

BORANG PENGESAHAN STATUS TESIS^**JUDUL: Application Access Monitoring System****SESI 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 hakmilik 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	(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 dimana penyelidikan dijalankan)
_____	TIDAK TERHAD	



(TANDATANGAN PENULIS)



(TANDATANGAN PENYELIA)

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

Nama Penyelia : En. Shekh Faisal B
Abdul Latip

Tarikh : 17/11/2006

Tarikh : 17/11/2006.

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

^Tesis dimaksudkan sebagai Laporan Projek Sarjana Muda (PSM)

raf

TK5105.7 .N67 2006



0000038923

Application access monitoring system / Norshida Abd
Malek.

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.

STUDENT

:  DATE: 17/11/2006
(NORSHIDA BT ABD MALEK)

SUPERVISOR

:  DATE: 17/11/2006
(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

Secara umumnya, Sistem Pemantauan Capaian Aplikasi adalah satu sistem yang mana dapat mengesan aktiviti yang dilakukan oleh pengguna. Sistem ini digunakan di dalam Rangkaian Komputer Setempat (LAN). Tujuan utama Sistem Pemantauan Capaian Aplikasi ini adalah untuk membantu pihak pentadbir sistem memantau aktiviti yang telah dan sedang diakses oleh pengguna. Selain itu, aktiviti yang dikesan akan disimpan secara automatik bagi tujuan rujukan pada masa hadapan. Sistem Pemantauan Capaian Aplikasi ini turut memaparkan proses yang sedang berjalan pada server tersebut. Sistem Pemantauan Capaian Aplikasi ini boleh dibahagikan kepada beberapa peringkat iaitu, Analisa, Rekaan, Perlaksanaan dan Pengujian. Di dalam fasa analisa, satu jenis metodologi telah diguna pakai kerana ianya bersesuaian dengan jadual perjalanan sistem ini. Di dalam fasa Perlaksanaan pula, pembangunan data, antaramuka dan proses bermula. Untuk membangunkan sistem ini, VB6 telah dipilih sebagai bahasa pengaturcaraan. Dalam fasa Pengujian, Sistem Pemantauan Capaian Aplikasi ini telah diuji bagi memastikan ianya memenuhi kehendak yang telah ditetapkan. Akhir sekali, di dalam fasa kesimpulan, kekuatan dan kelemahan sistem ini dipaparkan bagi rujukan di masa hadapan.

TABLE OF CONTENTS

CHAPTER	SUBJECT	PAGE
	DECLARATION	ii
	DEDICATION	iii
	ACKNOWLEDGEMENT	iv
	ABSTRACT	v
	ABSTRAK	vi
	TABLE OF CONTENTS	vii
	LIST OF TABLES	xi
	LIST OF FIGURES	xii
	LIST OF TERMS AND ABBREVIATIONS	xv
	LIST OF APPENDIX	xvi
CHAPTER I	INTRODUCTION	
	1.1 Project Background	1
	1.2 Problem Statements	2
	1.3 Objective	2
	1.4 Scopes	2
	1.5 Project Significance	3
	1.6 Expected Output	3
	1.7 Conclusion	4
CHAPTER II	LITERATURE REVIEW AND PROJECT	

	METHODOLOGY	
	2.1 Introduction	5
	2.2 Fact and Finding	5
	2.3 Project Methodology	19
	2.4 Project Requirements	21
	2.4.1 Software Requirement	21
	2.4.2 Hardware Requirement	21
	2.4.3 Other Requirement	22
	2.5 Project Schedule and Milestone	22
	2.6 Conclusion	23
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

4.2.1 System Architecture	31
4.2.2 User Interface Design	32
4.2.2.1 Administrator Login Interface	32
4.2.2.2 Running Process Interface	33
4.2.2.3 Navigation Design	34
4.2.2.4 Input Design	35
4.2.2.5 Output Design	36
4.2.3 Database Design	38
4.2.3.1 Conceptual and Logical Database Design	38
4.3 Details Design	41
4.3.1 Software Specification	41
4.3.2 Physical Database Design	55
4.4 Conclusion	57
CHAPTER V	IMPLEMENTATION
5.1 Introduction	58
5.2 Software Development Management	59
5.3 Software Configuration Management	61
5.3.1 Configuration Environment Setup	61
5.3.2 Version Control Procedure	62
5.4 Implementation Status	63
5.5 Conclusion	65
CHAPTER VI	TESTING
6.1 Introduction	66
6.2 Test Plan	66
6.2.1 Test Organization	67
6.2.2 Test Environment	67
6.2.3 Test Schedule	68
6.3 Test Strategy	68
6.3.1 Classes of Test	70
6.4 Test Design	70

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

LIST OF FIGURE

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

	System, Login	
4.10	A Level 1 DFD for an Application Access Monitoring System, Authenticate User	44
4.11	A Level 1 DFD for an Application Access Monitoring System, Track Users Activities	45
4.12	Registration process flowchart	47
4.13	Login process flowchart	48
4.14	Track User Activity process flowchart	49
4.15	Administrator login interface	50
4.16	Main Menu Interface	51
4.17	Admin Registration Interface	52
4.18	Process Running Interface	53
4.19	Select Column Interface	54
4.20	Track Application access by users' interfaces	54
4.21	List of User Status Interface	55
4.22	The admin table	56
4.23	PC_Info table	56
5.0	The Application Access Monitoring System client-server architecture.	60
5.1	Create a new project of the Application Access Monitoring System application.	62
6.0	Application Access Monitoring System Test Design	71
6.1	Error Message when login failed	73
6.2	Track Activities windows	74
6.3	Track Activities log	74
6.4	No Activities tracked	75
6.5	Running Process windows.	76
6.6	Successfully saved in Ms Excel	76
6.7	Successfully saved in process_server.txt	77
6.8	Data send to printer	77
6.9	Ready to print	77

6.10	Select column to be displayed in process running listview	78
6.11	Client Status Interface	79
6.12	Message box shows that the new admin had been registered successfully.	79
6.13	Message box shows that the new admin data had been found.	80
6.14	Ask either sure to delete the selected data	80
6.15	Selected data was successfully deleted.	80

LIST OF TERMS AND ABBREVIATIONS

ABBREVIATIONS	DEFINITION
AUT	Application Under Testing
C/S	Client/Server
GUI	Graphical User Interface
LAN	Local Area Network
OS	Operating System
PC	Personal Computer
PSM I	Bachelor Degree Project I
PSM II	Bachelor Degree Project II
WinSock	Windows Socket

LIST OF APPENDIX

APPENDIX	TITLE	PAGE
Appendix A:	Gantt chart Application Access Monitoring System	91
Appendix B:	Application Access Monitoring System Test Script	93
Appendix C:	Application Access Monitoring System Test Data	99
Appendix D	The Test Cases Output Result	100
Appendix E	User Manual for Application Access Monitoring System	102

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

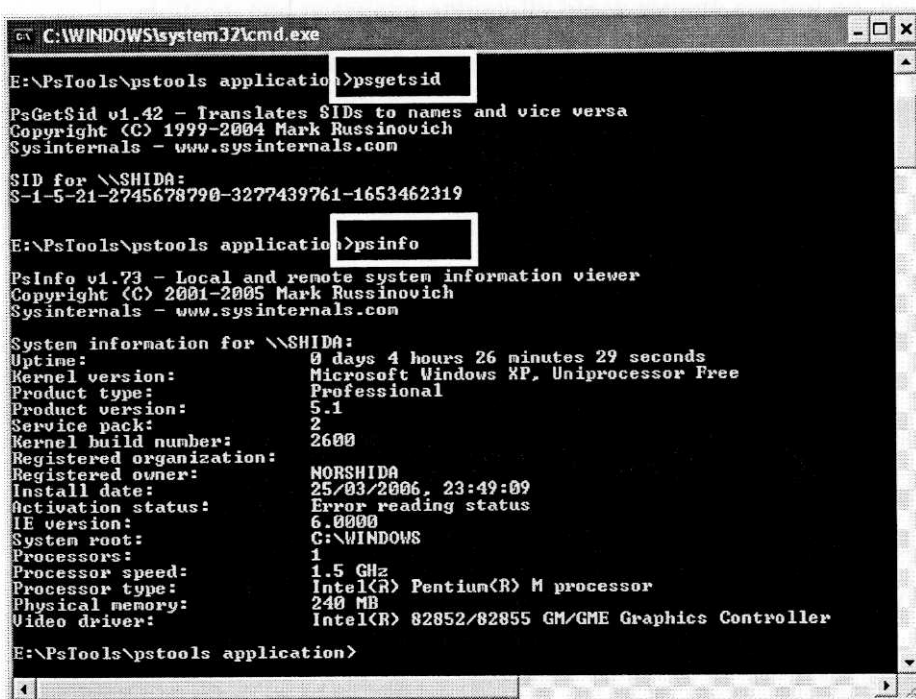
2.2.1 Study of the current system.

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



```

C:\WINDOWS\system32\cmd.exe
E:\PsTools\pstools application>psgetsid
PsGetSid v1.42 - Translates SIDs to names and vice versa
Copyright (C) 1999-2004 Mark Russinovich
Sysinternals - www.sysinternals.com

SID for \\SHIDA:
S-1-5-21-2745678790-3277439761-1653462319

E:\PsTools\pstools application>psinfo
PsInfo v1.73 - Local and remote system information viewer
Copyright (C) 2001-2005 Mark Russinovich
Sysinternals - www.sysinternals.com

System information for \\SHIDA:
Uptime:                0 days 4 hours 26 minutes 29 seconds
Kernel version:        Microsoft Windows XP, Uniprocessor Free
Product type:           Professional
Product version:        5.1
Service pack:           2
Kernel build number:    2600
Registered organization:  NORSHIDA
Registered owner:
Install date:           25/03/2006, 23:49:09
Activation status:      Error reading status
IE version:             6.0000
System root:            C:\WINDOWS
Processors:             1
Processor speed:        1.5 GHz
Processor type:         Intel(R) Pentium(R) M processor
Physical memory:        240 MB
Video driver:           Intel(R) 82852/82855 GM/GME Graphics Controller

E:\PsTools\pstools application>

```

Figure 2.1: Example of output from *PsGetSid* and *PsInfo* command

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.