CHAPTER I

INTRODUCTION

1.1 Introduction

Computer networks are the backbone and are a critical part of almost every organization. Computer networks facilitate information sharing that requires an efficient, high performance and errorless computer network. Impacts of an inefficient network impacts are unable to protect a network from viruses and intruders, e-mails cannot be received or sent, printers cannot be shared, unable to transfer data and remote database connections would be costly.

When the network is congested, a need to build software that performs data collection and analyses the data to identify problem continuously. Network monitoring is used the methodology used when trying to troubleshoot network related issues, watching network equipment and providing performance analysis.
1.2 Problem Statements

To design software that is able to monitor what is happening on the network in addition to knowing a real owner and a activity list of the owner automatically. All this using software which works by analysing the packets which are passing through it.

1.3 Project Objective

The objective of this project is to build software that will be used to identify owner of the captured packet and a list of its activities. Another objective is to analyse network packet in detail and extract characteristic of the packet.

1.4 Scope Of Project

In this project, the software uses Linux operating system as a platform. For language, Python and PHP were used and MySQL as the database. Ethereal is the main component behind this at it is being used to capture and provide packet data in a human readable and parse-able form. The software is currently running in campus FKE only.