BORANG PENGESAHAN STATUS TESIS

JUDUL: Application Access Monitoring System

SESJI PENGAJIAN: 2006/2007

Saya Norshida Bt Abd Malek mengaku membenarkan tesis PSM ini disimpan di Perpustakaan Fakulti Teknologi Maklumat dan Komunikasi dengan syarat-syarat kegunaan seperti berikut:

1. Tesis dan projek adalah hak milik Kolej Universiti Teknologi Kebangsaan Malaysia.
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

TERHAD

TIDAK TERHAD

(Mengandungi maklumat yang berdarjah keselamatan atau kepentingan Malaysia seperti yang termaktub di dalam AKTA RAHSIA RASMI 1972)

(Mengandungi maklumat TERHAD yang telah ditentukan oleh organisasi/badan dimana penyelidikan dijalankan)

(TANDATANGAN PENULIS)

(TANDATANGAN PENYELIA)

Alamat Tetap : No 114, Jalan TSS
4, Taman Sri Siantan, 28700 Bentong, Pahang Darul Makmur.

Tarikh : 17/11/2006

Nama Penyelia : En. Shekh Faisal B Abdul Latip

Tandatangan

Tarikh : 17/11/2006

CATATAN: **Jika tesis ini SULIT atau TERHAD, sila lampirkan surat daripada pihak berkauasa.

^Tesis dimaksudkan sebagai Laporan Projek Sarjana Muda (PSM)
APPLICATION ACCESS MONITORING SYSTEM

NORSHIDA BT ABD MALEK

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

FACULTY OF INFORMATION AND COMMUNICATION TECHNOLOGY
KOLEJ UNIVERSITI TEKNIKAL KEBANGSAAN MALAYSIA
2006
DECLARATION

I hereby declare that this project report entitled
APPLICATION ACCESS MONITORING SYSTEM

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

(NORSHIDA BT ABD MALEK)

(EN. SHEKH FAISAL ABDUL LATIP)
DEDICATION

“To my beloved parents, families, KUTKM lecturers and all my friends”
ACKNOWLEDGEMENTS

Alhamdulillah and thanks to Allah, for giving me the opportunity to finish up my PSM project successfully. I would like to express my deepest thanks and appreciation to my faculty supervisor, Mr. Shekh Faisal B Abdul Latip for his supervision, invaluable guidance, unfailing help, advice, suggestion, ideas, constructive criticism and supportive throughout the PSM.

My sincere thanks towards KUTKM Computer Centre Assistant Manager, Mr. Wan Imrul Nazimi Nordin, who has been very understandable provided me with the information's I want. Thanks also for their kindness and willingness to teach and guide me will be remembered. Last but not least, all the persons involved during the completion of this paperwork directly or indirectly.

Finally, to all my family members and friends that have given me moral support and motivation, a million thanks. Without all of them that I have mentioned, I will not be able to undergo my PSM project and the report successfully and meaningfully. All the experiences and knowledge that I have gained are their efforts and time spent.
ABSTRACT

Generally, Application Access Monitoring System is a system that detects user's activities. This system is implemented in Local Area Network (LAN) environment. The goal of this system is to help system administrators to view the users activities in real-time. Besides, activities that tracked will automatically save for later retrieval. The Application Access Monitoring System also displaying the server running process. The Application Access Monitoring System can be grouped into few stages; Analysis, Design, Implementation and Testing. In Analysis phase, a methodology was used because its deliverables of every stage matches the project milestones requirements. In the Implementation Phase the development of data, processes and interfaces of the system is started. To develop this system the VB6 language had been choose. While in testing phase, the Application Access Monitoring System is test in order to ensure that the system meets all the requirements. Lastly, for the conclusion this system strength and weaknesses are state for further studied.
ABSTRAK

# TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>CHAPTER</th>
<th>SUBJECT</th>
<th>PAGE</th>
</tr>
</thead>
<tbody>
<tr>
<td>DECLARATION</td>
<td></td>
<td>ii</td>
</tr>
<tr>
<td>DEDICATION</td>
<td></td>
<td>iii</td>
</tr>
<tr>
<td>ACKNOWLEDGEMENT</td>
<td></td>
<td>iv</td>
</tr>
<tr>
<td>ABSTRACT</td>
<td></td>
<td>v</td>
</tr>
<tr>
<td>ABSTRAK</td>
<td></td>
<td>vi</td>
</tr>
<tr>
<td>TABLE OF CONTENTS</td>
<td></td>
<td>vii</td>
</tr>
<tr>
<td>LIST OF TABLES</td>
<td></td>
<td>xi</td>
</tr>
<tr>
<td>LIST OF FIGURES</td>
<td></td>
<td>xii</td>
</tr>
<tr>
<td>LIST OF TERMS AND ABBREVIATIONS</td>
<td></td>
<td>xv</td>
</tr>
<tr>
<td>LIST OF APPENDIX</td>
<td></td>
<td>xvi</td>
</tr>
</tbody>
</table>

## CHAPTER I

**INTRODUCTION**

1.1 Project Background  
1.2 Problem Statements  
1.3 Objective  
1.4 Scopes  
1.5 Project Significance  
1.6 Expected Output  
1.7 Conclusion  

## CHAPTER II

**LITERATURE REVIEW AND PROJECT**
CHAPTER III  ANALYSIS

3.1 Introduction  24
3.2 Problem Analysis  24
3.3 Requirement Analysis  25
  3.3.1 Login Function Requirement  26
    3.3.1.1 Administrator Login  26
  3.3.2 Add, Delete, Edit and Save
    Function Requirement  26
    3.3.2.1 PCs Account Database  26
    3.3.2.2 Administration database  26
  3.3.3 Software Requirements  27
    3.3.3.1 Windows platform  27
    3.3.3.2 Microsoft Visual Basic 6.0  27
    3.3.3.3 Microsoft Access 2003  27
  3.3.4 Hardware Requirement  28
    3.3.4.1 Personal Computer  28
  3.3.5 Network Requirements  28
  3.4 Conclusion  29

CHAPTER IV  DESIGN

4.1 Introduction  30
4.2 High-Level Design  30
6.4.1 Test Description 71
6.4.2 Test Data 72
6.5 Test Result And Analysis 72
6.6 Conclusion 81

CHAPTER VII PROJECT CONCLUSION
7.1 Introduction 82
  7.1.1 Strength 82
  7.1.2 Weaknesses 83
7.2 Proposition for Improvement 83
7.3 Contribution 84
7.4 Conclusion 85

REFERENCES 86
BIBLIOGRAPHY 88
APPENDIX 90

APPENDIX A 91
APPENDIX B 93
APPENDIX C 99
APPENDIX D 100
APPENDIX E 102
# LIST OF TABLE

<table>
<thead>
<tr>
<th>TABLE</th>
<th>TITLE</th>
<th>PAGE</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.1</td>
<td>Application Access Monitoring System Milestone</td>
<td>22</td>
</tr>
<tr>
<td>3.1</td>
<td>Hardware Requirement Specifications</td>
<td>28</td>
</tr>
<tr>
<td>4.1</td>
<td>Application Access Monitoring System Input Design</td>
<td>35</td>
</tr>
<tr>
<td>4.2</td>
<td>Login Input/Output specification</td>
<td>36</td>
</tr>
<tr>
<td>4.3</td>
<td>System Menu Input/Output specification</td>
<td>36</td>
</tr>
<tr>
<td>4.4</td>
<td>Type of searching input/output specification</td>
<td>37</td>
</tr>
<tr>
<td>4.5</td>
<td>Track Activities input/output specification</td>
<td>37</td>
</tr>
<tr>
<td>4.6</td>
<td>Process Running input/output specification</td>
<td>37</td>
</tr>
<tr>
<td>4.7</td>
<td>Data Dictionary for Application Access Monitoring System</td>
<td>40</td>
</tr>
<tr>
<td>5.0</td>
<td>Lists of hardware used in the project</td>
<td>60</td>
</tr>
<tr>
<td>5.1</td>
<td>Lists of software used in the project</td>
<td>61</td>
</tr>
<tr>
<td>5.2</td>
<td>Application Access Monitoring System progress</td>
<td>63</td>
</tr>
<tr>
<td>5.3</td>
<td>Application Access Monitoring System Implementation Status</td>
<td>64</td>
</tr>
<tr>
<td>6.0</td>
<td>Test Schedule</td>
<td>68</td>
</tr>
<tr>
<td>6.1</td>
<td>Application Access Monitoring System Function/GUI Test Case Result</td>
<td>73</td>
</tr>
</tbody>
</table>
# LIST OF FIGURE

<table>
<thead>
<tr>
<th>FIGURE</th>
<th>TITLE</th>
<th>PAGE</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.1</td>
<td>Example of output from <em>PsGetSid</em> and <em>PsInfo</em> command</td>
<td>6</td>
</tr>
<tr>
<td>2.2</td>
<td>Example of applications that running in computer B0303010174</td>
<td>9</td>
</tr>
<tr>
<td>2.3</td>
<td>Example of foreground of computer B0303010174</td>
<td>9</td>
</tr>
<tr>
<td>2.4</td>
<td>Example of Windows Task Manager</td>
<td>10</td>
</tr>
<tr>
<td>2.5</td>
<td>Example of application log from Event Viewer window</td>
<td>12</td>
</tr>
<tr>
<td>2.6</td>
<td>Log Viewer</td>
<td>13</td>
</tr>
<tr>
<td>4.1</td>
<td>System Architecture for Application Access Monitoring System</td>
<td>31</td>
</tr>
<tr>
<td>4.2</td>
<td>Login interface for the Administrator</td>
<td>32</td>
</tr>
<tr>
<td>4.3</td>
<td>Running Process Interface for Administrator</td>
<td>33</td>
</tr>
<tr>
<td>4.4</td>
<td>Navigation Design of Application Access Monitoring System</td>
<td>34</td>
</tr>
<tr>
<td>4.5</td>
<td>ERD of Application Access Monitoring System</td>
<td>38</td>
</tr>
<tr>
<td>4.6</td>
<td>Context Diagram for Application Access Monitoring Systems</td>
<td>41</td>
</tr>
<tr>
<td>4.7</td>
<td>A Level 0 DFD for an Application Access Monitoring System</td>
<td>42</td>
</tr>
<tr>
<td>4.8</td>
<td>A Level 1 DFD for an Application Access Monitoring System, Registration</td>
<td>43</td>
</tr>
<tr>
<td>4.9</td>
<td>A Level 1 DFD for an Application Access Monitoring System</td>
<td>43</td>
</tr>
</tbody>
</table>
4.10 A Level 1 DFD for an Application Access Monitoring System, Authenticate User

4.11 A Level 1 DFD for an Application Access Monitoring System, Track Users Activities

4.12 Registration process flowchart

4.13 Login process flowchart

4.14 Track User Activity process flowchart

4.15 Administrator login interface

4.16 Main Menu Interface

4.17 Admin Registration Interface

4.18 Process Running Interface

4.19 Select Column Interface

4.20 Track Application access by users’ interfaces

4.21 List of User Status Interface

4.22 The admin table

4.23 PC_Info table

5.0 The Application Access Monitoring System client-server architecture.

5.1 Create a new project of the Application Access Monitoring System application.

6.0 Application Access Monitoring System Test Design

6.1 Error Message when login failed

6.2 Track Activities windows

6.3 Track Activities log

6.4 No Activities tracked

6.5 Running Process windows.

6.6 Successfully saved in Ms Excel

6.7 Successfully saved in process_server.txt

6.8 Data send to printer

6.9 Ready to print
6.10  
Select column to be displayed in process running listview

6.11  
Client Status Interface

6.12  
Message box shows that the new admin had been registered successfully.

6.13  
Message box shows that the new admin data had been found.

6.14  
Ask either sure to delete the selected data

6.15  
Selected data was successfully deleted.
# LIST OF TERMS AND ABBREVIATIONS

<table>
<thead>
<tr>
<th>ABBREVIATIONS</th>
<th>DEFINITION</th>
</tr>
</thead>
<tbody>
<tr>
<td>AUT</td>
<td>Application Under Testing</td>
</tr>
<tr>
<td>C/S</td>
<td>Client/Server</td>
</tr>
<tr>
<td>GUI</td>
<td>Graphical User Interface</td>
</tr>
<tr>
<td>LAN</td>
<td>Local Area Network</td>
</tr>
<tr>
<td>OS</td>
<td>Operating System</td>
</tr>
<tr>
<td>PC</td>
<td>Personal Computer</td>
</tr>
<tr>
<td>PSM I</td>
<td>Bachelor Degree Project I</td>
</tr>
<tr>
<td>PSM II</td>
<td>Bachelor Degree Project II</td>
</tr>
<tr>
<td>WinSock</td>
<td>Windows Socket</td>
</tr>
</tbody>
</table>
## LIST OF APPENDIX

<table>
<thead>
<tr>
<th>APPENDIX</th>
<th>TITLE</th>
<th>PAGE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Appendix A</td>
<td>Gantt chart Application Access Monitoring System</td>
<td>91</td>
</tr>
<tr>
<td>Appendix B</td>
<td>Application Access Monitoring System Test Script</td>
<td>93</td>
</tr>
<tr>
<td>Appendix C</td>
<td>Application Access Monitoring System Test Data</td>
<td>99</td>
</tr>
<tr>
<td>Appendix D</td>
<td>The Test Cases Output Result</td>
<td>100</td>
</tr>
<tr>
<td>Appendix E</td>
<td>User Manual for Application Access Monitoring System</td>
<td>102</td>
</tr>
</tbody>
</table>
CHAPTER I

INTRODUCTION

1.1 Project Background

Application Access Monitoring System is an application that detects the activities doing by users on Windows platform based on date and time accessing applications in a Local Area Network (LAN). This is one of the effectiveness monitoring system that can be used by the system administrator. This system can monitor all computers in LAN remotely from a single administrator’s PC. This helps the system administrator to keep an eye on users activities.

This system will track date and time for every single activities that users are doing. Application Access Monitoring System capture windows that is active together with the time. Firstly, install the Application Access Monitoring System at server and client PCs. Then, assign static IP Address to the server and all the clients. Then, start runs both application at server and clients. All the application users’ access together with date and time will be kept automatically in log file for administrators to view anytime they want.
1.2 Problem statement

To the best of my knowledge, there are many current systems that can track the users’ activities, the date, time and duration of time accessing an application. Here, there is one system known as Spy Lantern Keylogger that has been studied in order to take the ideas in implementing the new system. Spy Lantern Keylogger is a standalone system. It can detect all the users’ activities only in that PC. It is not suitable for remote monitoring activities.

In the Application Access Monitoring System, the administrator can capture activities not only in that PC, but also remote PCs which have been installed with the Application Access Monitoring System agent. This system is client server architecture. The system administrator can view activities doing by clients in one single PC.

1.3 Objective

- Develop the Application Access Monitoring System using Visual Basic.
- To track the application access, date access and time access based on PC IP Address that had been assigned manually.
- To log the users activities automatically.

1.4 Scopes

The Application Access Monitoring System can only running on Windows platform. The server agent PCs and the client agent PC will be running Windows XP Professional.
There are two users’ levels; administrators and users. The administrator is responsible to manage the Administrator database, the PC Account database and Statistic database. The system administrator can edit the databases; create, add, delete, view, save and search records. Another user are clients/users itself which is using the PC installed with the client agent of Application Access Monitoring System.

This system can only trace date and time accessing applications.

1.5 Project significance

The Application Access Monitoring System has several significances. Firstly, we can determine applications that access by user frequently. The most important is, this is a remote monitoring activity application and track activities based on IP Address.

1.6 Expected Output

Application Access Monitoring System is a system used by the system administrators to monitor the users activities based on application access, date access, and time access. This system also has disadvantages where the system will be running only in Windows platform. Both the agent PCs and system administrator PC will be installed with the Windows XP.
1.7 Conclusion

This chapter discussed on the Application Access Monitoring System background. This system is implemented due to problem to track the date, time, and total time spent on applications users' access. This system will be running on Windows platform. This system is suitable for administrator to keep track on the users' activities in LAN environments.

Next chapter, chapter II, will be discussing on the Literature Review and Project Methodology. Examples of case studies and journal will be provided. Project methodology will be focusing on steps of system development from the beginning till the system is finished. Projects requirements will be defined and Gantt chart will be developed to monitor the project planning and schedule.
CHAPTER II

LITERATURE REVIEW AND PROJECT METHODOLOGY

2.1 Introduction

In this chapter, we will review about the current systems in order to understand the way to develop Application Access Monitoring System. The current systems are studied to give clear understanding on how the system is functioning. The basic ideas of the system that will be implemented also being gathered to develop a good system.

2.2 Fact and finding

2.2.1 Study of the current system.

To implement the Application Access Monitoring System, a few similar systems had been studied. The first system is PsTools. PsTools is a set of command line utilities that allow administrator to manage local and remote systems. All of the utilities in the PsTools suite work on Windows NT, Windows 2000, Windows XP and Windows Server 2003. This application, doesn't even need to install any client software on the remote computers at which administrator target. Run them by typing their name and any command-line options administrator want. The feebleness of this program is, the administrator needs to familiar with the command line system in order to use this
application. Besides, administrator need to know the target client name/IP Address to start monitor their activities.

Below are the commands to view the client’s activities:

1. **PsExec** – execute processes remotely
2. **PsFile** – shows files opened remotely
3. **PsGetSid** – display the SID of a computer or a user
4. **PsInfo** – list information about a system
5. **PsKill** – kill processes by name or process ID
6. **PsList** – list detailed information about processes
7. **PsLoggedOn** – see who’s logged on locally and via resources sharing
8. **PsLogList** – dump event log records
9. **PsPasswd** – changed account passwords
10. **PsService** – view and control services
11. **PsShutDown** – shuts down and optionally reboots a computer
12. **PsSuspend** – suspend and resume processes

![Example of output from PsGetSid and PsInfo command](image)
Next similar application that studied is Kaseya. Kaseya is perfect for IT Administrators and Managed Service Providers who are interested in reducing complexity, increasing productivity, augmenting and expanding service offerings while increasing customer satisfaction and maximizing ROI. Kaseya has many functions which are:

1) **Inventory/audit** – Kaseya Computer Audit and Discovery provides automatic audits of your servers, workstations and remote computers. Flexible scheduling provides the administrator with full control to completely automate the computer audit function.

2) **Patch Management** – Kaseya Patch Management provides automatic discovery of all missing patches and updates. Flexible scheduling provides the administrator with full control to completely automate the patch scan function.

3) **Remote Desktop Management** – Kaseya Remote Desktop Management provides the tools needed for secure remote access to managed computers. Complete configuration of the remote control function is available to the administrator. Passwords, notification method, screen mode and control level. In addition, end users can optionally block remote control on their computers.

4) **LAN and Computer Monitoring** – Kaseya LAN and Computer Monitoring give IT professionals the ability to know what is going on with their networks. With little effort and minimal time, you can proactively monitor servers, workstations, remote computers, Windows Event Logs and applications.

5) **Help Desk and Trouble Ticketing** – Kaseya Help Desk and Trouble Ticketing assists IT professionals to manage user expectations and keep a history of all issues and resolutions.

6) **Software Deployment** – Kaseya Software Deployment provides the flexibility and reliability needed to deploy applications and updates automatically.

7) **Backup and Disaster Recovery** – provides real-time automated disk backup, disk imaging, file level backup and bare-metal restore for Windows servers and workstations.