# INTRODUCTION

## Introduction

Digital forensics is the usage of scientifically proven methods towards preservation, collection, validation, identification, analysis, interpretation, documentation, and presentation (Reith, M., Carr, C., & Gunsch, G., 2002, p.2). Computer forensic is divided into two steps, which is forensic in the occurrence area and laboratory forensic analysis (Kamal, K. M. A., Alfadel, M., & Munia, M. S., 2016, p.1). 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.

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.

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, K. M. A., Alfadel, M., & Munia, M. S., 2016, p.1). It is expected that analysis processing time can speed up and improve the investigation process.

## Problem Statement

With memory analysis tools, there are problems where business commercial software tools are failed in which leads to dependency towards open-source tools (Kamal, K. M. A., Alfadel, M., & Munia, M. S., 2016, p.2). There is also problem where the processing time are slow. As example, Windbg tool has a disadvantage where it is isolated from each other (Garcia, G. L., 2007, pg.4)

Table 1.2‑1 Summary of Problem Statement

|  |  |
| --- | --- |
| **PS** | **Problem Statement** |
| PS1 | Current processing time for certain memory analysis tools are slow and can be upgraded to fasten up the speed. |

## Project Question

Based on the problem statement above, 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 1.3‑1 Summary of Project Question

|  |  |  |
| --- | --- | --- |
| **PS** | **PQ** | **Project Question** |
| PS1 | PQ1 | How to fasten up the processing time speed of the specific memory analysis tools? |

## Project Objective

Based on the project question above, this project embarks on the following objectives which is to analyse memory analysis tools. Next, is to identify the techniques for improving memory analysis processing time and lastly to integrate the techniques with existing tool for improving memory analysis processing time.

Table 1.4‑1 Summary of Project Question

|  |  |  |  |
| --- | --- | --- | --- |
| **PS** | **PQ** | **PO** | **Project Objective** |
| PS1 | PQ1 | PO1 | To analyse memory analysis tools to find the slowest one and improve the speed. |

## Project Scope

### Comparison of different type memory analysis tools.

Several types of memory analysis tools on any operating systems are tested using the same data to get the different speed of the processing time. 3 types of memory analysis tools from free source are downloaded to test the speed of processing time. All these tools will be tested using the same forensic data. All three tools’ processing time will be monitored and recorded before finding the one with the slowest processing time.

### Improvising the memory analysis tool processing time.

To improve the memory analysis tool, the most important step is to run the tools to examine the processing time using the data found. After that, the tool is monitored and analysed before documenting the gained result. The same tool later will be improvised form the code and repeat the same steps as before to document again the processing time whether it improves or not.

## Project Contribution

This project can contribute to digital forensics field especially towards speeding up the time taken for forensics to get a result from specific memory forensic tools. Other than that, by speeding up the processing time of the tool, hopefully it can more digital forensics to complete their investigation faster.

## Report Organisation

Chapter 1: Introduction

Introduction chapter discusses about the overall picture of the project. This chapter also explains about the scope and explains the gist of the whole project.

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.

## Conclusion

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.