# Cardiff School of Computer Science and Informatics

## Coursework Assessment Pro-forma

**Module Code**: CM3111

**Module Title**: Forensics

**Lecturer**: Michael Daley

**Assessment Title**: Lard Land donuts case.

**Assessment Number**: 1

**Date Set**: w/b 16.11.2020

**Submission Date and Time**:04.12.2020at 9:30am

**Return Date**: 30.12.2020

This assignment is worth 60% of the total marks available for this module. If coursework is submitted late (and where there are no extenuating circumstances):

1 If the assessment is submitted no later than 24 hours after the deadline, the mark for the assessment will be capped at the minimum pass mark;

2 If the assessment is submitted more than 24 hours after the deadline, a mark of 0 will be given for the assessment.

Your submission must include the official Coursework Submission Cover sheet, which can be found here:

<https://docs.cs.cf.ac.uk/downloads/coursework/Coversheet.pdf>

## Submission Instructions

|  |  |  |  |
| --- | --- | --- | --- |
| Description | | Type | Name |
| Cover sheet | **Compulsory** | One PDF (.pdf) file | [student number].pdf |
| Coursework | **Compulsory** | Two PDF (.pdf) or Word file (.doc or .docx) Consisting of a Technical report and a Court/Summary report. | Report Title\_[student number].pdf/doc/docx |

Any deviation from the submission instructions above (including the number and types of files submitted) will result in a mark of zero for the assessment or question part

## Assignment

**Supplied materials:**

Instructions.

Scenario.

Image of a suspect USB drive.

Photo images of Mobile phone front and rear view (ExhibitAfront.jpg and ExhibitArear.jpg)

Exhibits B & C pcap captures of network traffic at time of incident)

**Basic Requirements:**

You are required to examine the USB image it is suggested that you use the Autopsy Tool, but you can use any method you wish.

**If you are using Autopsy you will first need to download and install Autopsy on your Windows,Apple or LINUX machine. The URL can be found below.**

https://www.sleuthkit.org/autopsy/

You are expected to show that you have followed the basic Forensic Methodology we have gone through to examine the USB image, and produce a scientific report that defines the methods you have used, the results obtained and answers the following questions:

1. Is there anyone else implicated? If so who? Show any evidence supporting your findings.
2. Where was Penelope planning to travel to? Show any evidence supporting your findings.
3. Can you find the secret recipe? How was this hidden and how did you recover it?
4. What other steps if any have been taken to hide the evidence?
5. Comment on the condition of the phone in exhibit A.
6. What is the likelihood of obtaining evidence from this phone?
7. Do a bit of background research on the options available to try and extract data from such a phone in this condition.

**HINTS:**

1. Look for deleted data.
2. Build a “dirty word list” and search the image.
3. There are four main files to recover. One file in particular should give you a clue as to where the picture is hidden and how to extract it.

**Basic Steps to follow:**

If you are starting the case in AUTOPSY. Then here are a few steps to get you started.

When it asks for an image use the usbimage.dd supplied.

Ensure you select “partition”.

Although you have not been given a specific time you should still revise the steps given in the lectures and create a timeline.

Then start the analysis. All this can be done through the AUTOPSY interface. Remember that it uses all the tools we have covered.

**DELIVERABLES:**

You are required to write a properly structured scientific report detailing your analysis and findings.

The report should contain a section outlining the scientific method you took to arrive at your conclusions.

It should also indicate how you extracted the evidence.

Remember that another examiner should be able to reproduce your results using the method you describe.

You should also remember the Chain of Custody, and show your evidence has not been tampered with.

You are also required to produce a summary of your findings in layman terms that could be used in court. This should be a short separate report from your main scientific report.

Any problems feel free to email me.

[DaleyM@cardiff.ac.uk](mailto:DaleyM@cardiff.ac.uk)

## Learning Outcomes Assessed

**L03, L04, LO6, L07**

# Criteria for assessment

**This piece of work is worth 60%**

Credit will be awarded against the following criteria.

As a guide

20 Marks allocated to Investigation process.

15 Marks allocated to the structure and presentation of the

technical report

5 Marks results and Court/summary.

8 Marks for evidence presentation.

8 Marks for finding and documenting all the evidence.

4 Marks for the background research on extracting evidence

from mobile phones.

Undergraduate

1st (70-100%)

2.1 (60-69%)

2.2 (50-59%)

3rd (40-49)

Fail (0-39%)

# Feedback and suggestion for future learning

Feedback on your coursework will address the above criteria. Feedback and marks will be returned on 30.12.2020 via Learning Central