BORANG PENGESAHAN STATUS TESIS

JUDUL:
EVALUATING DEVELOPMENT OF PACKET EXTRACTOR PROTOTYPE

SESI PENGAJIAN: 2011/2012

Saya, NORSUHAINI BT AHMAD RAZI

mengaku membenarkan tesis (PSM/Sarjana/Doktor Falsafah) ini disimpan di Perpustakaan Fakulti Teknologi Maklumat dan Komunikasi dengan syarat-syarat kegunaan seperti berikut:

1. Tesis adalah hakmilik Universiti Teknikal Malaysia Melaka
2. Perpustakaan Fakulti Teknologi Maklumat dan Komunikasi dibenarkan membuat salinan untuk 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 PENULIS)

Alamat tetap: Batu 1, Jln Ngulang,
Bukit Keteri, 02450,
Kangar, Perlis

Tarikh : _____

_____ (TANDATANGAN PENYELIA)

EN. NOR AZMAN BIN MAT ARIFF

Tarikh : _____

DEVELOPMENT OF PACKET EXTRATOR PROTOTYPE

NORSUHAINI BT AHMAD RAZI

This report is submitted in partial fulfillment of the requirements for the
Bachelor of Computer Science (Computer Networking)

FACULTY OF INFORMATION AND COMMUNICATION TECHNOLOGY
UNIVERSITI TEKNIKAL MALAYSIA MELAKA
2012

DECLARATION

I hereby declare this project report entitled

DEVELOPMENT OF PACKET EXTRACTOR PROTOTYPE

is written by me and is my own effort and that no part has been plagiarized without citations.

STUDENT : _____ Date: _____

(NORSUHAINI BT AHMAD RAZI)

SUPERVISOR : _____ Date: _____

(MR. NOR AZMAN BIN MAT ARIFF)

DEDICATION

This work is dedicated to my beloved family and siblings, who passed on a love of reading and respect for education.

To my supportive friends and my supervisor, thank you so much for assist and help.

ACKNOWLEDGEMENTS

Bismillahirrahmanirrahim

Alhamdulillah, Thanks to Allah SWT, whom with His willing give me the opportunity to complete this Final Year Project which is title 'Development of Packet Extractor Prototype'. This final year project report was prepared for Faculty of Information and Communication Technology (FTMK), Universiti Teknikal Malaysia Melaka (UTeM), basically for student in final year to complete the undergraduate program that leads to the degree of Bachelor of Computer Science. This report is based on the methods given by the university.

First and foremost, I would like to express my deepest thanks to my supervisor of this project, Mr. Nor Azman bin Mat Ariff for the valuable guidance and advice during my project research. He inspired me greatly to work in this project. His willingness to motivate me contributed tremendously to my project. . I also want to thanks the lecturers and technicians of FTMK for their cooperation during I complete the final year project that had given valuable information, suggestions and guidance in the compilation and preparation this final year project report.

Finally, an honorable mention goes to my lovely families and friends for their understandings and supports on myself in completing this project. Without helps of the particular that mentioned above, I would face many difficulties while doing this project.

ABSTRACT

This project aims to develop a network management tool that can be categorized as a packet analyzer. The idea is to provide methods and techniques for extracting data or packet in the network so that all activities of sending and receiving packets through the network card can be monitored. This is an idea to monitor the network to provide a way to extract data or packet in the network. This project should be able to monitor, open and save files transiting over the network. This project was only able to monitor only certain types of protocols FTP, ICMP, and HTTP. The main purpose of this project is to extract the data packet in the network in real time and analyze the protocol using the data at once can be a platform for research and enhancement of management tools in the future as the use of data mining. This software can be used in personal computers to monitor packets through the network. Oriented design of user-friendly interface is designed so that consumers can more easily understand how to use the software. Jpcap was chosen to capture packets and make the system run smoothly.

ABSTRAK

Projek ini dibangunkan bertujuan untuk membangunkan sebuah alat pengurusan rangkaian yang boleh dikategorikan sebagai penganalisa paket. Idea ini bertujuan untuk menyediakan cara atau teknik bagi mengekstrak data atau paket di dalam rangkaian supaya segala aktiviti penghantaran dan penerimaan paket yang melalui kad rangkaian dapat dipantau. Projek ini sepatutnya mampu untuk memantau, membuka dan menyimpan fail transit ke atas rangkaian. Projek ini hanya mampu memantau beberapa jenis protokol sahaja iaitu FTP, ICMP dan HTTP. Tujuan utama projek ini dibangunkan adalah untuk mengekstrak data paket dalam rangkaian dalam masa yang sebenar dan menganalisa protokol menggunakan oleh data sekaligus dapat menjadi sebuah platform untuk penyelidikan dan penambahan ciri alat pengurusan pada masa akan datang seperti penggunaan perlombongan data. Perisian ini boleh digunakan di dalam komputer peribadi untuk memantau paket yang melalui rangkaian. Rekabentuk antaramuka yang berunsurkan mesra pengguna direka supaya pengguna lebih mudah memahami cara penggunaan perisian. Jpcap telah dipilih untuk menangkap paket dan membuat sistem ini dapat berjalan dengan lancar.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

ABBREVIATIONS

ABBREVIATION	DESCRIPTION
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
ICMP	Internet Control Message Protocol
FTP	File Transfer Protocol
HTTP	Hypertext Transfer Protocol
SNMP	Simple Network Management Protocol
IDS/IPS	Intrusion Detection System/ Intrusion Prevention System
IPv4	Internet Protocol Version 4
ARP/RARP	Address Resolution Protocol/ Reverse Address Resolution Protocol

LIST OF ATTACHMENTS

CHAPTER I

INTRODUCTION

1.1 Project background

Accommodate to the networking system has been spread very quickly, so the packet extractor is develop as a tool to confine the data and try to evaluate and extract as details as possible of any data go through the network. It used to supervise the data travelling between computers on the network. As the function of packet extractor to extract the data, these tools will try to examine the activities happen on the network cable.

Packet extractor is an application for analyzing and monitoring every single packet or data that passes through the network link. They will read and process the packet that travel through the network by extract all the information carries like the packet header, type of protocol (TCP, UDP, ICMP and etc), source and destination address and many more. Network manager primarily used the packet analyzers tool to diagnose problems or understand the set of protocols that contribute to traffic on a network (Formoso, V. *et al.* ,2007).

1.2 Problem statement

When discussed the technology that involve in computer network, it turns to the packet. Packet used for the reliability and improve the performance on communication between two network devices. Each message is frequently divided into packets by the fundamental software and hardware.

Like human when they want to talk and exchange information but both using different dialects and language, they need to use the standard language to create the communication. In computing, computer converse on network by using protocols which are standardized all over the world that allow computers to understand each other. But it becomes problem when conversations between computer generally appear as random binary data. The packet extractor is needed to decode the network traffic, classify the protocol using and carry out many further interesting functions.

As there are a few tools have been develop and used to analyze packet like wiresharks, tcpdump and many more, these packet extractor software is been develop to use and understand how the packet is travel through the network. These tools also as platform to make sure that any extra features can be added in the future to make this software more efficient and practical to use.

In conclusion, there are a few problem statement has been figure out.

i. How to examine what protocol of data is carrier
ii. What are the packet activities behind the data on the network
iii. How to monitor user in email communications, ftp upload or download, internet access and other transaction to impose the company policies

1.3 Objective

The objectives that we want to achieve are:

i. to study the types of packet extractor available in current market and compared the characteristic of each tools
ii. to develop a packet capturing tools (packet extractor)
iii. to extract data packet on the network in the real time and analyze the protocol using by the data
iv. to provide a platform for further network management tools research on data mining purpose

1.4 Scope

This project is to develop an application that can be used as management tools. This packet extractor tools only develop for packet capturing and filtering purpose. There is a list of scope of this project:

i. User

There is the list of user scope which is cover on this packet extractor:

a. This software will cover on the control environment which is private network only.
b. This software covers only a few protocols (FTP, HTTP, and ICMP).

ii. Software

There is the list of equipment that needs to be use to develop this packet extractor which is:

a. Eclipse Software version 3.4.1
b. JDK 1.6.0
c. Jpcap 0.7
d. Microsoft Office Word 2007
e. Microsoft Office Project 2007
f. Microsoft Office Visio 2003
g. VMware

iii. Hardware

There is the list of equipment that needs to be use to develop this packet extractor which is:

a. Processor Intel Core i5, 2.53GHz
b. Random Access Memory (RAM), 4.00 GB
c. Hard disk 197 GB
d. Operating System Windows 7 Ultimate
e. Network interface card *Fast Ethernet*
f. External Hard Disk, 200 GB

1.5 Project Significance

In future, this software is one step to extract and analyze packet that travel through the network. This software will extract the network packet in details that contain layer 2 and layer 3 of Open Systems Interconnection (OSI) networking suite. On these OSI networking suite, there are a few protocol that related to each layer. For layer 2 which is Data Link Layer, it provides the functional and procedural means to transfer data between network entities and to detect and possibly correct errors that may occur in the physical layer. There are a few protocols in layer 2 that defines the procedures for operating the communication links, frames packets and also detects and correct the error that packet transmit.

For the network layer which is located on layer 3 of OSI model, in this layer, it will determines how data are transferred between network devices and then routes packet according to unique network device addresses..On this layer, it also provides flow and congestion control to prevent network resources depletion.

1.6 Expected Output

The packet extractor can view and extract the packet in details that will be useful to analyze the packet on the network.

1.7 Conclusion

As the conclusion, this software is developing to create an easy way for user to control and analyze the packet in more details. The management tools will be explains in detail on in the next chapter includes the comparison between the current management tools.

CHAPTER II

LITERATURE REVIEW AND PROJECT METHADOLOGY

2.1 Introduction

The previous chapter has discussed all the problems occur on the network management. The expected output has been decided as the outcomes from these tools. That chapter also explained the objectives as well as the scope pertain to the related research to develop new application tools a part of the network management tools.

On this chapter, the types of management tool will be explained which related to packet extractor. Here, also discuss the differences between a few existing tools that provide the same function to analyze packet which common used to manage network. The major function that concerned on this literature review is the tools that capable to analyze and extract packet to get the information details on the packet. This chapter also will provide the methodology used to develop the packet extractor. The development process of these software will be based on the timeline that been planned.

2.2 Facts and Findings

Nowadays, network evolution has growth so rapidly whether in wired or wireless technology. According to Lisa (2012), a suite of monitoring and maintenance tools is the primary method used for managing the network by network manager. Network management is necessary for all types of networks. Network manager uses network management which is an important aspect includes a set of tools, protocols, and frameworks as a way to monitor and maintaining and all networks components. Availability is the one of the most important aspect of network management. Users expect that network to be available for every second. This demand by users makes network management being crucial. It is required to understand the syntax and the semantics within each management system in order to develop one management system, with one language interpreter. Packet extractor is one of the network management tools developed to monitor the network by capture and analyze the entire packet traverse on the network.

Here are some types of network management tools. Network management tools can be categories into a few subcategories according to their general purpose as below:

i. Network Discovery
ii. Packet Analysis
iii. Flow Analysis
iv. Event Monitoring