[TITLE OF FINAL YEAR PROJECT]

[NAME OF STUDENT]

UNIVERSITI TEKNIKAL MALAYSIA MELAKA

**BORANG PENGESAHAN STATUS LAPORAN**

JUDUL: [TITLE OF FINAL YEAR PROJECT]

SESI PENGAJIAN: [20xx / 20xx]

Saya: \_\_\_\_[NAME OF STUDENT IN CAPITAL LETTER]\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

mengaku membenarkan tesis Projek Sarjana Muda ini disimpan di Perpustakaan Universiti Teknikal Malaysia Melaka dengan syarat-syarat kegunaan seperti berikut:

1. Tesis dan projekadalah hakmilik Universiti Teknikal Malaysia Melaka.
2. Perpustakaan Fakulti Teknologi Maklumat dan Komunikasi dibenarkan membuat salinan unituk tujuan pengajian sahaja.
3. Perpustakaan Fakulti Teknologi Maklumat dan Komunikasi dibenarkan membuat salinan tesis ini sebagai bahan pertukaran antara institusi pengajian tinggi.
4. \* Sila tandakan (✓)

|  |  |  |
| --- | --- | --- |
| \_\_\_\_\_\_\_\_\_\_ | SULIT | (Mengandungi maklumat yang berdarjah keselamatan atau kepentingan Malaysia seperti yang termaktub di dalam AKTA RAHSIA RASMI 1972) |
| \_\_\_\_\_\_\_\_\_\_ | TERHAD | (Mengandungi maklumat TERHAD yang telah ditentukan oleh organisasi / badan di mana penyelidikan dijalankan) |
| \_\_\_\_\_\_\_\_\_\_ | TIDAK TERHAD |  |

|  |  |  |
| --- | --- | --- |
|  |  |  |
| (TANDATANGAN PELAJAR) |  | (TANDATANGAN PENYELIA) |
| Alamat tetap: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |  | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |  | Nama Penyelia |
| Tarikh: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |  | Tarikh: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |

CATATAN: \* Jika tesis ini SULIT atau TERHAD, sila lampirkan surat daripada pihak berkuasa.

[TITLE OF FINAL YEAR PROJECT]

[NAME OF STUDENT]

This report is submitted in partial fulfillment of the requirements for the

Bachelor of [Computer Science (Software Development)] with Honours.

FACULTY OF INFORMATION AND COMMUNICATION TECHNOLOGY UNIVERSITI TEKNIKAL MALAYSIA MELAKA

[YEAR OF SUBMISSION]

# DECLARATION

I hereby declare that this project report entitled

[TITLE OF FINAL YEAR PROJECT]

is written by me and is my own effort and that no part has been plagiarized

without citations.

STUDENT : \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Date : \_\_\_\_\_\_\_\_

([NAME OF STUDENT])

I hereby declare that I have read this project report and found

this project report is sufficient in term of the scope and quality for the award of

Bachelor of [Computer Science (Software Development)] with Honours.

SUPERVISOR : \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Date : \_\_\_\_\_\_\_\_

([NAME OF THE SUPERVISOR])

# DEDICATION

[To my beloved parents...]

# ACKNOWLEDGEMENTS

[I would like to thank En. Muhammad bin Ahmad for giving assistant to complete this project successfully…...

I would also like to thank my beloved parents who have been giving me support and motivation throughout my project…]

# ABSTRACT

[Abstract must start from here. Abstracts should be concise, WRITTEN IN ONE SPACING and justification and **NOT MORE THAN 300 WORDS** IN A SINGLE PAGE. Abstract is not the same as synopsis or report summary. Abstracts are WRITTEN WITH **ONE PARAGRAPH**. It should briefly state **the field of report studies, problems to be solved, solutions, research processes; and the results obtained.**]

# ABSTRAK

[Abstrak mesti bermula disini. Abstrak mestilah ringkas, DITULIS DALAM SATU LANGKAU dan justifikasi **TIDAK LEBIH DARIPADA 300 PERKATAAN** DALAM SATU MUKASURAT sahaja. Abstrak tidak sama dengan sinopsis atau ringkasan tesis. Abstrak DITULIS DALAM **SATU PERENGGAN**. Ia hendaklah menyatakan dengan ringkas **bidang kajian tesis, masalah yang hendak diselesaikan, cara penyelesaian, proses penyelidikan; dan keputusan yang diperolehi**.]

# table of contents

|  |  |
| --- | --- |
|  | **PAGE** |

DECLARATION ii

DEDICATION iii

ACKNOWLEDGEMENTS iv

ABSTRACT v

ABSTRAK vi

table of contents vii

list of tables ix

list of figures x

List of Abbreviations xi

List of ATTACHMENTS xii

Chapter 1: INTRODUCTION 1

1.1 About Chapters and First Subtitle 1

1.1.1 Second Subtitles 2

1.1.1.1 Third Subtitles 2

Chapter 2: literature review AND PROJECT METHODOLOGY 3

2.1 About Figures 3

Chapter 3: ANALYSIS 5

3.1 About Tables 5

Chapter 4: DESIGN 7

4.1 About Table of Content 7

Chapter 5: IMPLEMENTATION 9

5.1 About List of Tables 9

5.2 About List of Figures 9

5.3 About List of Figures 9

5.4 About List of Figures 9

5.5 About List of Figures 10

Chapter 6: TESTING 11

6.1 About References 11

Chapter 7: PROJECT CONCLUSION 12

7.1 Wrap-Up 12

references 13

# list of tables

|  |  |
| --- | --- |
|  | **PAGE** |

[Table 3.1: Table Example 5](#_Toc21534973)

# list of figures

|  |  |
| --- | --- |
|  | **PAGE** |

Figure 2.1: Caption Window 3

Figure 2.2: Caption Numbering Window 4

Figure 2.3: Example Figure with citation from a book (Pike, 2008. Used with permission) 4

Figure 4.1: How to update Table of Contents in this template 7

Figure 4.2: Updating the whole list 7

# List of Abbreviations

|  |  |  |
| --- | --- | --- |
| **FYP** | **-** | **Final Year Project** |

# List of ATTACHMENTS

|  |  |  |  |
| --- | --- | --- | --- |
|  | | | **PAGE** |
|  | | |  |
| **Appendix A** |  | **Sample of data** | **19** |
| **Appendix B** |  | **Analysis of data collection** | **78** |
| …….. |  | ………… |  |
| …….. |  | ………… |  |
|  |  |  |  |

# INTRODUCTION

## Introduction

Digital forensics is the usage of scientifically proven methods towards preservation, collection, validation, identification, analysis, interpretation, documentation, and presentation (Reith, Carr, & Gunsch, 2002). Computer forensic is divided into two steps, which is forensic in the occurrence area and laboratory forensic analysis (Kamal, Alfadel, & Munia, 2016). Forensic tools are also divided into two parts which are the hardware and software. To complete an investigation, forensic tools are required to capture the data. In this case, memory analysis tools are required to get the wanted data.

To speed up the processing time, a technique is selected and integrated, and a prototype will be developed to test the tool. This project focuses on the RAM as we can get a lot of information from it. This is because from RAM, investigators can see what occurs in the PC in specific point of time (Kamal, Alfadel, & Munia, 2016). It is expected that analysis processing time can speed up and improve the investigation process.For the first subtopic in each chapter, student can use Heading 2 style for the title. Do not leave any empty line before starting a new subtitle.

## Problem Statement

Next, memory is an important source of digital evidence in digital forensic investigations because it contains traces of criminal activities. These traces discover through the process of memory analysis. A memory analysis tool is used to retrieve volatile data from a computer's memory dump to identify the offender throughout this investigation. There is also problem where the processing time are becoming slower as alongside the growth of many things such as the growth of storage devices, I/O speed, and sophistication of digital forensic analysis, (Roussev, & Richard III, 2004).

Table 1.1 Summary of Problem Statement

|  |  |
| --- | --- |
| **PS** | **Problem Statement** |
| PS1 | The growth of high-capacity storage devices and I/O speed have made the processing time of digital forensic tool slow. |

## Project Question

Based on the problem statement, few memory analysis tools are required to be analysed. Deep study and analysis are required to know deeper about the tool that is used. The code of the tool may be analysed to find the way to fasten up the processing time.

Table 1.2 Summary of Problem Statement

|  |  |  |
| --- | --- | --- |
| **PS** | **PQ** | **Project Question** |
| PS1 | PQ1 | What are the tools used for analysing memory for digital forensics? |
| PS2 | PQ2 | What technique is used to improve the speed of processing time? |
| PS3 | PQ3 | How to improve the current memory analysis tool that can help forensic investigators effectively tracing the evidence of the incidents? |

## Project Objective

The aim of this project is to improve the processing time of a memory analysis tool. Based on this aim, three project objectives are derives as summarised in Table 1.3.

Table 1.3 Summary of Project Question

|  |  |  |  |
| --- | --- | --- | --- |
| **PS** | **PQ** | **PO** | **Project Objective** |
| PS1 | PQ1 | PO1 | To analyse memory analysis tools. |
| PS2 | PQ2 | PO2 | To identify the techniques for improving memory analysis processing time. |
| PS3 | PQ3 | PO3 | To integrate the techniques with existing tool for improving memory analysis processing time. |

## Project Scope

The scope of this project is:

### The project only focusing on the open-source memory analysis tools.

In this project, all the memory analysis tools used are only based on the open source only. Few memory analysis tools will be analysed, and one will be chosen to be improved. A specific technique will be used to the specific memory analysis tool so that a prototype can be developed to create a better processing time.

## Project Contribution

This project has contributed to several issues as presented in this section which are derived from the project aim and objectives described in Section 1.4. The summary of the research contributions is illustrated in Table 1.5.

Table . Summary of Project Contribution

|  |  |  |  |
| --- | --- | --- | --- |
| PS | PQ | PO | Project Contribution |
| PS1 | PQ1 | PO1 | Comparative analysis of memory analysis tools. |
| PQ2 | PO2 | Resolve the way of improving memory analysis tool. |
| PQ3 | PO3 | Produce prototype of the improved memory analysis tool. |

## Report Organisation

There are seven chapters to be presented in visualizing the work under study as depicted in Figure 1.1.

Figure .: Report Organization

Chapter 1: Introduction

Chapter 1 discusses the project background, the project gap, project questions, project aim, project objectives, project contributions and the report organisation.

Chapter 2: Literature Review

In Literature Review, it will discuss about the problem statement in more detail. Next, this chapter will also discuss the findings found in research papers that are related to this topic. Things that are required to be inserted here are such as citation of the research papers.

Chapter 3: Project Methodology

In Project Methodology chapter, it will discuss the method of how to complete this whole project. It will follow the project milestone given to make sure that each chapter are completed in time.

Chapter 4: Design

In Design chapter, it contains the preliminary analysis result of the project. As example, on ways to speed up the processing time and the result of the comparison between different memory analysis tools.

Chapter 5: Implementation

In Implementation chapter, it will talk about the way to implement the analysis. It includes the tools and requirement to complete the prototype. In this chapter also will talk about the process of creating the prototype to improve the current memory analysis tools.

Chapter 6: Testing and Analysis

In Testing and Analysis, it will talk about the way of testing the prototype. Testing of the prototype will be done using the same data as tested before the tool is upgraded. This is to check the difference between the speed of processing time.

Chapter 7: Conclusion

In Conclusion chapter, it concludes the result of the whole project. Starting from the design until testing and analysis chapter. This chapter will also conclude whether the project is a success or vice versa.

## Summary

This chapter explains the rough idea about the whole project. This can be seen from the explanation of the problem statement, project question, project objective and project scope. It directly explains on the improvement of memory analysis tools for digital forensic investigation. In the next chapter, which is the literature review, it will talk about the in depth regarding the research of memory analysis tools.

# literature review AND PROJECT METHODOLOGY

## Introduction

In previous chapter, the problem statement, project question, scope and objectives have been discussed. In this chapter, it will be about the literature review and project methodology of this project. The topics that will be discussed are listed below in Figure 2.1.

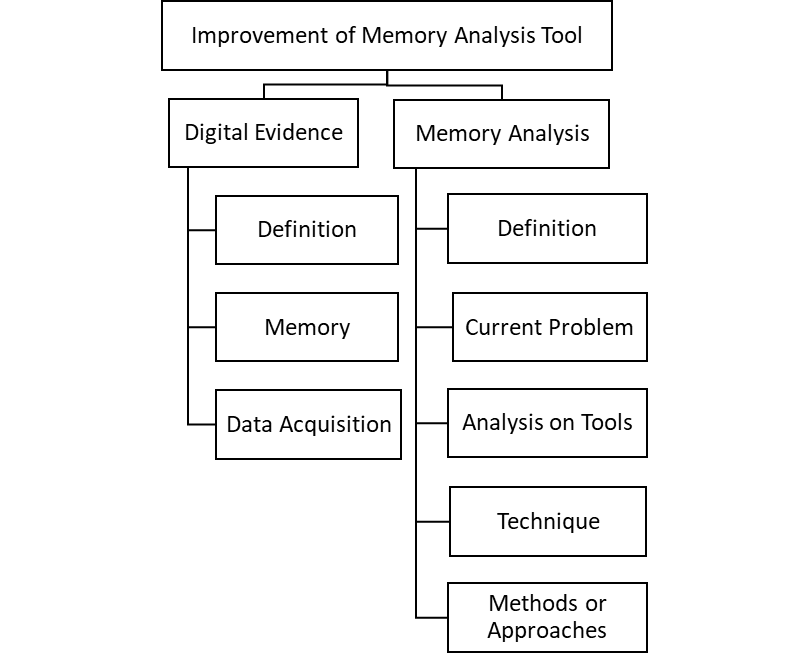


Figure . Framework of literature review

## Digital Evidence

### Definition

Digital evidence is any kind of data and information stored in binary form and is transmitted by electronic devices. It is found in computer, hard drives and even phones. Usually, digital evidence is linked to electronic crime and e-crime such as credit card fraud. There are two types of digital evidence which is volatile and non-volatile. Volatile is the type of data that are kept when the machine is running, which means the memory will be lost once the machine stopped running. Meanwhile, non-volatile is data stored in memory where the content is still available even when the machine stopped working.

### Memory

Memory is a type of cyber investigation which allows an investigator to detect unauthorized activity on target digital evidence such as server or computer. To achieve it, some special software is required. This software may capture the current state of the system’s memory as a snapshot file which is also known as a memory dump.

### Memory Acquisition

In every digital forensic investigation, the evidence collection phase is always the critical one. It is to ensure that the evidence and data collected are not damaged. In an article written by Gabriela Limon Garcia (2007), it is written that acquisition tools are separated into two approaches which are the hardware based and software based. The details of the example tools are as written in Table 2.1.

Table .: Data Acquisition Tools

|  |  |  |
| --- | --- | --- |
| Approaches | Tools | Explanation |
| Hardware based | Tribble | A hardware expansion card that accesses directly to the target’s memory to acquire volatile memory from a still running computer system while ensure of the integrity of the vital information in case of computer misconduct |
| FireWire bus | FireWire is a connection type for lots of electronic devices. It supports any speeds of devices to its nature of vary speed. |
| Software based | Data Dumper | A tool to dump segments of data. It works by extracting stream of binary data from source image. |
| Windows crash dump utility | Occurs when Windows no longer able to run properly. The system state will freeze, and any physical memory contents will be copied to the disk. |

## Memory Analysis

### Definition

Memory forensics (sometimes referred to as memory analysis) refers to the analysis of volatile data in a computer’s memory dump. Information security professionals conduct memory forensics to investigate and identify attacks or malicious behaviours that do not leave easily detectable tracks on hard drive data.

### Current Problem

Figure .: Current Problem of Memory Analysis

According to a paper titled Breaking the Performance Wall: The Case for Distributed Digital Forensics written by Roussev, Vassil, and Golden Richard III (2004), the advancement of current network technology has overwhelmed attempts of digital forensics investigations. These advance tools have absentmindedly decreased the speed of memory analysis. Below are the explanations on the current problem of memory analysis.

1. *High-capacity storage devices*

The growth of high-capacity storage device has increased the amount of time taken to complete the processing time. This is due to the massive amount of data that need to be tested by the tools. Based on the investigation done by Roussev, Vassil, and Golden Richard III (2004) by using FTK tools, it took them about 2 hours just to open just to solve a 6GB hard disk.

1. *Improvement of the I/O speed vs capacity gap*

This is due to the aggressive growth of CPU speed but linear growth of I/O transfer speeds (Roussev, Vassil, and Golden Richard III, 2004). As both components growth speeds are not the same, I/O transfer speeds unfortunately was left behind compared to the growth of high-capacity storage devices. In the same article written by Roussev, Vassil, and Golden Richard III, (2004), they said that if both have the same speed, the processing time to image a 20GB drive will be the same as it would be to image a 200GB drive. But unfortunately, that is not what happened currently.

1. *Sophistication enhancement of digital forensics analysis*

Many functions need little CPU processing power such as the cryptographic hashing of files, keyword indexing, and thumbnail generation. However, the dark side of it is that to complete more “sophisticated” evidence, it will require more CPU power (Roussev, Vassil, and Golden Richard III, 2004). For example, as written in the same paper, it said that classifying tens, hundreds, or thousands of images from a single digital forensics’ workstation would be awfully slow.

### Analysis on Tools

Tools that are used for memory analysis are such as Tribble, FireWire bus, Data Dump and CrashDump utility. The comparison for advantages of the tools is written in Table 2.2.

Table .: Tools Comparison

|  |  |  |  |
| --- | --- | --- | --- |
| Approaches | Tools | Advantage | Disadvantage |
| Hardware based | Tribble | Null system impact | Require preinstallation |
| FireWire bus | Hardware availability | Incompatible memory |
| Software based | Data Dumper | No disruption of service | In Windows 2003 there are no physical memory object |
| Windows crash dump utility | Minidump format | Certain keyboards are not compatible |

|  |  |  |
| --- | --- | --- |
| Tools | Advantage | Disadvantage |
| Magnet RAM Capture |  |  |
| RAM Capturer |  |  |
| Data Dumper |  |  |
| Windows crash dump utility |  |  |

### Techniques

Figure .: String Searching

In memory forensics, string searching is a traditional technique to search for valuable strings such as passwords, IP addresses and more private data (Gabriela Limon Garcia, 2007). Also, according to Gabriela Limon Garcia (2007) there are 3 approaches for string searching which are String.exe, Grep.exe and Clustering algorithms. For String.exe, string is defined as a program that returns strings from any initialized and loaded sections of object file. Next, grep is a programme used to seek for series of characters in a file (Gabriela Limon Garcia, 2007).

### Methods or Approaches

In a paper published, Impacts of increasing volume of digital forensic data: A survey and future research challenges, there are many solutions written in it. The list of solution are as follows:

1. *Data Mining*

Technique that is suitable to speed up the processing time is data mining. According to Darren Quick and Kim-Kwan Raymond Choo (2014), data mining is a specialty field that assists digital forensics in analysing. Darren Quick and Kim-Kwan Raymond Choo (as cited by Abraham, 2006) wrote data mining is useful with large datasets. The advantages of data mining are that it reduces the processing time, analysis cost, improve information quality and even able to discovers information that are hard to be discovered (Beebe and Clark, 2005). However, the downside of it is the general lack of understanding of data mining between the digital forensics (Darren Quick and Kim-Kwan Raymond Choo, 2014).

1. *Data reduction and subsets*

Data reduction is a process of evidence collection focusing on the ones that provide accurate analysis. This concludes that not every evidence will be collected but only those that are accurate. Quick and Choo (2014) summarises Data Reduction Framework which has helped full forensic analysis to collect any subset of data that has been reduced with intention of fast review.

1. *Triage*

This is a process of sorting research into different groups based on either the data is going to benefit the examination or vice versa (Parsonage, 2009). As explained by Darren Quick and Kim-Kwan Raymond Choo (2014), they focus on using an experienced partitioner to identify the data or evidence through quick investigation to figure out on which part of the partition that may contain the evidence.

## Proposed Solution

This project will be using data mining towards the data to improve the processing time of digital forensics. The data mining is chosen because it benefits digital forensics the most with its ability to reduce the processing time while at the same time improves the quality of the information. To complete this project, the scope will be limited only to free source which is to limit the bare minimum. The data will be run through over and pre-process. For instance, this project will test on different size of data at first to check on the speed of the processing time before making a full comparison between them. Plus, in paper titled Impacts of increasing volume of digital forensic data: A survey and future research challenges, the authors used data mining in relation to reduce the processing time.

## Conclusion

In conclusion, data mining will be used to improve the speed of processing time of memory analysis tools for digital forensic investigation. Next chapter will discuss on the methodologies that will be done throughout this project.

# ANALYSIS

## About Tables

Tables are printed within the body of the text at the center of the frame and labeled according to the chapter in which they appear. Thus, for example, tables in Chapter 3 are numbered sequentially: Table 3.1, Table 3.2. The label should be placed above the table itself and has the format shown in Table 3.1. Any text inside a table must follow “Table Text” style.

Table 3.1: Table Example

|  |  |
| --- | --- |
| Column Name | Column Name |
| Text | Text |

To insert label above a table, click “Insert Caption” under the “References” tab and select “Table” in the dropdown list, as shown in Figure 2.1. Click on “Numbering” and tick the “Include chapter number” and select “period (.)” as separator, as shown in Figure 2.2. When done, click “Update Table” to update the List of Tables.

If the table contains a citation, the source of the reference should be placed below the table.

To insert label above a table, click “Insert Caption” under the “References” tab and select “Table” in the dropdown list, as shown in Figure 2.1. Click on “Numbering” and tick the “Include chapter number” and select “period (.)” as separator, as shown in Figure 2.2. When done, click “Update Table” to update the List of Tables.

If the table contains a citation, the source of the reference should be placed below the table

# DESIGN

## About Table of Content

In this template, the table of contents rely on the use of styles to format chapter headings and subtitles and generates the table of content automatically. To generate the table of content in this template, place the cursor on the current table of content. Next, go to “References” tab and click on the “Update Table” icon, as shown in Figure 4.1.

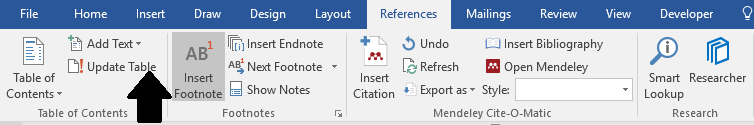


Figure 4.1: How to update Table of Contents in this template

In the “Update Table of Contents” window, choose option “Update the entire table” and click OK. Microsoft Word will generate a new table of contents based on the student’s updates.

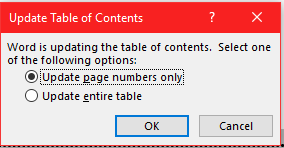


Figure 4.2: Updating the whole list

In the “Update Table of Contents” window, choose option “Update the entire table” and click OK. Microsoft Word will generate a new table of contents based on the student’s

# IMPLEMENTATION

## About List of Tables

To update List of Tables, place the cursor on the list that needs to be updated. Similar to the Table of Content, click on the icon “Update Table” under References tab to list down the updates, as shown in Figure 4.1

## About List of Figures

To update List of Figures, place the cursor on the list that needs to be updated. Next, click on the icon “Update Table” under References tab to list down the updates, as shown in Figure 4.1.

## About List of Figures

To update List of Figures, place the cursor on the list that needs to be updated. Next, click on the icon “Update Table” under References tab to list down the updates, as shown in Figure 4.1.

## About List of Figures

To update List of Figures, place the cursor on the list that needs to be updated. Next, click on the icon “Update Table” under References tab to list down the updates, as shown in Figure 4.1.

## About List of Figures

To update List of Figures, place the cursor on the list that needs to be updated. Next, click on the icon “Update Table” under References tab to list down the updates, as shown in Figure 4.1.

# TESTING

## About References

All works or studies referred to in the research report in the form of quotations or citations must be included in the references. The references should be written consistently in the Harvard Referencing format or in another format approved by the faculty. Students are encouraged to use reference manager software such as Mendeley to assist in creating citations and references.

Choose “Body Text 3” style for the list of the references.

# PROJECT CONCLUSION

## Wrap-Up

Please enjoy writing your FYP

# references

Buchwalow, I. B., and Böcker, W. (2010). Immunohistochemistry: basics and methods. Berlin: Springer Verlag.

Caamaño-Tubío, R. I., Pérez, J., Ferreiro, S., and Aldegunde, M. (2007). Peripheral serotonin dynamics in the rainbow trout (Oncorhynchus mykiss) Comparative Biochemistry and Physiology Part C: Toxicology & Pharmacology. 145(2): 245-255.

Cameron, A. A., Plenderleith, M. B. and Snow, P. J. (1990). Organization of the spinal cord in four species of elasmobranch fishes: cytoarchitecture and distribution of serotonin and selected neuropeptides. The Journal of Comparative Neurology. 297: 201-218.

Desa, M.I (1995). Bus fleet maintenance modeling in a developing country. Ph.D Thesis, University of Salford.

Improve indigenous housing now, government told, 2007. accessed 8 February 2009, <http://www.architecture.com.au/i-cms?page=10220>.

International Narcotics Control Board 1999, United Nations, accessed 1 October 1999, <http://www.incb.org>.

Theusen, G. J. and Fabrycky, W. J. (1984). Engineering Economy. 6th. Ed. Englewood Cliffs, N. J.: Prentice Hall. 150-178.