**Chapter 2**

**Live Acquisition and Analysis**

**V1**

**A blue outline of a bird with a crown and text

Description automatically generatedSID: 2103022**

**Anglia Ruskin Final Project**

**Table of Contents**

[**Introduction** 2](#_Toc159770207)

[**Objective** 2](#_Toc159770208)

[**1.0** **Process Capture** 3](#_Toc159770209)

[**2.0 RAM Capture** 6](#_Toc159770210)

[**3.0. Retrieving files from RAM** 7](#_Toc159770211)

# **Introduction**

The second chapter covers Random Access Memory (RAM) forensics allowing an investigator to gather large amounts of important information about a user’s system. RAM is volatile and does not always save to the Hard drive. This chapter aims to teach the reader how to firstly acquire system RAM on Windows 10 and how to search for results to identity data worthy of being evidence by finding jpegs only saved in memory.

# **Objective**

* Create a process capture in the ‘dmp’ format using Magnet Process Capture
* Create a raw image.
* Import a memory image in the ‘mem’ formatting and search for ‘jpgs’.

1. **Process Capture**

1.Login as Digital-Forensics and use the password **‘password’** to login to the VM.

A login screen with a beach and rocks

Description automatically generated

2. Launch Magnet Process Capture found in the tools folder on the **Desktop. Desktop>Tools> MagnetProcessCapture**

A screen shot of a computer

Description automatically generated

3. You should see an application that looks like the figure below.

A screenshot of a computer

Description automatically generated

|  |  |
| --- | --- |
| **Section** | **Description** |
| Select Processes to Capture | Main windows in middle of screen. Reveals all currently running process on current system so if a new process starts after you opened the application you can click ‘refresh list’ for this to appear. Can select or unselect all by selecting the individual boxes or using the ‘check all’ or ‘uncheck all’ boxes. |
| Select an Output Folder | Allows the user to select a location to hold the captured processes. |
| Start | Starts the capture going. |

4. Click ‘Check All’

A screenshot of a computer

Description automatically generated

5. Copy the following location for adding an output folder. **C:\Users\Digital-Forensics\Desktop\EVIDENCE**

A screenshot of a computer

Description automatically generated

6.Click Start.

A grey rectangular sign with black text

Description automatically generated

7. Wait for the capture too complete and the output should look like the figure below.

A screenshot of a computer error message

Description automatically generated

# **2.0 RAM Capture**

1. Launch Magnet RAM Capture found in the tools folder on the **Desktop. Desktop>Tools> MRCv120.**

A computer screen shot of a computer

Description automatically generated

2. Click browse and copy the following location for adding an output folder. **C:\Users\Digital-Forensics\Desktop\EVIDENCE** and name your file ‘**ram\_dump1’**.

A screenshot of a computer

Description automatically generated

3. Wait for the following pop up as seen in the figure below and then your ram capture is complete.

A screenshot of a computer

Description automatically generated

# **3.0. Retrieving files from RAM**

1. Launch FTK imager found in the tools folder on the Desktop. **Desktop>Tools> FTK imager**.

A screenshot of a computer

Description automatically generated

2. Click ‘File’ then click ‘Add Evidence Item’.



3. Click ‘Image File’ then click ‘next’.

A screenshot of a computer

Description automatically generated

4. Click ‘Browse…’ and locate the ‘memdump.mem’ file as shown in the figure below.

A screenshot of a computer

Description automatically generated

5. Click finish.



6. Open the ‘memdump.mem’ from the evidence tree panel.

A blue rectangle with black text

Description automatically generated

7. Right click on the bottom right panel and select ‘Fit to window’.

A screenshot of a computer program

Description automatically generated

8. Right click on the bottom right panel and select ‘Find’.

9. From this screen its possible to search for headers and footers of a file. A JPEG file header is FF D8 FF E0 in Hex, and the footer is FF D9. Enter the header, check the type is ‘Binary(hex)’ and click ‘Find’.

A screenshot of a computer

Description automatically generated

10. If correctly entered the figure below should match your result.



11. Select the text highlighting the header and drag to the end of the footer.

12. Right click on the highlighted text and select ‘Save selection’.

A screenshot of a computer program

Description automatically generated

13. Save the file as ‘image1.jpg’ in the ‘Evidence’ folder on the Desktop.

A white and blue rectangular object with a blue border

Description automatically generated

14. Locate the file path and open the image to reveal an image like the figure below.

A blue and black logo

Description automatically generated

15. The chapter is complete, and you can now create a process capture, RAM capture and can extract data from RAM. You can close all applications and return to the desktop for Chapter 3 or shutdown if you wish to continue later.