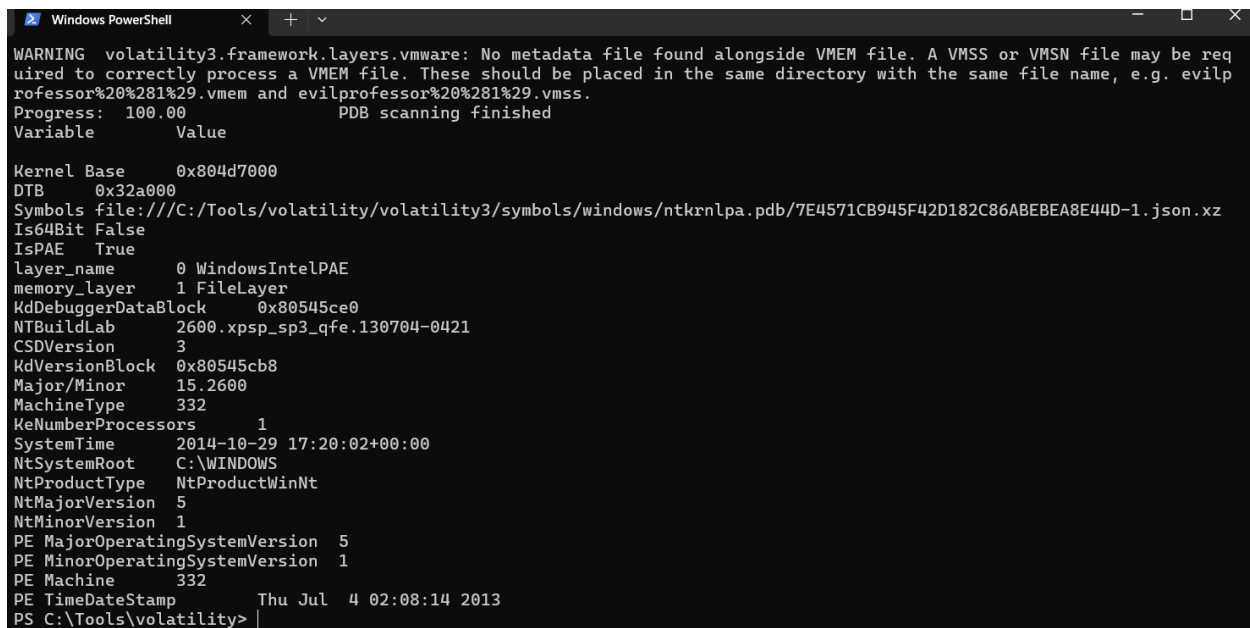
*Fig 2: obtaining a raw file from the directory successfully*

This PC > Local Disk (C:) > Tools > dumpit

Name	Date modified	Type	Size
DESKTOP-QE5QNCM-20241202-134548	02-12-2024 07:19 PM	RAW File	75,85,792 ...
Dumplt	02-12-2024 05:36 PM	Application	203 KB

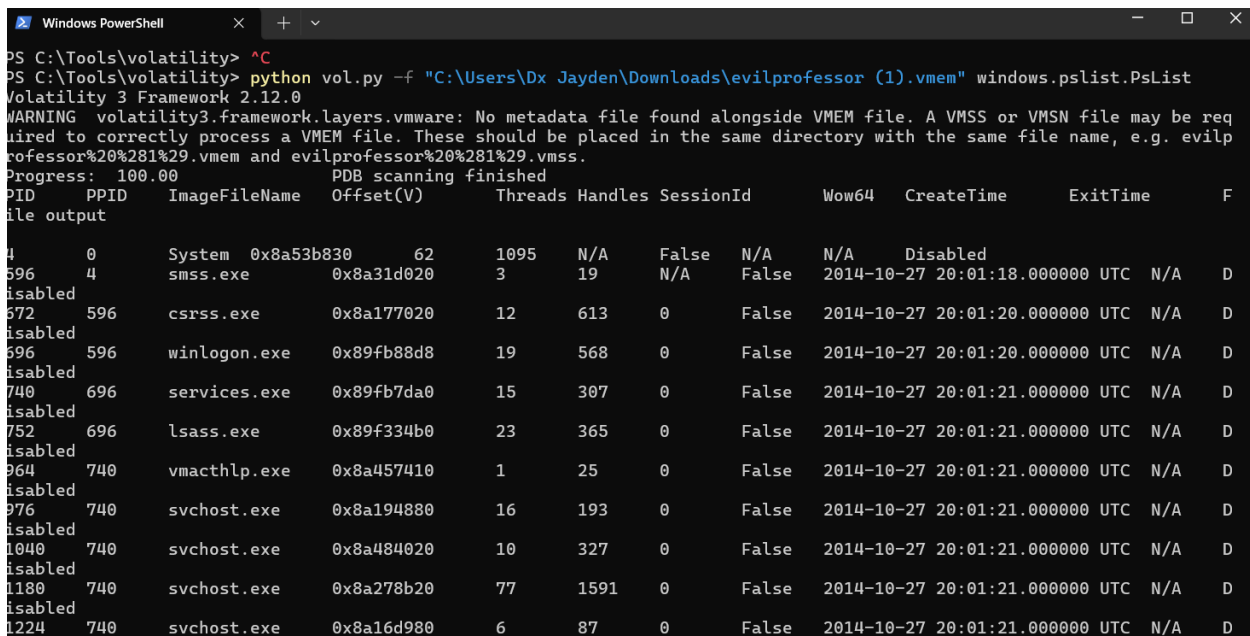
*Fig 3: The obtained raw file*

## Memory Analysis Lab



```
WARNING volatility3.framework.layers.vmware: No metadata file found alongside VMEM file. A VMSS or VMSN file may be required to correctly process a VMEM file. These should be placed in the same directory with the same file name, e.g. evilprofessor%20%281%29.vmem and evilprofessor%20%281%29.vmss.
Progress: 100.00 PDB scanning finished
Variable Value
Kernel Base 0x804d7000
DTB 0x32a000
Symbols file:///C:/Tools/volatility/volatility3/symbols/windows/ntkrnlpa.pdb/7E4571CB945F42D182C86ABE8EA8E44D-1.json.xz
Is64Bit False
IsPAE True
layer_name 0 WindowsIntelPAE
memory_layer 1 FileLayer
KdDebuggerDataBlock 0x80545ce0
NTBuildLab 2600.xpsp_sp3_qfe.130704-0421
CSDVersion 3
KdVersionBlock 0x80545cb8
Major/Minor 15.2600
MachineType 332
KeNumberProcessors 1
SystemTime 2014-10-29 17:20:02+00:00
NtSystemRoot C:\WINDOWS
NtProductType NtProductWinNt
NtMajorVersion 5
NtMinorVersion 1
PE MajorOperatingSystemVersion 5
PE MinorOperatingSystemVersion 1
PE Machine 332
PE TimeDateStamp Thu Jul 4 02:08:14 2013
PS C:\Tools\volatility>
```

Fig 4: Checking the profile using volatility



```
PS C:\Tools\volatility> ^C
PS C:\Tools\volatility> python vol.py -f "C:\Users\Dx Jayden\Downloads\evilprofessor (1).vmem" windows.pslist.PsList
Volatility 3 Framework 2.12.0
WARNING volatility3.framework.layers.vmware: No metadata file found alongside VMEM file. A VMSS or VMSN file may be required to correctly process a VMEM file. These should be placed in the same directory with the same file name, e.g. evilprofessor%20%281%29.vmem and evilprofessor%20%281%29.vmss.
Progress: 100.00 PDB scanning finished
file output
```

PID	PPID	ImageFileName	Offset(V)	Threads	Handles	SessionId	Wow64	CreateTime	ExitTime	F
4	0	System	0x8a53b830	62	1095	N/A	False	N/A	Disabled	
596	4	smss.exe	0x8a31d020	3	19	N/A	False	2014-10-27 20:01:18.000000 UTC	N/A	D
672	596	csrss.exe	0x8a177020	12	613	0	False	2014-10-27 20:01:20.000000 UTC	N/A	D
696	596	winlogon.exe	0x89fb88d8	19	568	0	False	2014-10-27 20:01:20.000000 UTC	N/A	D
740	696	services.exe	0x89fb7da0	15	307	0	False	2014-10-27 20:01:21.000000 UTC	N/A	D
752	696	lsass.exe	0x89f334b0	23	365	0	False	2014-10-27 20:01:21.000000 UTC	N/A	D
964	740	vmacthlp.exe	0x8a457410	1	25	0	False	2014-10-27 20:01:21.000000 UTC	N/A	D
976	740	svchost.exe	0x8a194880	16	193	0	False	2014-10-27 20:01:21.000000 UTC	N/A	D
1040	740	svchost.exe	0x8a484020	10	327	0	False	2014-10-27 20:01:21.000000 UTC	N/A	D
1180	740	svchost.exe	0x8a278b20	77	1591	0	False	2014-10-27 20:01:21.000000 UTC	N/A	D
1224	740	svchost.exe	0x8a16d980	6	87	0	False	2014-10-27 20:01:21.000000 UTC	N/A	D

Fig 5: Finding the oldest processes, launching cygrunsrv.exe, detecting active processes, and verifying instances of the cmd.exe process



```
Windows PowerShell
PS C:\Tools\volatility> python vol.py -f "C:\Users\Dx Jayden\Downloads\evilprofessor (1).vmem" windows.psscan.PsScan
Volatility 3 Framework 2.12.0
WARNING volatility3.framework.layers.vmware: No metadata file found alongside VMEM file. A VMSS or VMSN file may be required to correctly process a VMEM file. These should be placed in the same directory with the same file name, e.g. evilprofessor%20%281%29.vmem and evilprofessor%20%281%29.vmss.
Progress: 100.00 PDB scanning finished
PID PPID ImageFileName Offset(V) Threads Handles SessionId Wow64 CreateTime ExitTime F
file output
3852 3076 iexplore.exe 0x9658020 33 826 0 False 2014-10-29 17:18:25.000000 UTC N/A D
isabled
488 1576 cmd.exe 0x969cb20 1 33 0 False 2014-10-29 16:52:05.000000 UTC N/A Disabled
2308 488 keylogger-local 0x969d638 1 24 0 False 2014-10-29 16:52:10.000000 UTC N/A D
isabled
1604 1576 cmd.exe 0x96a5020 1 32 0 False 2014-10-29 16:52:17.000000 UTC N/A Disabled
3100 360 ipconfig.exe 0x9866af8 0 - 0 False 2014-10-29 17:20:02.000000 UTC 2014-10-29 17:20:02.000000 UTC Disabled
3148 2360 chrome.exe 0x98822d0 6 135 0 False 2014-10-29 17:18:15.000000 UTC N/A D
isabled
1140 1576 CodeMeterCC.exe 0x991c8d8 1 82 0 False 2014-10-27 21:59:29.000000 UTC N/A D
isabled
1988 1576 ctfmon.exe 0x991d528 1 77 0 False 2014-10-27 21:59:29.000000 UTC N/A D
isabled
1232 1576 jusched.exe 0x99212d8 2 222 0 False 2014-10-27 21:59:28.000000 UTC N/A D
isabled
2828 2360 chrome.exe 0x993a7c8 5 135 0 False 2014-10-27 21:59:52.000000 UTC N/A D
isabled
1172 1576 MagicDisc.exe 0x9966da0 1 32 0 False 2014-10-27 21:59:29.000000 UTC N/A D
isabled
1272 740 alg.exe 0x998e870 6 109 0 False 2014-10-27 20:01:34.000000 UTC N/A Disabled
```

Fig 6: Checking the instances of cmd process

```
Windows PowerShell
PS C:\Tools\volatility> python vol.py -f "C:\Users\Dx Jayden\Downloads\evilprofessor (1).vmem" windows.pstree.PsTree
Volatility 3 Framework 2.12.0
WARNING volatility3.framework.layers.vmware: No metadata file found alongside VMEM file. A VMSS or VMSN file may be required to correctly process a VMEM file. These should be placed in the same directory with the same file name, e.g. evilprofessor%20%281%29.vmem and evilprofessor%20%281%29.vmss.
Progress: 100.00 PDB scanning finished
PID PPID ImageFileName Offset(V) Threads Handles SessionId Wow64 CreateTime ExitTime A
udit Cmd Path
4 0 System 0x8a53b830 62 1095 N/A False N/A N/A - - -
* 596 4 smss.exe 0x8a31d020 3 19 N/A False 2014-10-27 20:01:18.000000 UTC N/A \
Device\HarddiskVolume1\WINDOWS\system32\smss.exe - -
** 672 596 csrss.exe 0x8a177020 12 613 0 False 2014-10-27 20:01:20.000000 UTC N/A \
Device\HarddiskVolume1\WINDOWS\system32\csrss.exe - -
** 696 596 winlogon.exe 0x89fb88d8 19 568 0 False 2014-10-27 20:01:20.000000 UTC N/A \
Device\HarddiskVolume1\WINDOWS\system32\winlogon.exe - -
*** 752 696 lsass.exe 0x89f334b0 23 365 0 False 2014-10-27 20:01:21.000000 UTC N/A \
Device\HarddiskVolume1\WINDOWS\system32\lsass.exe - -
*** 740 696 services.exe 0x89fb7da0 15 307 0 False 2014-10-27 20:01:21.000000 UTC N/A \
Device\HarddiskVolume1\WINDOWS\system32\services.exe - -
**** 132 740 TNSLNR.EXE 0x8a454980 3 89 0 False 2014-10-27 20:01:27.000000 UTC N
/A \Device\HarddiskVolume1\Oracle\Product\10.2.0\AccessDataDB\bin\TNSLNR.EXE - -
**** 1672 740 svchost.exe 0x8a16cda0 6 93 0 False 2014-10-27 20:01:26.000000 UTC N
/A \Device\HarddiskVolume1\WINDOWS\system32\svchost.exe - -
**** 1800 740 mdm.exe 0x8a3766f0 5 85 0 False 2014-10-27 20:01:26.000000 UTC N/A \
Device\HarddiskVolume1\Program Files\Common Files\Microsoft Shared\VS7DEBUG\mdm.exe - -
**** 1040 740 svchost.exe 0x8a484020 10 327 0 False 2014-10-27 20:01:21.000000 UTC N
/A \Device\HarddiskVolume1\WINDOWS\system32\svchost.exe - -
**** 1684 740 CodeMeter.exe 0x8a078da0 6 126 0 False 2014-10-27 20:01:26.000000 UTC N
/A \Device\HarddiskVolume1\Program Files\CodeMeter\Runtime\bin\CodeMeter.exe - -
```

Fig 7: To check the parent-child relationships and identifying terminated processes, sshd.exe service spawning & spawning of mysqld-nt.exe

```
Windows PowerShell
** 3852 3076 iexplore.exe 0x89658020 33 826 0 False 2014-10-29 17:18:25.000000 UTC N/A \
Device\HarddiskVolume1\Program Files\Internet Explorer\iexplore.exe
* 488 1576 cmd.exe 0x8969cb20 1 33 0 False 2014-10-29 16:52:05.000000 UTC N/A \Device\
HarddiskVolume1\WINDOWS\system32\cmd.exe
** 2308 488 keylogger-local 0x8969d638 1 24 0 False 2014-10-29 16:52:10.000000 UTC N/A \
Device\HarddiskVolume1\keylogger-local.exe
* 816 1576 vmtoolsd.exe 0x899a64f8 6 281 0 False 2014-10-27 21:59:29.000000 UTC N/A \
Device\HarddiskVolume1\Program Files\VMware\VMware Tools\vmtoolsd.exe
* 1232 1576 jused.exe 0x899212d8 2 222 0 False 2014-10-27 21:59:28.000000 UTC N/A \
Device\HarddiskVolume1\Program Files\Common Files\Java\Java Update\jused.exe
* 1456 1576 WINWORD.EXE 0x8a36bda0 9 920 0 False 2014-10-29 17:14:42.000000 UTC N/A \
Device\HarddiskVolume1\PROGRA~1\MICROS~2\Office12\WINWORD.EXE
* 948 1576 rundll32.exe 0x8a2c9940 4 76 0 False 2014-10-27 21:59:28.000000 UTC N/A \
Device\HarddiskVolume1\WINDOWS\system32\rundll32.exe
* 1140 1576 CodeMeterCC.exe 0x8991c8d8 1 82 0 False 2014-10-27 21:59:29.000000 UTC N/A \
Device\HarddiskVolume1\Program Files\CodeMeter\Runtime\bin\CodeMeterCC.exe
* 1172 1576 MagicDisc.exe 0x89966da0 1 32 0 False 2014-10-27 21:59:29.000000 UTC N/A \
Device\HarddiskVolume1\Program Files\MagicDisc\MagicDisc.exe
* 1176 1576 GrooveMonitor.e 0x8a18c368 1 119 0 False 2014-10-27 21:59:28.000000 UTC N/A \
Device\HarddiskVolume1\Program Files\Microsoft Office\Office12\GrooveMonitor.exe
PS C:\Tools\volatility> python vol.py -f "C:\Users\Dx Jayden\Downloads\evilprofessor (1).vmem" windows.hollowprocesses.H
ollowProcesses
Volatility 3 Framework 2.12.0
WARNING volatility3.framework.layers.vmware: No metadata file found alongside VMEM file. A VMSS or VMSN file may be req
uired to correctly process a VMEM file. These should be placed in the same directory with the same file name, e.g. evilp
rofessor%20%281%29.vmem and evilprofessor%20%281%29.vmss.
Progress: 100.00 PDB scanning finished
PID Process Notes
PS C:\Tools\volatility> |
```

Fig 8: Checking of hidden processes

## 4. Problem Solving and Troubleshooting

### Memory Acquisition Lab

#### Problem: Usage of DumpIt Tool to acquire memory for analysis

**Solution:** When the DumpIt utility was used, the proper administrator rights were used. To enable the tool to access the system memory, a permission screen first arose, requesting confirmation. The memory acquisition was finished without any more problems after the proper permissions were given.

### Memory Analysis Lab

#### Problem 1: Determining Active Processes

**Solution:** When the windows.pslist.PsList plugin was executed, the RAM dump showed 28 running processes.

#### Problem 2: Detecting Instances of cmd.exe

**Solution:** Three instances of cmd.exe utilizing the windows.pslist.PsList and windows.psscan.PsScan plugins were found throughout the study. According to this plugin, we observe that three cmd.exe processes are active.

#### Problem 3: Identifying Parent-Child Relationships and Terminated Processes

**Solution:** The parent-child relationships were displayed and 27 terminated processes were found using the windows.pstree.PsTree plugin. The following are the names of some of the processes: Services, TNSLNR, svchost, CodeMeter, lsass, winlogon, csrss, and SMS.

#### **Problem 4: Determining the Oldest Executing Process**

**Solution:** Keylogger-local was identified as the oldest running process by the windows.pslist.PsList plugin.

#### **Problem 5: Identifying the Parent Process of sshd.exe**

**Solution:** Using the windows.pstree.PsTree plugin, it was discovered that cygrunsrv.exe was the parent process of sshd.exe.

#### **Problem 6: Identifying the Parent Process of mysqld-nt.exe**

**Solution:** Using the windows.pstree.PsTree plugin, it was discovered that services.exe was the one that started the mysqld-nt.exe process.

#### **Problem 7: Detecting Hidden Processes**

**Solution:** No hidden processes were detected using the windows.hidden\_modules.HiddenModules and windows.hollowprocesses.HollowProcesses plugins.

The reasons are given here as follows:

- ❖ No Malicious Activity Detected: System Integrity
- ❖ Memory Dump Completeness.
- ❖ No Use of Anti-Forensic Techniques.
- ❖ Type of Malware

## **5. Conclusion and Recommendations**

The lab showed fundamental methods for acquiring and analyzing memories. Parent-child relationships, terminated processes, and running processes were all revealed by tools such as DumpIt and Volatility. The system seems to be clean during memory capture if there are no hidden processes.

### **Recommendations**

Future laboratories should incorporate more complex situations that include realistic issues with malware obfuscation and anti-forensics. Furthermore, employing a variety of memory analysis methods would broaden viewpoints regarding forensic techniques.

## 6. Reference

- ❖ Volatility Foundation. (n.d.). *Volatility Framework Documentation*. Retrieved from [Volatility Docs](#).
- ❖ DumpIt Tool Documentation. (n.d.). *Tool Guide for Memory Acquisition*.