CHAPTER 1
INTRODUCTION

1.1 Background

Internet is a huge media for communication and transaction very quickly and can connect wide area. internet give a positive impact because help people or organization get fast information in all sector. Especially in the present , the internet helps a lot of in education and work. On the other hand, with all the internet capabilities. The internet also opens opportunities for bad people to infiltrate, steal and destroy data through the internet by using malicious software as known as malware.

Malware is software that intended to damage computers systems. Some ways a system can be infected with malware is caused by the vulnerability of a system itself and mistake user. Malware installed generally unknowingly by victims. On the victim computer malware steal information and modify data quietly.

In this project, it is possible to recognize attacks and to create a program. The program is called a packet sniffer. A program that can filter and capture packet data traffic to observe the pattern of dangerous activities. With a known malware attack then the right action can be done immediately.

1.2 Scope

1. Packet sniffer program created using python programming language.
2. PHP programming language will be used to create data monitoring program which generated by the packet sniffer.
3. Sqlite3 will be used as database to store packet data from packet sniffer program.

4. Analyzing malware by comparing the data traffic of two computers where one of computer is infected with a virus.

1.3 Objective

Objectives to be achieved from this project are:

1. Can create a packet sniffer program to capture data traffic on the local network.
2. Can monitor network data traffic with web-based program.
3. Can identify malware that infects the computer.