Module Title:	Computer Forensics Project
Module Code:	CSD3998
Module Leader:	Dr Ian Mitchell

Challenges to Digital Forensics

Student:	Anita Patel
Student Number:	M00000000
Supervisor:	S. Hara

A thesis submitted in fulfilment of the requirements
for the degree of BSc (Hons) Computer Forensics

Dept. of Computer Science

2017-18

Declaration

I, Anita Patel, declare that this thesis titled, "Challenges to Digital Forensics" and the work presented in it are my own. I confirm that:

- This work was done wholly for a degree at Middlesex University.
- Where any part of this thesis has previously been submitted for a degree or any other qualification at Middlesex University or any other institution, this has been clearly stated.
- Where I have consulted the published work of others, this is always clearly attributed.
- Where I have quoted from the work of others, the source is always given. With the exception of such quotations, this thesis is entirely my own work.
- I have acknowledged all main sources of help.
- Where the thesis is based on work done by myself jointly with others, I have made clear exactly what was done by others and what I have contributed myself.

Signed:

Date:

Abstract

The Thesis Abstract is written here (and usually kept to just this page). The page is kept centred vertically so can expand into the blank space above the title too ...

Acknowledgements

The acknowledgements and the people to thank go here, don't forget to include any support you may have received from family and friends ...

Contents

Chapter 1

Proposal

1.1 Introduction

Include a few words here about the background and motivation of the project.

This can be helped by explaining what has happened in the past; what you are going to do in the present; and how this action will help and change the future.

1.2 Aims

This should be a general aim of the overall project. This should be explained in one or two paragraphs.

1.2.1 Objectives

These are a list of clearly defined objectives that can be aligned to outcomes in the project. We can define the success of the project based on these fulfilling these objectives.

- Research
- Explore Hypotheses
- Design Experimental Framework
- Run experiments under Experiment Framework and test hypotheses
- Analyse Results
- Provide detailed recommendations and guidelines

1.2.2 Deliverables

Deliverables are a result of actions that complete and attempt to satisfy objectives and can include:

- Complete proposal
- Complete Research Ethics approval
- Complete research on specified related area
- Complete research on another specified related area
- Complete Literature Review
- Conduct Experiments under completed Designed Experimental Framework
- Complete Software Development
- Complete Experiments based on Experimental Framework
- Collate and gather information and data from Experiments
- Analyse Results and complete write-up of results
- Complete Conclusions
- Complete Turn-it-in submission
- Print, bind and submit two hard copies to Unihelpdesk.

1.3 Resources

List any software or hardware that may be required for the completion of the project.

- Forensic ToolKit
- The Sleuth Kit
- Laptop
- 10 1Gb memory sticks
- 2 128Gb SSD
- FTK Imager

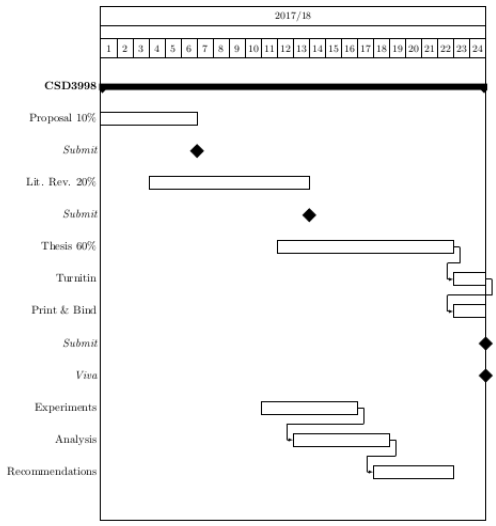


Figure 1.1: GANTT Chart showing indicative milestones.

1.4 Schedule

Typically include a GANTT chart indicating when the objectives and deliverables are met.

This can be completed by Excel or other dedicated software and then imported into this document as shown in Fig.1.1.

1.5 Summary

Optional, but this section could outline and emphasise the structure of the thesis. It could also be used to emphasise what the project is about and can sometimes be used to disambiguate any areas, e.g., your project may look into applying text mining to e-discovery and you may want to emphasise that this is an application and not a project on text mining.

The structure of the rest of this thesis (never refer to the thesis as a paper and always write in third person) is as follows: Chapter 2 covers the literature review and current research related to the problem; Chapter 3 investigates the experiment and rationalises the method undertaken; Chapter 4 analyses the results; and Chapter 5 includes the recommendations and conclusions.

Chapter 2

Literature Review

2.1 Introduction

Outlining the main area you are researching. This may also include any motivation for investigation.

2.2 Subject

You can divide your Literature Review into several sections, one for each topic/area you are reviewing.

2.2.1 title

Each subject area will probably be broken down to several subsections.

title

It is generally unnecessary to go further than the subsection level, however, in rare circumstances the subsubsection command can be used.

2.3 Citation & Reference

Exercises show two there are two parts to a citation: the citation; and the reference. There are many styles and configurations of the citations and references, which the exercises will make clear.

Essentially, to start with, we are going to keep this simple and use the plain bibliography setting. As we advance the national bibliography package can be used and this is in the exercises on citations. This setting orders all bibliography items in alphabetical order and only uses the cite command. It does have its restrictions and we will come across these and how to cope with them. The

following is an example paragraph using citations and a plain bibliography and should be adequate to get us started.

The first generation of Neural Networks are generally considered as Perceptrons [4]. Minsky and Papert [3] wrote a critique of the perceptron which showed that it could not solve non-linear problems, typically XOR. To solve the non-linear problem Rumelhart, Hinton and Williams [5] made an enormous contribution with the Back-propagation error Artificial Neural Network, ANN. This and related ANN are generally referred to as second generation and inspire many of the techniques used in machine learning. The third generation of neural networks are based on biologically-inspired neurons and are generally referred to as, "spiking neurons". Oddly many third generations are based on research pre-dating to first and second generations, namely Hebbian Learning [1]. These spiking neurons can be built into bigger networks to solve complex problems,e.g., see [2].

2.4 Summary

Conclude on your main findings and how they are going to contribute to solving objectives.

This thesis is an outline and can be deviated from. For example, it would be completely justified to have two Literature Review Chapters, if the subject areas are unrelated and completely separate. Often new research can be considered as two subject areas merged together to form a new area, e.g., text-mining and e-discovery. This would result in two literature review chapters: i) text-mining; and ii) e-discovery.

Chapter 3

Method

3.1 Introduction

Go over the objectives of the experiment relying on new research in your literature review.

3.2 Experiment 1

Many Experiment Frameworks require two experiments, one with x, the other without. These are often referred to as control experiments.

3.3 Experiment 2

All experiments are repeated for reproducibility, you need to show how each stage of the experiment is designed to help prove or disprove your hypothesis.

3.4 Summary

You have no results, however, you have a clear and concise experiment to run. With your knowledge from Literature Review you can mention the expected outcomes of each experiment.

Chapter 4

Analysis & Results

4.1 Introduction

Include any set up for the experiment. This could be as follows:

- Architecture: x86_64
- CPU op-mode(s): 32-bit, 64-bit
- Byte Order: Little Endian
- CPU(s): 4
- On-line CPU(s) list: 0-3
- Thread(s) per core: 2
- Core(s) per socket: 2
- Vendor ID: GenuineIntel
- CPU family: 6
- Model: 61
- CPU MHz: 500.000
- RAM: 8Gb

4.2 Experiment 1

Use graphics to display results. Most results can be shown in tables. Use package longtables if you have trouble getting all data into a single page. Remember to label and reference the table.

4.3 Experiment 2

Experiment 2 should differ from Experiment 1. Each experiment should be repeated a number of times for reproducibility. Do not confuse Experiment 2 as a repeat of Experiment 1, they are different.

4.4 Summary

Bad results happen, but it is not bad science. Still write up the results. If given time run more experiments. Rejecting or accepting an hypothesis is still a result worth writing up.

Good results will yield a clear direction and give clear recommendations and guidelines that can be mentioned here and emphasised in the next chapter - it is OK to repeat.

Chapter 5

Conclusions

Usually the weakest chapter, but the most important. This is where you state your main contribution. Computer Science and Computer Forensics is unlike many other topics, you can become an expert in a small area of computing, say FAT file systems in a matter of months. What you are studying, not only should you enjoy, but you should be an expert in. In Medicine it could take 20 years to be an expert in some field.

Have all you aims and objectives been met, if so where and how did you prove them?

5.1 Recommendations

This expertise should leave you to some insight and recommendations based on your knowledge of the subject and your results. These are mentioned here.

5.2 Future Work

Any new areas this research could lead to.

5.3 Reflections

How would you complete this project again?

5.4 Summary

Odd to have a summary in a chapter entitled conclusion, however, the purpose of this is to end on a high note. Your reader will have been examining and assessing this thesis for some time and you need to finish it on a high note. Make it succinct and punchy. You should include: the aims and objectives;

the hypothesis; any outcomes; any development; accept or reject hypothesis; results; any recommendations; and finally your main contribution.

Bibliography

[1] D. Hebb. *The Organization of Behavior*. John Wiley and Sons, 1949.

[2] Christian R Huyck and Ian G Mitchell. Compensatory hebbian learning for categorisation in simulated biological neural nets. *Biologically Inspired Cognitive Architectures*, 6:3–7, 2013.

[3] Marvin Minsky and Seymour Papert. Perceptrons. 1969.

[4] Frank Rosenblatt. The perceptron: a probabilistic model for information storage and organization in the brain. *Psychological review*, 65(6):386, 1958.

[5] David E Rumelhart, Geoffrey E Hinton, and Ronald J Williams. Learning internal representations by error propagation. Technical report, DTIC Document, 1985.

Appendices

Appendix A

Code

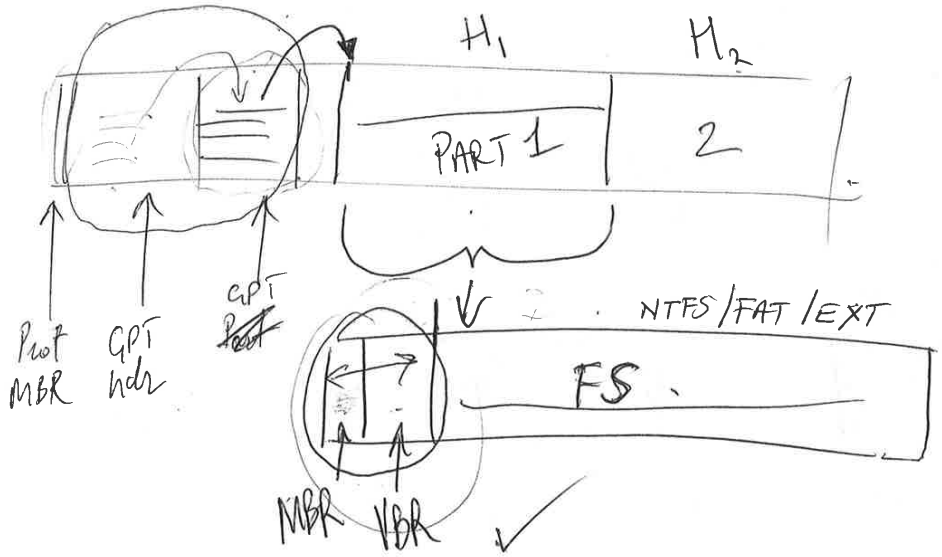
```
#record
popTL.getPop().record(['spikes'])
popTR.getPop().record(['spikes'])
popRight.getPop().record(['spikes'])
popLeft.getPop().record(['spikes'])
popExp.getPop().record(['spikes'])
```

Appendix B

Meetings with Supervisor

24/11/2016.

- TRIM
  - works when removing GPT header & part
  - does not work when removing protected MBR.



- removal/deconstruction of "GPT" does not preserve state of the parts.

① ~~delete~~ decon GPT X – evidence – facts

② decon each MBR/VBR ✓

Appendix C

Ethical Approval

$cat(\overset{f}{H_1}, \overset{t}{H_2}) \rightarrow \overset{f}{H_3}$. check