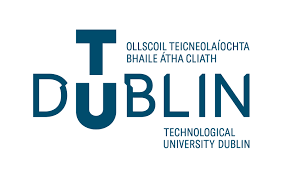
**Forensics CA2 Memory Analysis**

**Submission 01/05/2022**

****

**Name: Philip Herweling**

**Student No.: C18470774**

**Email: c18470774@mytudublin.ie  
Lecturer: Mr Jonathan McCarthy**

**Network Analysis**

For this part of the assignment I will be describing in detail the process to following in examining a network packet capture.

Before I start describing the process one should follow, I will explain what a packet capture is. Packet capture is the action of capturing Internet Protocols IP packets to review for analysis.

Step 1.)

The first step is identifying the data source. This involves figuring out what out there on the network. This has to be done before the analysis starts as you can’t analyse something if you don’t know it exists. The next step is identifying the types of source you are dealing with and what data you can get from them. There are different methods in identifying data source you have t choose which methods are best suited for the job on hand.

Step 2.)

The next step is determining the best way to collect data from the identified data sources. There are two main ways of collecting this data the first is Agent-based collection and the second is agentless collection.

Agent-based collection:

This technique is when one deploys software on your data source. These so called aga=ents can collect and array of information such as information on running processes, I/O network communication, system resource performance etc.

Agentless collection:

As the name suggests this this method doesn’t employ agents rather they use processes protocols and API’s already supported by the data source. The data gathered using this technique is known as granular data.

Step 3.)

**Memory Analysis**

In this part of the assignment I will be attempting to answer the six questions and complete the memory analysis on the memory image which was allocated to me. For this section I used an ubuntu virtual machine which runs the Linux operating system.

**F1 - How was the RAM profile identified? What version of the OS is this potentially?**

The command I used to find out the ram profile and what version the OS is I used the following command: ./vol.py -f /home/philip/Documents/Memory.raw imageinfo

Graphical user interface, text

Description automatically generated

As you can see from the screen shot this command shows me all the information about the machine the image was taken from.

The command shows me the processors, CPU etc. It also tells me that the machine being used ran the Windows 7 operating system.

**F2 - State how many processes were running at the time. Give the full OS process  
list.**

**A picture containing table

Description automatically generated**

In order to determine how many processes are running on the image I used the command that can be seen in the screenshot above. This gave me a list of all the current processes. I determined that there were 47 processes open by adding | wc -l to the end of the command. This command just counts all the lines which pslist prints out.



The pslist command prints all the current processes running in the terminal. I have a screenshot with a few of the processes but not all of them as it would take up to much space in the document.

**F3 - How many files were open at the time? How many jpeg files were open at the  
time?**

**Text

Description automatically generated**

I used the filescan command in order to determine how many files were open on the image. The screenshot above again shows some of the files but not all of them as there were to many open in order to include them all in this document. I tried counting the files by adding | wc -l to the end of the command but was getting errors.



I determined that there were 6803 files open on the disk image.

Text

Description automatically generated

In order to get all the .jpg files I modified the first command and added | grep .jpg. This returned only the files with a .jpg extension. There were 25 .jpg files of the disk image. The grep command searches for strings in files and that’s why I decide to use it in order to determine how many .jpg files there were on the disk image.



**F4 - What searches appear in the Internet history? What browser was used in the  
search?**

Text

Description automatically generated

A lot more search history was printed in the terminal but for the sake of this documents length I wont show it all. The iehistory command is what I used to show the internet history. As you can see the command returns the browser that was used, the username of the user browsing the internet, location etc.

I determined that there was two browsers used internet explorer and google chrome.

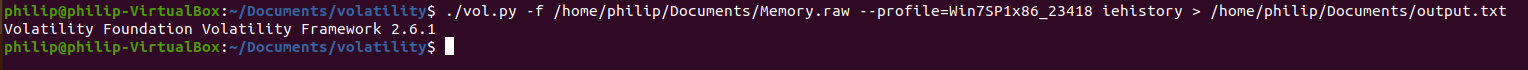
**F5 - A file called duck.gif was downloaded. When did this happen? What program do  
you think was used to open the file? Give reasons for your answer.**

The first thing I done was use the grep command with the iehistory command to see how much that would show me. This didn’t really tell me what I wanted to know so I decided to change my approach.

Text

Description automatically generated

I decided to output all of the internet browsing history into a txt file called output.txt. This allowed me to search for duck.gif and allowed me to see more details on when it was downloaded etc.



Graphical user interface, text, application

Description automatically generated

I determined that duck.gif was downloaded in 22013-03-13 at 21:16:56.

From the information I was able to gather it was opened using chrome and internet explorer:

Text, letter

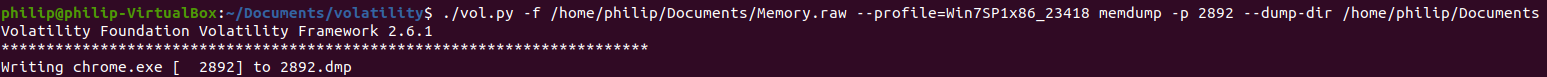
Description automatically generated

Text

Description automatically generated

**F6 - Choose a likely process and dump its memory to a file. Examine the dump with  
strings. Search for ASCII strings and UTF16 strings. Find something and point it out.**

In order to do the memory I dump I had to use the following command:



This dumps all the chrome process into my documents folder and stores it in a file called 2892.dmp. the process that chrome uses is process 2892.