CHAPTER 1

INTRODUCTION

Introduction

Nowadays, we all live in the digital era, which most information moves from one place to another digitally. The information can be derived easily from everywhere and send it to whoever, only in minutes or even seconds. Unfortunately, wherever we are, including in this digital information era, threats always exist, perhaps in the different shapes. One of the computer threats which always peering us in this era, is Computer Virus.

The virus is a threat, because it can do bad things to whomever. It can make the computer becomes slow, broken, or even it can delete the data. The virus can run automatically and hide the process, so that users cannot see the processes and activities, which occupied by virus. What can users see from the virus is what they have done.

Background of Study

The current tool that nearest to virus world now is AntiVirus (AV), as it can detect and [illegible] almost all kinds of virus. However, the AntiVirus cannot produce the analysis report, which is able to describe the viruses' behavior in details. Analysis report is quite important for those who want to learn how viruses actually act. Furthermore, people can eliminate the viruses from their PC and recover the Operating System from viruses attack by reading the virus behavior analysis report (FuYong, DeYu, & JingLin, 2009). Such kind of report is only provided by several tools, which mostly do not have a capability in virus detection system, such as CWSandbox, Capture, MBMAS, Joebox and ThreatExpert (FuYong, DeYu, & JingLin, 2009).

The aforementioned tools indeed are able to produce the behavior analysis report in details. Unfortunately, by using these tools, the type of malicious file, that have been tested, cannot be known. Even though the analysis report can be derived, it is not easy to determine which virus file is classified as traditional or polymorphic only by reading this report (Bayer, [illegible] FuYong, DeYu, & JingLin, 2009).

Based on the explanation above, a polymorphic virus analysis tool, which can solve both problems above, which are able to report the viruses' behavior as well as classify the tested virus, whether it is traditional or polymorphic virus needs to be developed.

Problem Statement

The problem statement in this report reviews the weaknesses that are found in the real world. There are two main reasons why virus behavior analysis system needs to be developed: The existing of antivirus products cannot impede the curiosity of common users to know the activity or behavior of the viruses. Antivirus is only able to produce the report which inform to us which file is malicious. It cannot produce the analysis report that describes the viruses' behavior. By this case, it could be difficult for common users to learn how viruses acts, and further, they will face the difficulties when they want to combat or eliminate the virus and recover the operating system by themselves. There are several tools and techniques proposed by other researchers which are able to analyze several types of malwares. However, they still can not distinguish and classify which file is classified as a traditional or polymorphic virus.

Research Questions

The main research questions for this study are given as follows:

What is polymorphic virus and how does it act and propagate?

How to monitor and analyze the behavior of virus, produce report in details, and classify the virus whether it is traditional or polymorphic virus?

How to test and validate the architecture which is used by the virus behavior analysis system to monitor and analyze the behavior of virus, produce report in details, and classify the virus whether as a traditional or polymorphic virus?

1.5 Research Objectives

Based on the research questions above, there are two objectives for this research. These objectives are:

1. To study the viruses' characteristic, behavior, and propagation technique which used by traditional and polymorphic virus.
2. To propose an architecture which can be used to monitor and analyze the behavior of virus, produce report in details, and classify the virus whether it is traditional or polymorphic virus.
3. To test and validate the architecture refering to the virus behavior analysis.

1.6 Research Methodology

The research methodology that has been used throughout the research is an iterative process where the study specifications consists of literature review by referring to some documents and books that lead to some ideas. Furthermore, Virus Monitoring and Analysis System (VMAS) for traditional and polymorphic virus will be developed.

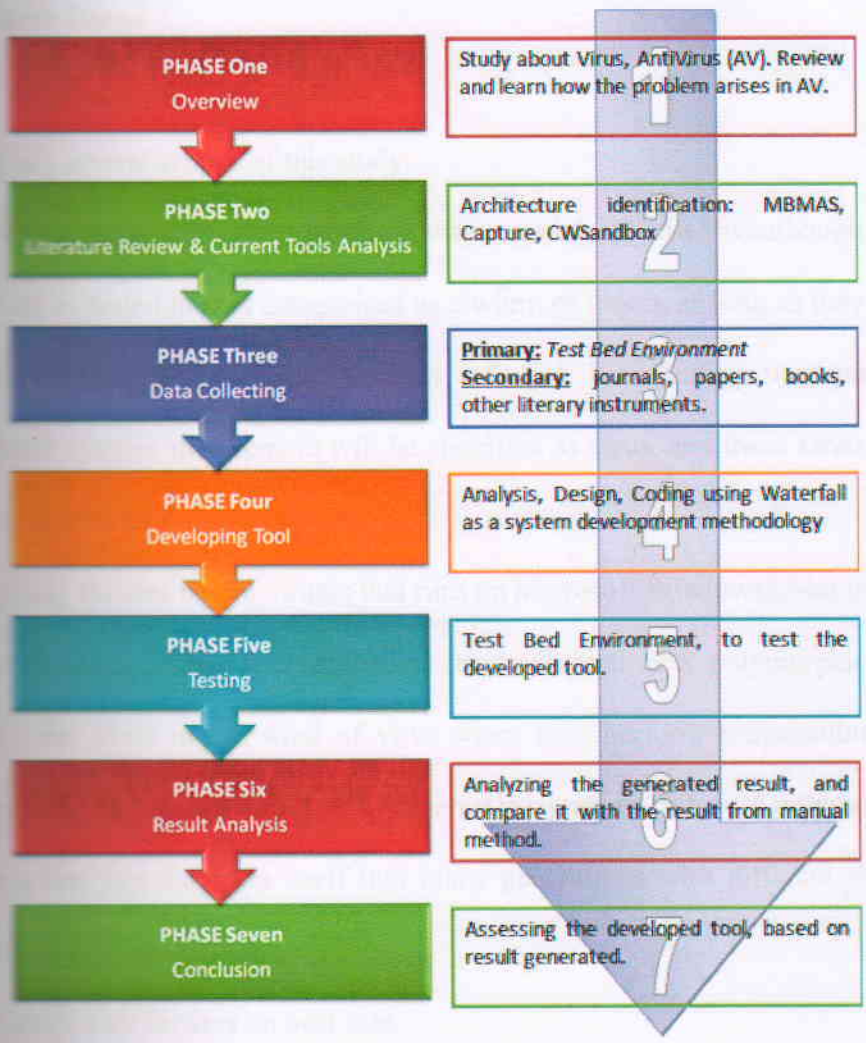

Figure 1.1: Research Methodology

In order to achieve the objectives, this research is divided into seven different phases. Figure 1.1 shows the research phases of this research, which are: research overview, literature review, collecting the required data, developing VMAS tool to monitor and analyze polymorphic and traditional virus, perform testing for the developed tool, and finally assessing the developed tool based on result generated.

Research Contribution

The contributions of this research are given as follows:

This system comes up with the analysis report, and it can be utilized by interested person to get a quick understanding of the purpose of a virus, either traditional or polymorphic virus.

By using this system, common users can learn more about virus, and find out which virus is classified as a traditional or polymorphic virus, and they can see the differences between traditional and polymorphic virus, especially in term of signature generated.

Beside the proposed architecture can be used by antivirus software directly, the produced report can be used by common users to eliminate the virus, either traditional or polymorphic virus, and recover the operating system as well.

With the ability to classify a virus, further, it can be utilized to create intelligent virus remover which is able to clean the system effectively either from traditional or even polymorphic virus attack.

Project Report Overview

Chapter 1, Introduction, this chapter provides a justification and also background information of this research, problem statement, research question, objective, methodology, and research contribution.

Chapter 2. Literature Review, this chapter explains about computer virus, including [illegible] viruses. It will be followed by the discussion about current architectures and tools [illegible] been proposed.

Chapter 3. Research Methodology, this chapter discusses the methodology which used [illegible] research objective, including research phase, system development methodology, [illegible] in collecting data.

Chapter 4. Implementation, it is the main part of this research, where analysis, design, [illegible] will be discussed in depth in this chapter.

Chapter 5. Testing, this chapter focuses on testing part of this research by which the [illegible] tool have been discussed and developed in the previous phase.

Chapter 6. Summary and Conclusion, this chapter will provide the summary of this [illegible] conclusions and future work.

[illegible] Conclusion

[illegible] on the aforementioned explanation, this study necessary to be conducted from [illegible] that antivirus software is indeed able to detect and defeat virus accurately, but it [illegible] analysis report regarding malicious behavior of the detected or identified virus. [illegible] actually there are several tools and architectures which have been proposed to [illegible] viruses' behavior. Unfortunately it cannot be used for differentiating between [illegible] polymorphic virus.

The objectives of this study are to study the virus characteristic, behavior, and [illegible] technique which used by traditional and polymorphic virus. After that, it will