Name: _____ Student ID:_____

You will need:
Sift Workstation Installation Guide (Assignment 2)
memory_2024_Sep_12_215606 .raw (assignment 2)

COS30015 IT Security

Lab 12 week 12 (Optional Lab)

This lab will demonstrate how a forensic environment can be deployed to analyse a memory capture. The Sift Workstation is to be deployed as a virtual machine. This needs to be done on a device where you can safely create a new virtual machine.

Basic steps are provided for memory analysis, with this optional lab serving as in introduction to enable you to analyse the memory capture. It will not give you step by step instructions.

Task 1 Install the Sift Workstation via Option 2A

Follow the guide attached to the assignment titled SIFT Workstation Installation Handbook.pdf. This walks you through the required steps to have a functioning forensics device.

Task 2 Copy over the memory capture

Once you have installed the Sift Workstation you will need to copy over the memory_2024_Sep_12_215606.raw file. This file is compressed, so you will need to extract it in the virtual machine.

All steps from here can be obtained via a command reference:
https://github.com/volatilityfoundation/volatility/wiki/command-reference

Task 3 Analyse the profile

Determine the image info of the memory capture so you can apply the right profile to analyse the capture further. Note, this will take a while and likely resource intensive. This will be used in all further commands.

Task 4 Explore the memory capture

Familiarise yourself with items which can be performed. Consider commands such as:

- pslist
- pstree
- netscan
- shellbags

Task 5 Explore files on disk

It is recommended you explore a command that lets you export to determine all files that have existed on the disk

Task 6 Dump process memory

It is recommended you investigate how to dump the memory of a process (memory resident pages).

Task 7 Investigate strings

It is recommended you investigate how to output the strings of a process. These can then be further investigated. Note, you can simply just call the utility without the .exe extension as your workstation is Linux. Hint, 16-bit bigendian.