NAME: \_Coleton Sanheim\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_



Lab 7:   
Memory Analysis and Documentation

ITSC 306: Computer Forensics

Table of Contents

[Lab Outcome 4](#_Toc494964283)

[Readings 4](#_Toc494964284)

[Introduction 4](#_Toc494964285)

[1.0 Lab Set-Up 5](#_Toc494964286)

[2.0 Volatility 5](#_Toc494964287)

[Questions 5](#_Toc494964288)

ITSC 306: Computer Forensics

Lab 7: Memory Analysis and Documentation

Lab Outcome

* Import a captured memory image. Use Volatility and specific plugins to analyze the memory. Create a basic procedure and results report.

Readings

Download and review the [Volatility Memory Forensics Cheat Sheet](https://blogs.sans.org/computer-forensics/files/2012/04/Memory-Forensics-Cheat-Sheet-v1_2.pdf).

Introduction

Your co-worker is complaining about suspicious activity on his computer. He tells you that the last thing he did was open a PDF file attached in an email he received from a colleague. You tell him you may be able to help. You have a RAM capture of the system and you can begin an examination.

Examine the RAM by following and answering the included questions to determine the possible cause of your co-worker’s complaint. Document your procedure and findings to create a basic procedure and results report. One option is to open a text editor. Another idea is to direct the output of the commands to a text file and add to it with each command to format a report, or copy and paste the results into a final report.

**Sample Report**

20170427

1610

I copied the U6L2.vmem file to the SIFT Desktop. I ran md5sum to verify the file had not changed.

**Results**

1615

I ran the Volatility Plugin [ \*\*\*\*\*\*\*\*\*\* ] to determine what profile to use with Volatility.

**Results**

1618

To determine what processes were running on this system, I ran the [\*\*\*\*\*\*] plugin.

**Results**

Continue answering and documenting the process.

1. Lab Set-Up
2. Locate the memory capture **U6L2.vmem** and copy to your SIFT Forensic workstation.

File: U6L2.vmem

MD5: 20d420729287026a3f55704154bd6163

1. Volatility
2. Use Volatility on the provided image to complete the following steps and to answer the following questions.
3. Use gedit to document your actions to generate a basic report named **U6L2\_(Name).txt**.

Note: Remember to document all the commands you run.

## Questions

1. What is the command to determine which Volatility profile to use with this capture?
2. Run this command. What suggested profiles can be used with this capture?
3. When was this image created?
4. What processes were running on this person’s computer?
5. Review the results. Do you notice anything?
6. Your co-worker stated the last this he did was to open a PDF file. Is there any executable in the output worth investigating? What is the file?
7. What is the AcroRd32.exe file’s PID? What is the Parent Executable and its PID?
8. List the network connections that were opened on the system.
9. Review the results. Using the file’s PID, did the suspicious file make a network connection? Document your findings.
10. Run the whois command on the IP. Who does the IP resolve to?
11. What sockets are associated to the suspicious PID? Use grep to isolate 1752.
12. You suspect the AcroRd32.exe file contains malware. Dump the file for additional analysis to a folder on your system.
13. Before you report your findings, run the plugin **screenshot**. Did the plugin provide any additional evidence?
14. Dump the hivelist to recover any Registry Hives.
15. Run **hashdump** to recover the account password hashes. Output the results to a text file.
16. Can you determine the Administrator account password?
17. Install **John the Ripper**.
18. From a Terminal, run sudo apt-get install john.
19. Run the command john (Path to the exported password file you created in question o).
20. Run the command john Desktop/U6L2/passwords.