PROG8290W22 - Assignment 5

**Check eConestoga for due date.**

## Introduction

In this assignment, we will use the Caine 11.0 Incident Response Live DVD to perform a simple (as in shallow, not easy) forensic analysis of a computer.

The computer image we will use is the same image as we used for Assignment3. If you accidentally deleted your copy, please return to the Assignment3 specification and follow those steps to download and validate the image files.

Similarly, if you haven't downloaded the Caine Incident Response Live DVD Version 11, please do so now. It is available at `https://www.caine-live.net/page5/page5.html`.

## Preparation

Before starting the analysis, you will want to have/create a Caine virtual machine image that boots/runs live off the DVD image and has an additional virtual hard drive (formatted using exFAT) for evidence storage.

By formatting this drive in exFAT format, you will be able to attach it to a Windows virtual machine and be able to read/transfer the data as required.

## Specification

### Part 1 – Memory collection

a. In much the same way you did for Assignment 3, download and configure the 'target' Virtual machine to run within VirtualBox. Following the specific instructions in the course Digital Forensics Handbook, image the memory of your 'target' system after booting the system.

**Take a full screenshot of your system, showing both the running Virtual machine and the command prompt window with the imaging command shown (similar to the screen snippet shown in the Handbook, but you must submit an entire - full resolution screen shot).**

After this step is complete, you can power down the Assignment 3 virtual machine.

b. After copying this memory dump to your Caine system, start your analysis with a Volatility `imageinfo` examination. **Snap a full screen shot and include in final report.**

Part 2 – Forensic imaging of disk

Ensuring that your Assignment 3 virtual disk is attached to your Caine Virtual Machine, boot into Caine.

Mount your evidence disk RW and use Guymager to create a "Expert Witness Format" image of your Assignment 3 disk. **As the capture is running, snap a full screen shot and include in final report.**

Part 3 – Image analysis

a. Mount your newly acquired "E01" file using `ewfmount`. **Snap a full screen shot and include in final report.**

b. Extract the `user` users `NTUSER.dat`. Once the command has finished printing its response, **Snap a full screen shot and include it in final report (ensuring that the tail of the command output is still visible).**

Part 4 – Memory dump analysis

Before starting this Part, make sure you have updated Volatility to the latest available version.

a. Using Volatility extract a list of processes running on the system at the time of the scan. Once the command has completed outputting its response, **snap a full screen shot and include in final report (ensuring that the tail of the command output is still visible).**

b. Again, using Volatility, identify the `war-ftpd` process and dump its process content to a file. Once the command has completed outputting its response, **snap a full screen shot and include it in final report (ensuring that the tail of the command output is still visible).**

Part 5 – Timeline creation

Use `fls` then `Volatility` to create timelines for your system. Combine these timelines (into what we call a SuperTimeline), convert to .CSV file, then boot Windows 10 and open and review the file in TimelineExplorer. **Snap a full screen shot and include in final report (ensuring that the entire Window is shown (and the item count (lower right) is visible)).**

Part 6 – Image Analysis

Shut the Caine system down, boot into Windows 10 and attempt to open the dumped process in IDA pro. **Regardless of the outcome, snap a screen shot**

**of this recovered file in IDA Pro or whatever error message is displayed on screen.**

Deliverable

You will submit a written report (MSWord or PDF only) containing screen shots as required, see Specification and Marking Rubric sections. Please include any required explanations and/or answer the questions posed in the Specifications section.

Please do not zip your submission and do make sure all the screenshots are clearly legible.

Marking Rubric

Wrap your screen shots into a professional looking Word document formatted as if it were an actual forensic report.

List of Screenshots:

| **Part** | **Description** | **Weight** |
|---|---|---|
| 1a | Memory capture to file | 5% |
| 1b | Volatility: memory capture imageinfo | 5% |
| 2 | Disk capture to file | 5% |
| 3a | Mount disk image | 10% |
| 3b | Extract/display Registry file | 20% |
| 4a | Volatility: capture ps list | 15% |
| 4b | Volatility: extract process image | 15% |
| 5 | Create Timeline, display in TimelineExplorer | 15% |
| 6 | Open extracted process image in IDA (or Ghidra) | 10% |

Standard deductions

- 5% for not having name and assignment # in your Word/PDF document
- 10% for submitting a 'zip'ed (compressed) document
- 50% for submitting screenshots not inserted/formatted into Word/PDF document
- 100% for any question that does not include requested/supporting screenshots ** This includes screen shots that are either too small or too grainy to read its contents **

- 100% for any question whose screenshots do not have date/time stamp.
- 100% for a date/time earlier than 4/1/2022 and later than the submission date.
- Regular late submission penalty (see Program Handbook)
- Penalties applied as per the Student Handbook for any plagiarism and/or academic dishonesty.