DESIGN AND IMPLEMENTATION OF NETWORK ACTIVITY MONITORING SYSYTEM.

(A CASE STUDY OF ANAMBRA STATE FEDRAL INLAND REVENUE SERVICES, F.I.R.S)

PRESENTED BY

OKOYE-EZENWA EMMANUEL .C.

CST/2009/348

CARITAS UNIVERSITY AMORJI-NIKE, ENUGU STATE

FACULTY OF NATURAL SCIENCES.

IN PARTIAL FULFILMENT OF THE REQUIREMENTS FOR THE AWARD OF BACHELORS OF SCIENCE DEGREE (B.Sc.) IN COMPUTER SCIENCE & INFORMATION TECHNOLOGY.

JULY 2013

CHAPTER ONE

INTRODUCTION

Attacks on computer by outside intruder are more publicized but the ones perpetrated by insiders are very common and often more damaging. Insiders represent the greatest threat to computer security because they understand their organization's business and how their computer systems work. They have both the confidentiality and access to perform these attacks. An inside attack will have a higher probability of successfully breaking into the system and extracting critical information. The insiders also represent the greatest challenge to securing the company network because they have authorized level of access to the file system.

In a quest for maximum profitability in a network, there is need to monitor the activities performed such that the network activity in a real time would be tracked, confidential information safeguarded and control over the daily activities of every staff established. The question is: which and how would one develop the so much needed system that would exhibit all these potentialities?

Network activity monitoring system is used to detect inside threats by monitoring file access and process activity (Behr et al, 2009). It is a powerful tool that allows one to track any local area network, giving you the most detailed information on when, how and what your network users do on daily basis. If it is a library public network, university or commercial organization network, Activity Monitor offers efficient control. This work targets the monitoring of every activity of a user in a computer network and maximizes the security for the organization or corporate body.

1.1 BACKGROUND OF STUDY

The Federal Inland Revenue service (FIRS) is one of the federal ministries charged with the responsibility of accessing, collecting, and accounting for the various taxes to the federal government since 1943.

Tax revenue has been reliable from time, from where government rely for decision making, and aids for development and administrative planning, hence the need for optimum human resource of the organisation or ministry; for it's considered to be their most valuable asset if properly harnessed and are well motivated to perform their assigned tasks so as to enhance the organisations goals and objectives.

Computer network activity monitoring system has become one of the vital tools in providing evidence in cases such as computer misuse and fraud. Computers and other devices are being used increasingly to commit, enable or support unwanted activity perpetrated against individuals, organizations or assets. Although it is most often associated with the investigation of a wide variety of computer crime, network activity monitoring system may also be used in civil proceedings. The discipline involves similar techniques and principles to data recoveryand a lot of information is retained on the computer than most people realize. It's also more difficult to completely remove information than it is generally thought. For these reasons (and many more), network activity monitoring system can often find evidence or even completely recover lost or deleted information, even if the information was intentionally deleted.

This system consist of two tier application – server and client whereby the activity monitoring server can be installed in any computer in the entire local area network and the client which is the remote spy software is installed on all the computers on the network to be monitored.

1.2 STATEMENT OF PROBLEM

The existing system used by FIRS has been a challenge to them. Amongst the problems affecting the FIRS from maintaining a steady reliable accounting figures and estimates are:-

- With the current system, staffs easily erase or add data in order to cover up their fraud since there is no back up of the activity log. Frauds like computer fraud: - loss or damage to money, securities resulting directly from the use of any computer to fraudulently cause a transfer of money or other property from inside the premises to a personat a place outside the premise.
- Their method of operation is not so efficient for both units in the department (Operations and Reconciliation units).Both units cannot work at the same time, and this is because the staffs in one of the unit (reconciliation unit) has to wait for the staffs in the other unit (operation unit) to get their work to some extent before they can process their own work, and while they are processing their own work, the staffs in the operation unit has to pause their work a little,and with this manual of operation in the department, rooms for corporate fraud is being created.

These are the more reasons, why the researcher embarked on this research.

1.3 OBJECTIVES OF STUDY

This project targets towards discovering what should be done to improve the existing system, monitoring the daily activities of every user in a network and using it to provide evidence to frauds or crimes committed using computer technology which some people referred to as digital crime; that is crime committed using a computer system.

The objective of this work is to develop a system that should be able to;

1. Monitor the daily activities of every user in a network in real time.
2. Detect active users.
3. Provide accurate evidence on corporate fraud when investigation is being carried out in an organization.
4. Has a good memory management for efficient carrying out of activities.

1.4 SIGNIFICANCE OF STUDY

This work was embarked upon for several reasons discussed below and again provides answers to some questions like:

- What is the value in adopting an investigation system?
- Why should you invest time and money on this?
- What are the benefits to organisations?

Therefore some of the significance and benefits of this work include:

- Increased employers loyalty: -What ultimately creates the employers loyalty is meeting and exceeding their expectation.
- Maintaining system integrity.
- Staying current on work status so as to know how well the organisation is going.
- Ensure proper handling of investigation in computing:This is the reason why we need a careful, methodical process for gathering digital data in the first place; and this is why we need network activity monitoring system.
- Increased employer’s retention:-The employees are an investment. Generally, it takes nine to twelve months or longer before an employee is a productive asset to a company. If an employee leaves after a year or two, the company has lost most of its investment.

- Information empowered decision making**:** -Most managers, executives and employers make decisions based upon all relevant information. There are some actions that can have a profound effect on corporate decision making; those actions are more easily justifiable when you have easily accessed the users system.

1.5 SCOPES OF THE STUDY

Although a network activity monitoring system involves many things and activities that can be run within it, yet due to lack of time and space, we were not able to use this software in other operating systems apart from windows operating system (that is from windows XP to windows operating system of higher versions). Furthermore this work did also not involve internet connectivity as well as detection of virus in a network.

1.6 LIMITATIONS OF THE STUDY

During the course of this study, many things militated against its completion, some of which are;

- Lack of finance
- Refusal of the Federal Inland Revenue Services Awka, to give detailed answers and in some cases no answer at all to some questions.
- This project is limited to all the data associated with the information gotten from the Federal Inland Revenue Service commission, and due to time factor, not all the commissions were reached for sources of data and information.

1.7 DEFINITION OF TERMS

- **NAMS (Network activity monitoring system):** This is the system that is used monitor the daily activity of every user on a network
- **Corporate fraud:** This is the fraud committed by insiders in a large, publicly traded (or private) corporation, and/or by senior executives.
- **Real time:** Occurring immediately, this is used for such task as navigation, in which the computer must react to a steady flow of new information without interruption.
- **LAN (local area network):** This is computer network that spans a relatively small area. Most LANs are confined to a single building or group of buildings.
- **Suid:** A file attributes which allows a program to run as a specific user no matter who executes it.
- **Corporate decision making:** This is connected with a corporation, this involves the image of a company or organization where all its members involve taking critical decision making (finance/planning/strategy)
- **Internal Auditor:** An employee of a company charged with providing independent and objective evaluations of the company's financial and operational business activities, including its corporate governance. Internal auditors also provide evaluations of operational efficiencies and will usually report to the highest level of management on how to improve the overall structure and practices of the company
- **External Auditor:** An external auditor is an audit professional who performs an audit in accordance with specific laws or rules on financial statements of a company, government entity, other legal entity or organization, and who is independent of the entity being audited.

CHAPTER TWO

LITERATURE REVIEW

2.0 COMPUTER NETWORK

A computer network can be defined as a grouping or interconnection of different computer on a single platform for information exchange among various nodes (clients) or independent functioning computers or workstations (Agbasi, 2012). In a technology context, network is usually short for "computer network" or "data network" and implies that computers are the things sharing the meaningful information. At a conceptual level, all data networks consist of nodes, which refer to any computer or digital device using the network and links, the physical connections that carry messages between nodes (Zhirkov, 2004).

Computer networks can also be said to be a collection of hardware components and computers interconnected by communication channels that allow sharing of resources and information. Where at least one process in one device is able to send/receive data to/from at least one process residing in a remote device, then the two devices are said to be in a network.Networks may be classified according to a wide variety of characteristics such as the medium used to transport the data, communications protocol used, and topology, their roles and responsibilities and geographical area.

2.1 MEDIUM USED TO TRANSPORT DATA

Transmission media is a medium through which data can be transmitted over a long distances. The speed or rate at which data is transmitted over a communication channel is denoted by a parameter called bandwidth. The various transmission media are two wire open lines, twisted pair, coaxial cable, optical fibres, and all the transmission media listed above uses guided media. It isalso possible to transmit information into free space, using a high frequency electromagnetic wave. Electromagnetic waves in the frequency range of 500MHz and above are known as microwaves. Some of the unguided transmission media (wireless) are Geo-stationary satellites, light-of-sight microwave, radio waves and infrared.

2.2 PROTOCOLS

Communications protocols define the rules and data formats for exchanging information in a computer network, and provide the basis for network programming. Well-known communications protocols are Ethernet, a hardware and link layer standard that is ubiquitous in local area networks, and the internet protocol suite, which defines a set of protocols for internetworking, i.e. for data communication between multiple networks, as well as host-to-host data transfer, and application-specific data transmission formats.

2.3 TOPOLOGY

Topology is geometrical arrangements of nodes. Nodesrefer to various computer resources and communication devices. The following are different classes of network based on the topological structure.

- Bus network: In a bus network, all nodes are connected to a single communication channel called bus. It is also referred as a time-shared bus.

- Star network: In a start network, each node is connected by means of a dedicated point-to-point channel to a central node called server that act as a switch.
- Ring network: Nodes in a ring network are connected in the form of a closed loop.
- Mesh network: In a mesh network, each pair of nodes is connected by means of an exclusive point-to-point link.
- Tree network: A tree network is another form of a bus. Several nodes are connected into a hierarchical form.

2.4 ROLES AND RESPONSIBILITIES OF COMPUTER NETWORK

Networks vary considerably in terms of the roles and responsibilities of the computers on that network and the relationships that tie those machines together. A computer totally disconnected from other devices is typically referred to as a stand-alone machine.

When several computers are interconnected, but no computer occupies a privileged position, the network is usually referred to as a **peer-to-peer network (**Balasubramanian et al, 2006**)**. In this type of network, every computer can communicate with all the other machines on the network, but in general each one stores its own files and runs its own applications.

With a **client-server network**, one or more servers will perform critical functions on behalf of the other machines (the clients) on the network (Aguboshim, 2008). These functions might include user authentication, data storage, and the running of large, shared, resource-intensive applications such as databases and client relationship management (CRM) software.

Typically, both peer-to-peer and client-server networks rely on a shared Internet connection for access to external resources of these basic network structures.

Another type of network that's been rapidly gaining in popularity over the past decade is the cloud-based network. In this model, an organization pays a third-party vendor to host data, applications and other resources on servers and manages those resources via a web browser. A cloud-dependent network can be simpler, cheaper, and greener than a client-server network since you aren't buying, maintaining and powering your own servers. However, it’s not necessarily the right solution for every organization, particularly those that handle and store sensitive client data or health records.

2.5 GEOGRAPHICAL AREA

Computer networks are classified according to their geographical area (Balasubramanian et al, 2006). They are:

Local area network (LAN): This is a network that connects computers and devices in a limited geographicalarea such as home, school, computer laboratory, office building, or closely positioned group of buildings. Each computer or device on the network is a node. Current wired LANs are most likely to be based on Ethernet technology, although new standards like ITU-TG.hn also provide a way to create a wired LAN using existing home wires (coaxial cables, phone lines and power lines).

Technically, this is the simplest type of computer network, they are widely used to connect personal computers and work stations in company offices and factories and to share both hardware and software resources. Examples of the resources shared are printers, scanners, laminators.

The defining characteristics of LANs, in contrast to WANs (Wide Area Networks), include their higher data transfer rates, smaller geographic range, and no need for leased telecommunication lines. Current Ethernet or other IEEE 802.3 LAN technologies operate at speeds up to 10gigabit/s. This is the data transfer rate. IEEE has projects investigating the standardization of 40 and 100gigabit/s. LANs can be connected to Wide area network by using routers.

Wide Area Network (WAN): WAN is a computer network that spans a large geographical area. It uses dedicated or switched connections to link computers in geographically remote locations wide area networks are implemented to connect large number of WANs and MANs. Due to this reason, it is possible to see a large number of heterogeneous components in a wide area network. Different communication media are used and the network spreads across several national boundaries. Computers connected to a WAN are often connected to a public network. They can also be connected through leased lines or satellite links. WAN is mostly used by government or large concerns because of the huge investment made to implement them.

Computer networks also enable resource sharing, an important consideration in all budget-conscious organizations. Rather than buying one printer for every employee and replacing them when they wear out, an organization with a network can buy a single printer, connect it to the network, and configure it in such a way that every computer user in the organization can print to it. The initial cost of a networked printer is usually more than the cost of a single desktop printer, but when considering costs on a per-user basis, the average cost of the networked printer is often much less than the cost of buying a printer for every employee. While some networked devices such as printers, scanners, and fax machines have predetermined, specialized functions, you can also network and share generic, unspecialized computing power in the form of servers.

Servers are large, powerful computers that can handle resource-intensive tasks more efficiently than desktop computers. As with the networked printer, the initial outlay for a server is more than that for a desktop computer, but across the organization, it's often cheaper to run the server-based version of a program since individual users won't need expensive, high-performance desktop and laptop computers. Servers can also deploy software to other networked machines at a lower cost

2.6 NETWORK MONITORING SYSTEM

Network monitoring system monitors an internal network for problem(s). It can find and help resolve snail placed webpage downloads, lost in space e-mail, questionable user activity and file delivery caused by overhead, crashed servers delay network connections or other devices.

Network monitoring systems are much different from intrusion detection systems, it let one knows how well the network is running the course of ordinary operation; its focus isn’t on security. Network monitoring can be achieved using various software or a combination of plugs and play hardware and software appliances solutions.

Virtually any kind of network can be monitored. It doesn’t matter whether it is wired or wireless, a corporate LAN, VPN or service providers WAN. One can monitor devices on different operating systems with multitude of functions, ranging from blackberries, cell phones, to servers, routers and switches. These systems can help identifies specific activities and performance matrices, producing results that enables business to address sundry needs, including meeting compliances requirement, stomping out internal security threats and providing operational visibility.

According to Winggin and Christopher (1998), a network monitoring systems comprises the following:

- A computer including processing means for executing a multi-tasking operating systems which is capable of running a plurality of user applications each of which being associated with an active or inactive window, with a user application provided by atleast one of a service and a server.
- A graphical user interface on the system running monitoring software.
- The network monitoring system should have a user prompting means for first time in the priority scheduling.
- A closing menu user application is associated to inactive window for a period greater than the predetermined scheduled time.
- The network monitoring systems should have identification (ID) means for generating an access request for user application and a termination request when an ID is invalid which is subject to license restriction.

2.6.1 NETWORK MONITORING SYSTEM WITH REFERENCE TO APPLICATION SERVER OR APPLICATION SERVER MONITORS (ASM).

(Agomuo&Nwachukwu, 2009) analysed the architecture of Network monitoring system with reference to application server or application server monitor, they describe the system as a desktop based application, developed to assist micro company in monitoring their application servers running on their network domain to decrease downtime cost, improve staff productivity, create flexible reporting of their application servers on their network and to focus on business core among others.

The authors embarked on this work to create a system that has the ability to monitor and identify the state of application servers, and report within the shortest possible time. A system that can monitor many servers concurrently by alerting appropriate person(s) when critical events occurs, and a system whose flexibility in reporting error or problem on the application server can not only be display on the screen but also by audio signals.

The control centre contains the operational environment with five main menu that is seen when you log in. these main menus are file, edit, monitor, log and help. The input to the system comes in two major ways: First, is the operator's registration. Here the user is required to fill in his/her information in the registration input specification form. The data supplied will be used to configure the individual access to the system, that is, user ID and password. The second is the application server configuration settings which are divided into two forms: request for HTTP server and request for TCP server configuration. The output can be displayed on the screen, printed or recorded. The recording aspect is because the system will have an alert mechanism which will inform unique sound which can easily be identified by the operator. In the output menu you have the name, activity and state. At the main interface, the operator wishes to perform some operations on the server he/she wants to monitor. These could be, start all the monitors, stop all monitors, add monitors, remove all monitor, actions.

This work, Network Monitoring System with Reference to application servers also called Application server monitor (ASM) is carried out to improve the monitoring system of organization that maybe using application servers. At the end of this work, they were able to develop a system that can integrate live data (application servers) on the network server which other systems can have access to, the application detects faults on either TCP server or HTTP server and alerts the operator by displaying the states of the server on the screen or by making three different sounds signifying various states of the server.

2.6.2 NETWORK MONITORING AND LAWFUL INTERCEPT (NETWORK TELEMETRY)

One of the application of Network telemetry is **Network Monitoring and Lawful- Intercept,** these are important to Service Providers and impose unique requirements on network equipment, which makes network telemetry to be the monitoring and reporting information on a network whether LAN or WAN. (www.brocade.com/downloads/whitepapers/Network.Telemetry). It helpsto provide a system that monitors their networks for security intrusion detection, application performance management, packet inspection and analysis. A wide range of other applications pointed two approaches of network architectures which a service provider can use to design a monitoring network: In-band network architecture and Out-of-band network architecture.

In-band network architecture: it is based on software that must be installed on the remote system being managed and only works after the operating system has been booted. This solution is cheaper, but it does not allow access to Bios settings or the reinstallation of the operating system and cannot be used to fix problems that prevent the system from booting.

Out-of-bound network architecture: This involves the use of a dedicated management channel for device maintenance. It allows a system administrator to monitor and manage servers and other network equipment by remote control regardless of whether the machine is powered on, or if an operating system is installed or functional.

2.6.3 NETWORK MONITORING AND DIAGNOSIS BASED ON AVAILABLE BANDWIDTH MEASUREMENT.

(Ningning, 2006) analysed the architecture of Network Monitoring and Diagnosis based on available bandwidth measurement. The researcher pointed out in his work that Network monitoring and diagnosis systems are used by

ISPs for daily network management operations and by popular network applications like peer-to-peer systems for performance optimization. However, the high overhead of some monitoring and diagnostic techniques can limit their applicability. Network monitoring and diagnosis system periodically records value of network performance metrics in order to measure network performance, identify performance anomalies, and determine root causes for the problems, preferably before customers' performance is affected.

The researcher went further to state that end-to-end available bandwidth and bandwidth bottlenecks can be efficiently and effectively estimated using packet-train probing techniques, source and sink tree structures that can capture network edge information, and with the support of a properly designed measurement infrastructure, bandwidth-related measurements can also be scalable and convenient enough to be used routinely by both ISPs and regular end users". These claims are supported by four techniques presented in his work, the (IGI/PTR) end-to-end available bandwidth measurement technique, the Pathneck bottleneck locating technique, the BRoute large-scale available bandwidth inference system, and the TAMI monitoring and diagnostic infrastructure. The IGI/PTR technique implements two available bandwidth measurement algorithms, estimating background traffic load (IGI) and packet transmission rate (PTR), respectively. It demonstrates that end-to-end available bandwidth can be measured both accurately and efficiently, thus solving the path-level available bandwidth monitoring problem.

The Pathneck technique uses a carefully constructedpacket train to locate bottleneck links, making it easier to diagnose available-bandwidth related problems. Pathneck only needs single-end control and is extremely light-weight. Those properties make it attractive for both regular network users and ISP network operators.

The BRoutesystem uses a novel concept source and sinks trees to capture end-user routing structures and network-edge bandwidth information.

Equipped with path-edge inference algorithms, BRoute can infer the available bandwidth of all N2 paths in an N-node system with only O (N) measurement overhead. That is, BRoute solves the system-level available-bandwidth monitoring problem. The TAMI measurement infrastructure introduces measurement scheduling and topology-aware capabilities to systematically support all the monitoring and diagnostic techniques that are proposed in this work. TAMI not only can support network monitoring and diagnosis, it also can effectively improve the performance of network applications like peer-to-peer systems.

At the end of this work the author was able to put forth that monitoring end-to-end available bandwidth and bandwidth bottlenecks on individual network paths can be efficiently and effectively estimated using packet-train probing techniques. Large-scale available bandwidth can be estimated efficiently by using the source and sink tree data structures to capture network edge information. Also with the support of a properly designed measurement infrastructure, bandwidth-related measurement techniques can be convenient enough to be used routinely by both ISPs and regular end users.

2.7 ACTIVITY LOG

The Activity Log reveals all changes that are made on networked computers. This is useful to show how active different forms are on a network and for tracking down the account history in case something seems off (Chapple, 2011). An activity log (also known as an Activity Diary or a Job Activity Log) is a written record of how a user spends his or her time (Chapple, 2011).

By keeping an activity log for a few days, one can build up an accurate picture of what he or she does during the day, and how he or she invests time. This will tell one whether the memory is quite a poor guide, and that keeping the log is an eye-opening experience.

Activity Logs helps one identify non-core activities that doesn’t help him or her meet important objectives. For example, one might spend far more time than he thinks surfing the Internet, or getting coffee each afternoon. When he sees how much time wasted on such activities, the author can then change the way that he works to eliminate them.

2.7.1 WHAT ACTIONS ARE LOGGED?

When an action is logged, the user who performed the action is stored along with the date, time, and IP address where necessary. Internal data about the type of action is also stored. For example, if a form is deleted, it will keep track of the form name. Below is a list of the types of actions that can be logged.

- **Form**: Almost everything on the Form Manager is a Form related activity. Creating, deleting and editing a form are common occurrences. In addition to these, it will let you know when a theme has been changed or a form has become inactive.
- **Entry**: It would serve little purpose to show a log of every entry created, but it is important to keep track of any edits or deletions made.
- **Report**: Similar to forms, the Report Manager controls the main activities here. In addition to creating, editing and deleting a report it can also keep track of toggle password protection and privacy.
- **Theme Activity**: Logging themes is fairly straightforward. In the Theme Designer you can create, edit, duplicate, change the name of, and delete themes. These are the things you can keep track of.
- **User Activity**: Stores a record every time a user log in or out of his or her account. It takes down the activity of every activity done by a user depending on the time-set of the software. It can store it with .jpg file

extension by taking the screenshot of the activities performed on the users system, or as a file which can still be able to run and save some underground files. There are still many other ways of taking records of user's activity but these depends on the technology used and the organization involve. The activity log of a user looks like this "Wed mar 28 10.16.04 WAT 2012.jpg", with the captured picture on top of it.

2.8 FILE ACTIVITY MONITORING

File Activity Monitoring (FAM) products are designed to plug a hole in existing Data Loss Prevention (DLP) products by monitoring access to the thousands of files enterprises have in their repositories (Chapple, 2011). There's a wealth of information stored on file servers, document management systems and other repositories up for grabs to the malicious insider with authorized access that is seeking to steal intellectual property. FAM products provide organizations with the ability to monitor the way insiders use sensitive information.

File activity monitoring products are designed to monitor the patterns of legitimate users accessing enterprise file stores and alert security administrators to unusual activity. FAM is designed to go above and beyond the access control and logging capabilities built-in to operating systems, providing a usable way to perform both proactive and reactive security monitoring.

FAM solutions could be used to:

- Track file access in real time and take action when abnormal activity is detected. The definition of "abnormal" may be customized to individual users, groups or the entire organization.
- Audit all accesses to a file in the event of a data leak to assist with the investigation.

- Identify all files accessed by a particular user who is suspected of corporate espionage.
- Identify users that have access permissions but are not using them. This may be especially helpful when performing audits designed to identify permissions that have accumulated as a result of privilege creep but are no longer necessary.

2.9 DETECTING INSIDER THREATS BY MONITORING SYSTEM CALL ACTIVITY.

(Kuenning et al, 2001) analysed the detection of inside threats by monitoring system call activities. In their paper, they analysed there results using system call traces to see if it is possible to detect insider threats by monitoring file access and process activity, raw data are looked at in a different manner: the relationships between users and files, users and processes, and processes and files. By analysing these models and relationships, the authors want to learn whether it is possible to build an effective insider threat detection system for each of these relationships. If any of the models do not work, they want to discover the reasons and all technical difficulties behind the problem. Furthermore, they want to discover any characteristics or promising approaches that can help to build good profiles for users and processes. As a proof of concept, they implemented a small detection system that use one of these profiles to detect a large set of buffer-overflow attacks.

To analyse file access and process execution, they has a log of system activity, they already had a large database of system call traces, collected for the project using software developed for Seer. The traces were collected from ten machines with twenty users over two years. Their approach for analysing file access was to develop patterns for two models: user-oriented and process oriented. When analysing patterns for each user, the authors decided to categorize the users into two sets: system users and normal users.

At the end of the result, the authors where able to design a system that detects insider misbehaviour, monitor system call activity and watch for danger signs or unusual behaviour. The authors describe an experimental system designed to test this approach. They tested the system's ability to detect common insider misbehaviour by examining file system and process-related system calls management

CHAPTER THREE

SYSTEM ANALYSIS AND RESEARCH METHODOLOGY

3.1 INTRODUCTION

System analysis is the study of a system, with the view to determine the bottlenecks and desired end product and establish the most efficient method of obtaining this end (American Heritage Dictionary, 2003). It is the analysis of the requirements of a task, and expression of these tasks in a form that enables a computer to perform the task. System analysis also refers to the process through which an existing system is examined with the intent of improving it, or creating a new system, through better procedures and methods (Schach, 1996).

3.2 METHODS OF DATA COLLECTION

Before the design of the proposed system, the basic problems and weaknesses confronting the present system were identified and defined in other to get the needed requirements of the proposed input/output specifications in line with what the automated proposed system would achieve.

The method used in data collection during the course of finding the feasibility of the new system includes;

Oral Interview

This was done when we visited the federal Inland Revenue service, which gave us an insight of how they carry out their operation with the system they already had, which led to the identification of problems listed above, and the zeal in finding lasting solutions to the identified problems.

Review of Document

We tried as much as we could to lay our hands on documents and journals that relates to our work at large and seeing the ideas of other people.

Website Research

This provides us with a wide range of information relating to network monitoring system and network activity monitoring system.

Library Research

It was quite helpful though little information was gotten from there.

3.3 ANALYSIS OF THE EXISTING SYSTEM

The activities of the bursary unit of FIRS include collecting taxes, collecting transaction request voucher (TRV) from the cash office for income collection, receiving and recording the retirement vouchers, receiving semi-annual inventory report (SIR) that emanates from different units and they also account for expenditure purpose through the cash office. The department has two sections, the operations unit and the reconciliation unit. These units consist of systems which are all on the same network, and serve as client.It also has a server where the accounting software is installed.

The individual client's works as well as store directly to the server. With the help of their monitoring software, the system records the daily activities with their respective dates only at the end of each day in each user's folder.

At the end of every month, the staffs at the operation unit will stop operation for the staff at the reconciliation unit to process the data they have already worked on. This is to avoid malfunctioning of the server such as hanging or disrupting the operations done by the reconciliation unit. The operation unit will resume work when the reconciliation staffs are through with their work. The time limit depends on the volume of work to be processed by the reconciliation unit.

The CPU usage depends on size of the work on the general ledger at a given time and because the server has a low memory and space, both units at the bursary department cannot work at the same time. However, this system does not explore the hierarchy of the processes, which can reveal important information on user behaviour.

3.3.1 ADVANTAGES OF THE EXISTING SYSTEM

From the observation and analysis of the present system, it is clear that the advantages exhibited by the existing system are limited. Such advantages are:

1. The users of each client system can carry out their operation using any system on that network without having any access to the work or operations of the original owner of the system been used.
2. In as much as the client systems have their own memories, the activities done on this client systems saves to the server system directly, and with this, one cannot trace the activities of the individual client systems on that system even if access is granted. The activities of each client system can only be mirrored from the server.

3.3.2 DISADVANTAGES OF THE EXISTING SYSTEM

1. It monitors the activities on the network with dates only, and does not give the exact time record which would be ineffective in time of investigation at the extreme level.
2. It is not memory efficient, because it does not only monitor the activities on the network, every operation done on the network is from the server.
3. It limits the speed of processing the works placed on the general ledger due to the server's low memory attribute

4. The proposed system does not explore the processes hierarchy and these is because it takes it logs with the dates only.

3.4 ANALYSIS OF THE PROPOSED SYSTEM

The proposed system is out to improve the detection of inside threats and investigations (fraud) of activities done by the network users. These systems uses screen capture traces to create a log for every activity (files) that is accessed by the user.

In the proposed system, the accounting software used by the bursary department of FIRS will be installed on the server system, so that while the server will be doing its work as a server system and the human users working with the client system stores their work directly in the server's memory. while the software will be keeping track of the activities of the client systems in real time (which can be changed at any time) and keeping the logs in the server system.

3.4.1 JUSTIFICATION OF THE PROPOSED SYSTEM

Clearly, it's not a responsible approach to run an organization on the basis of blind faith that every single employee can be trusted not to cause any damage. Implicit trust is a recipe for disaster, and it's not surprising that many corporate executives deploy some kind of transaction-monitoring system to mitigate some of the consequences that ill-judged or malicious employee actions can visit upon the welfare of their organization. The system is more effective and efficient when compared to the existing one being monitored, and because this system have the ability to protect the results of monitoring and only allow authorized personnel to have access to it, it is now obvious that the proposed system has both advantages and disadvantages, but the advantages outweighs the disadvantages thereby justifying the proposed system.

3.5 METHODOLOGY

A methodology is a system of methods and principles used in a particular "school" of design.

A methodology can be regarded as a system converting an input into an output. The system is a human-activity system, and is therefore not deterministic.

Different people will achieve different results. The unit of execution of a methodology (soft or hard) is called a project. There are basically four types of system methodology:

1. Prototyping System Methodology.
2. Expert System Methodology.
3. OOADM – Object-Oriented Analysis and Design Methodology
4. SSADM – Structured System Analysis and Design Methodology

The international accepted Structured System analysis and Design Methodology (SSADM) and Object Oriented Analysis and Design methodology (OOADM) unit will be deployed in this research. SSADM will be adopted for data collection while OOADM will be used for design phase.

The steps taken in SSADM to achieve this model are as follows:

3.5.1 PROBLEM DEFINITION

Before the design of the proposed system, the basic problems and weaknesses confronting the present system were identified and defined in other to get the needed requirements of the proposed input/output specifications in line with what the automated proposed system would achieve, which would be enumerated as the weaknesses in the subsequent subheading. Some of the problems identified in the present system are:

1. It monitors the activities on the network with dates only.

2. It is not memory efficient.

3. The speed of processing is slow due to the small memory of the server.

4. The activity logs for each user are arranged according to the size of the captured image.

3.5.2 FEASIBILITY STUDY

At this phase, investigations were thoroughly made in order to develop the new system in sufficient depth. This is done to enable the proposed system to provide information that can satisfy its implementation. Thus, deciding if the new system is feasible within the present budget.

The method used in data collection during the course of finding the feasibility of the new system includes

Oral interview

This was done when we visited the bursary department, which gave us an insight of how they carry out their operation with the system they already had, which led to the identification of problems listed above, and the zeal in finding lasting solutions to the identified problems.

Review of document

We tried as much as we could to lay our hands on documents and journals that relates to our work at large and seeing the ideas of other people.

Website Research

This provides us with a wide range of information relating to network monitoring system and network activity monitoring system.

Library research

It was quite helpful though little information was gotten from there.

3.5.3 INVESTIGATION AND ANALYSIS

The user's requirement was analysed with the description on a document which stated the functions, procedures and capabilities of the present system and that of the proposed network activity monitoring system.

To design this system, two specifications were made. The specifications involve an architectural design and a detailed design process.

During the architectural design process, the proposed system was broken down into different modules. Then each of these modules in turns is designed which resulted in the detailed design. The two design documents describe the basic processes on how network activity monitoring system performs its operation. In addition to the architecture, it was built to be platform independent to enable it to run in any operating system.

3.5.4 OBJECT ORIENTED ANALYSIS AND DESIGN METHODOLOGY

An Object Oriented Analysis and Design Methodology can be used to analyse the problem requirements, design a solution to the problems and implement a solution in a programming language or database. Object Modelling Technique (OMT) and Unified Modelling language (UML) are the two most popular object oriented methodologies which provide a set of concepts and notations which can be used throughout the entire software development process.

Object Oriented Analysis deals with the discovery, Analysis, and specification of requirements in terms of objects with identity that encapsulates properties and operations, message parsing, classes, inheritance, polymorphism and dynamic binding. The use of object oriented programming's like JAVA would be great importance because the data and instructions for processing are combined in a self-sufficient objects which are modules consisting of pre-assembled programming code, which can be re-use in other programming or modules in the design phase.

Object Oriented Design (OOD) will be the final step; it transforms the model produced in object oriented analysis. It will take into account the constraints imposed by the architecture and any non-functional technological or environmental constraints. This includes response time, transaction throughput, development environment, run-time platform, or the programming language.

CHAPTER FOUR

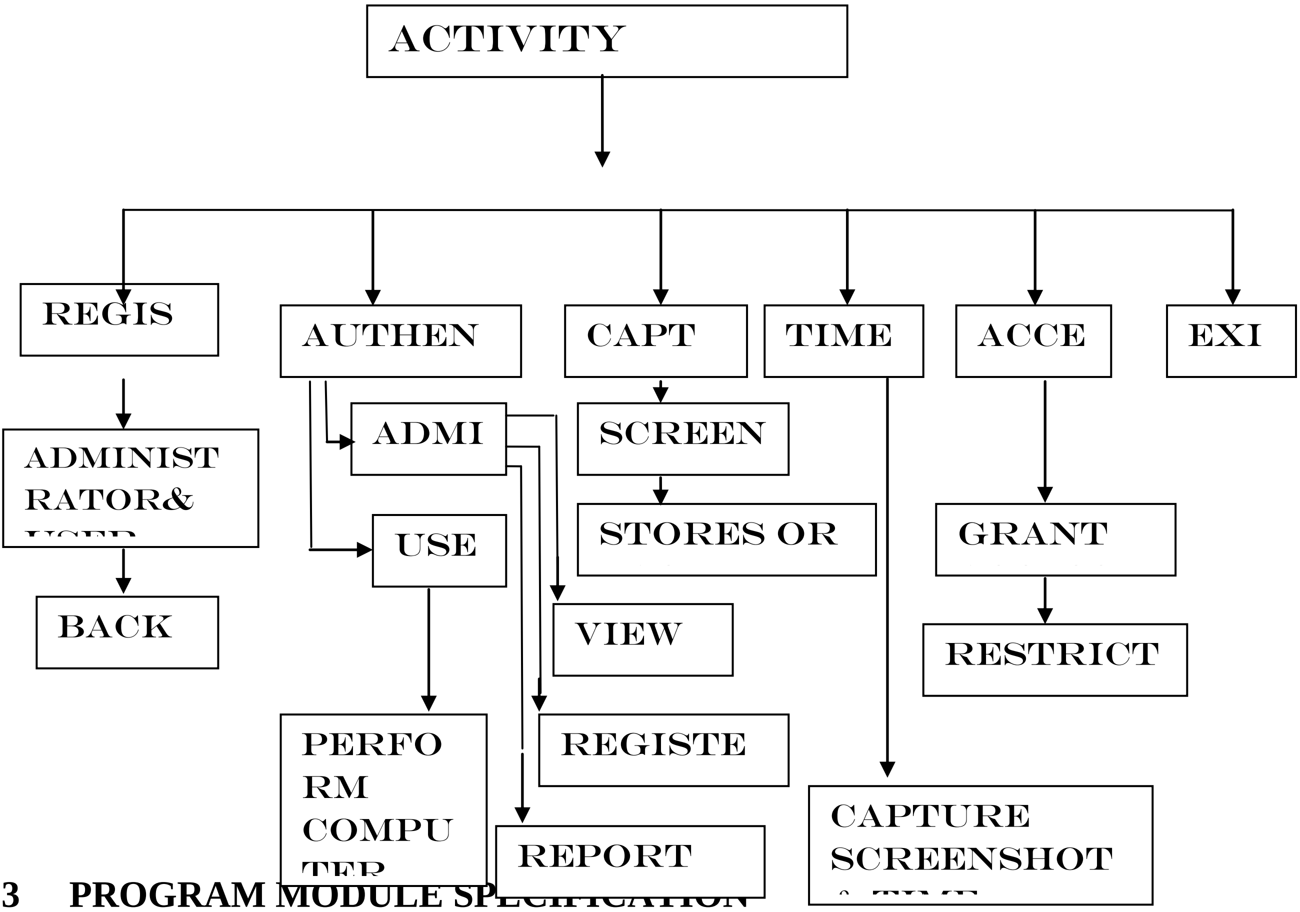
SYSTEM DESIGN AND IMPLEMENTATION

4.1 OVERVIEW OF THE DESIGN

The major objective of this research work is to design and implement a network activity monitoring system which will monitor the daily real time activities of every client system on a local area network.

The network activity monitoring software designed uses screen capturing in taking its activity logs, and these capturing consumes less memory, which makes the software memory efficient and the system able to contain as much logs a possible depending on the working hour without affecting other operations been carried out on the network.

4.2 MAIN MENUOF THE NETWORK ACTIVITY MONITORING SYSTEM.



4.3 PROGRAM MODULE SPECIFICATION

The program module specifies the various modules that will run the system.

Program module

Modules	**Description**
Loginpage.php	This is the first page after the system is powered on. It gives access to the server in which the software is installed based on accurate username and password.
File.php	This menu holds the following actions to be executed by the application (open, save, print, exit).
amsAdmin.php	This is where the administrator performs the auditing of the logs
regAdmin.php	This provides an interface where the administrator will be registered
regUser.php	This provides an interface where the user will be registered
logoutAdmin.php	This is where the administrator closes or logs out after his activities.
logoutClient.php	This is where the clients closes after daily transactions.

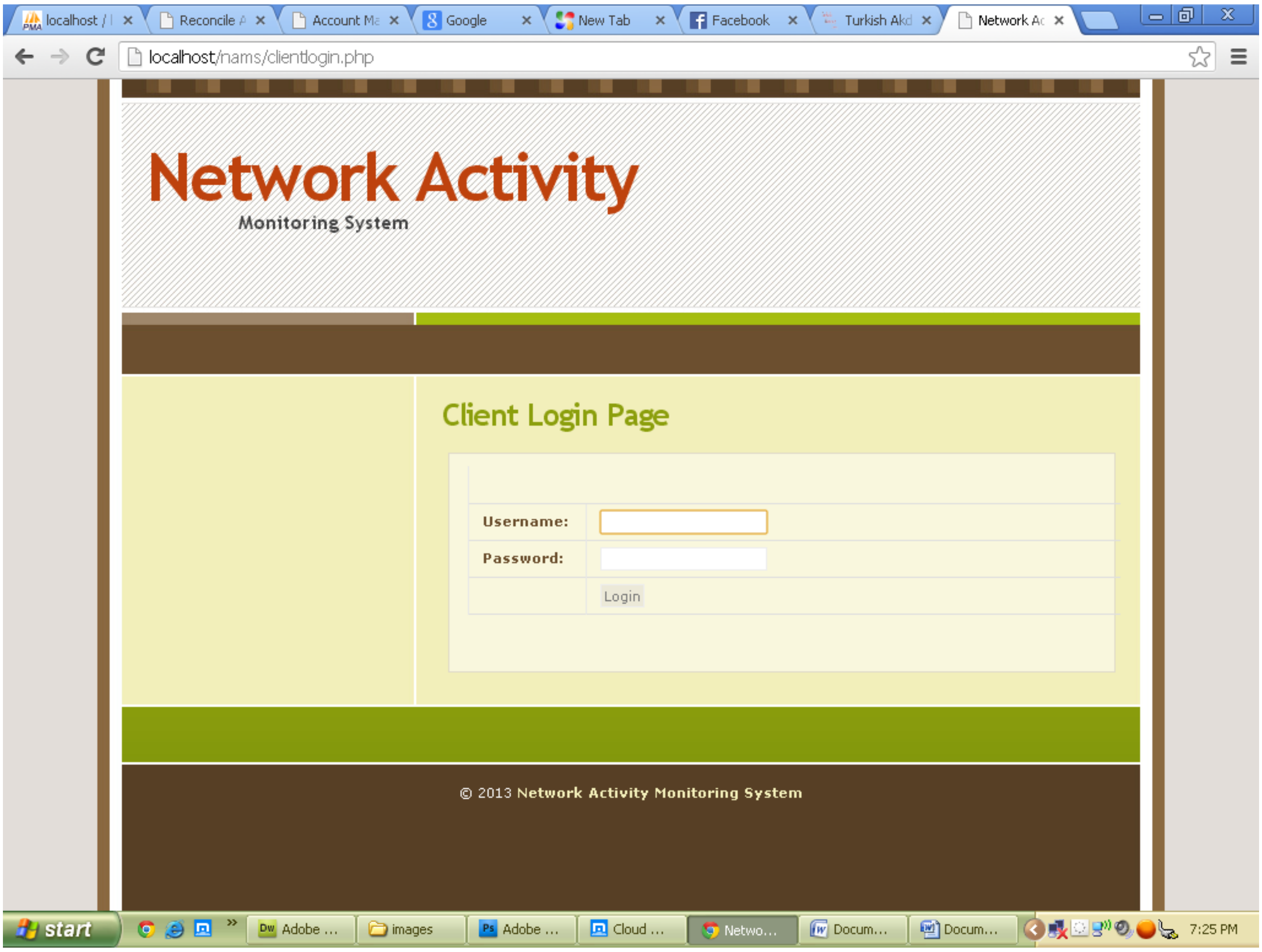
SPECIFICATION

The application is primarily intended to take and inconspicuously hide the activity logs which only the internal and external auditor would be the only people that will have access to it. The main advantage of this program for organizations is that they do not need to have knowledge of how the system takes it activity logs or the capturing time settings, they only need to log in there authentication and carry out their activities.

4.3.1 INPUT SPECIFICATION

Input specifications to the system are the User or client, Adminregistration form and login form and open new account form.

Fig 4.1 Input format for client login page



Network Activity

Monitoring System

Client Login Page

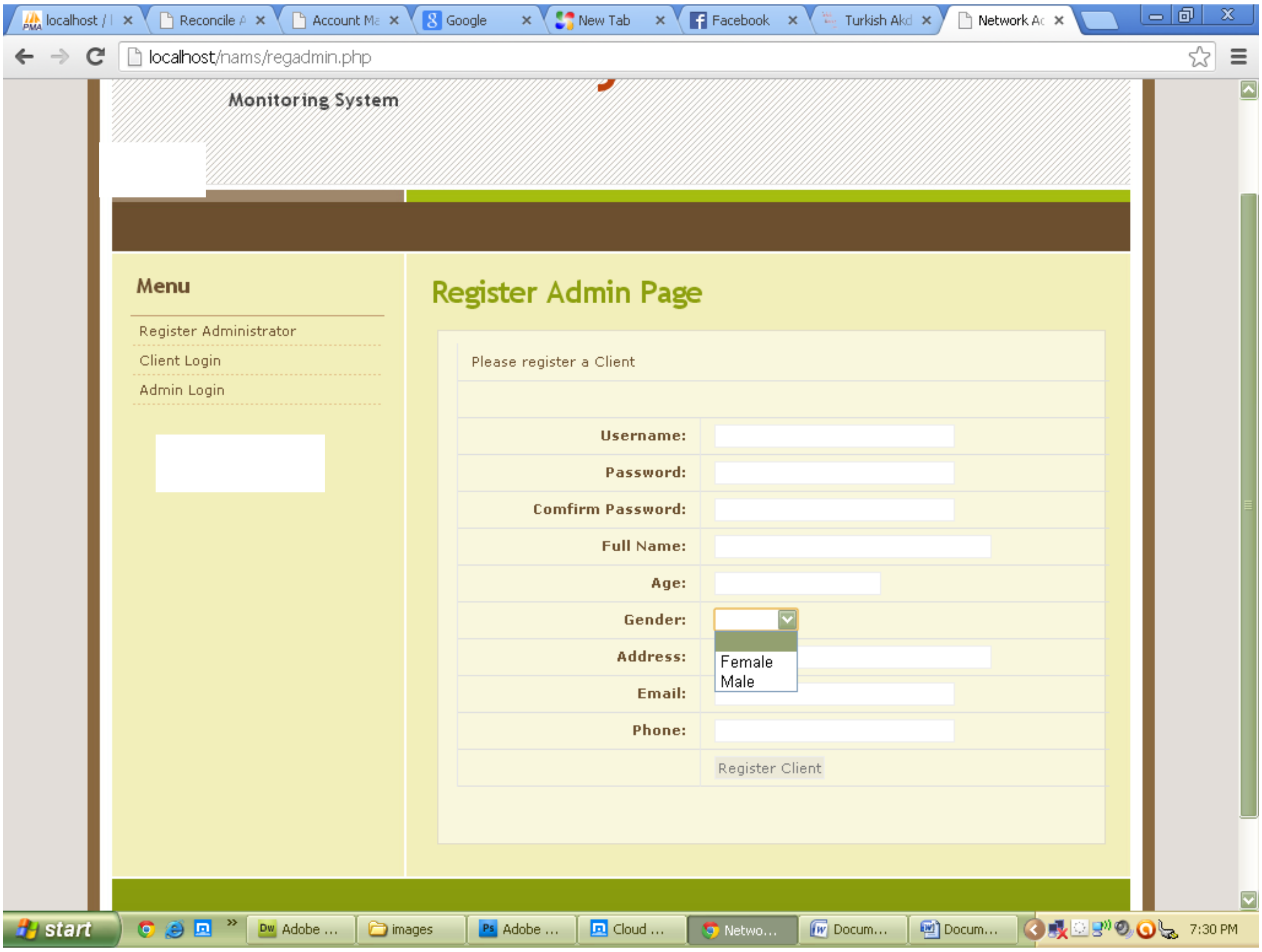
Username:

Password:

Login

© 2013 Network Activity Monitoring System

Fig 4.2 Input format for registering admin.

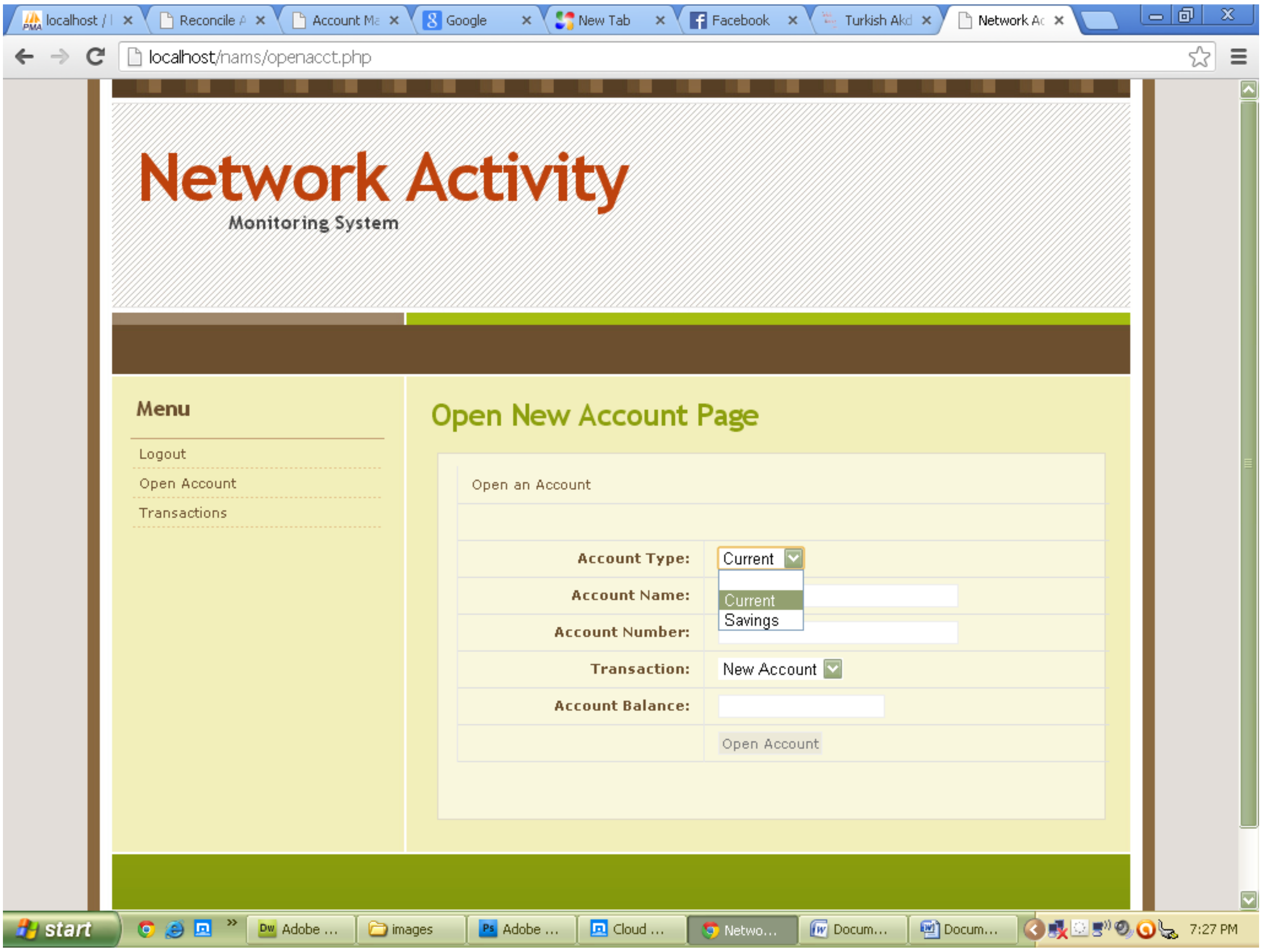


Register Admin Page

Please register a Client

Username:	
Password:	
Comfirm Password:	
Full Name:	
Age:	
Gender:	
Address:	
Email:	
Phone:	

Fig 4.3 Input format for opening new account.



Open New Account Page

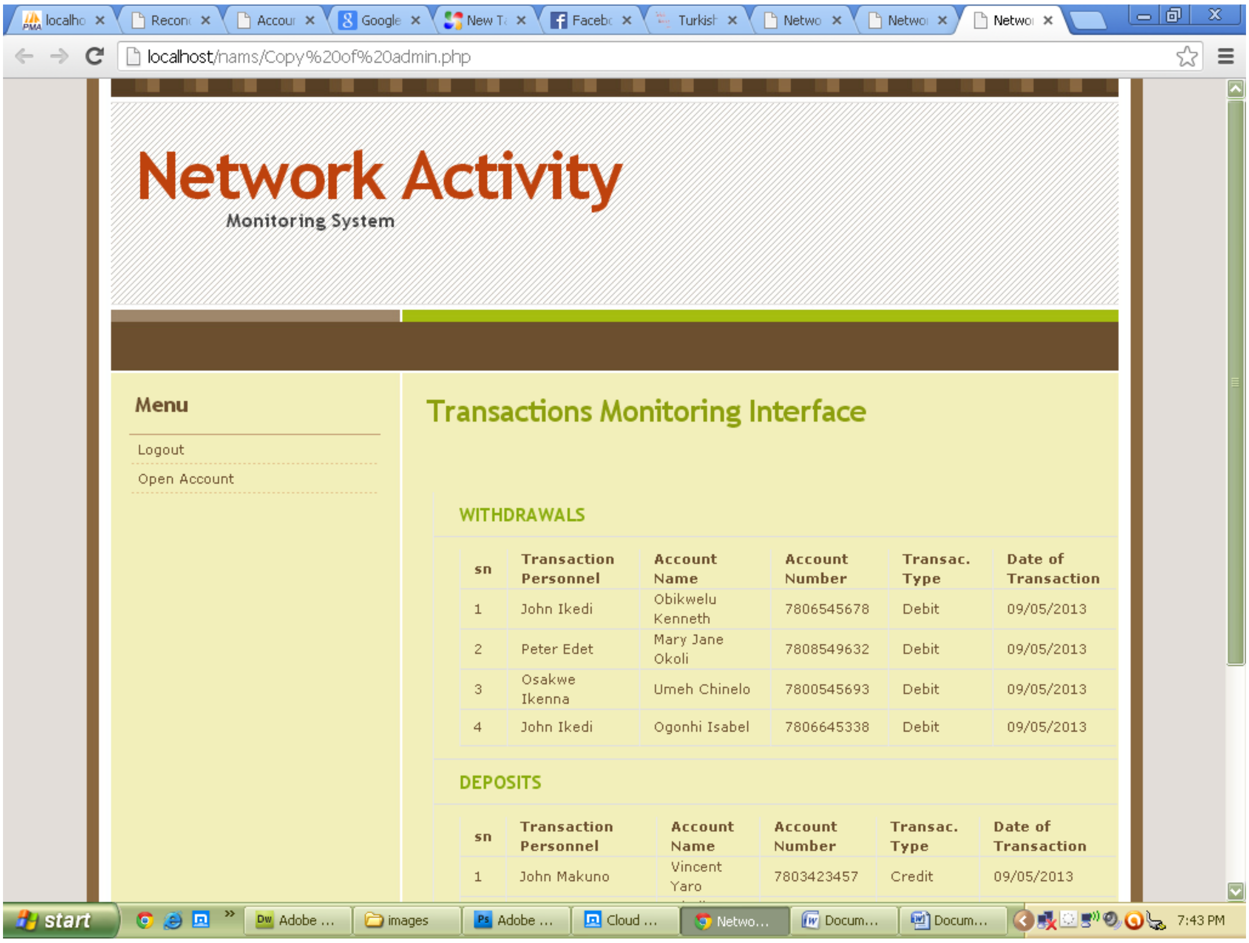
Open an Account

Account Type:	Current Current Savings
Account Name:	
Account Number:	
Transaction:	New Account
Account Balance:	

4.3.2 OUTPUT FORMAT

The operations that run in the system or the activities that are performed by the networked systems are captured to produce an activity logs. These activity logs are the output which contains the captured screenshots with the date and time. The captured screenshots are saved for future retrieval.

Fig.4.4 Output format of transactions activities.



Network Activity

Monitoring System

Menu

Logout

Open Account

Transactions Monitoring Interface

WITHDRAWALS

sn	Transaction Personnel	Account Name	Account Number	Transac. Type	Date of Transaction
1	John Ikedi	Obikwelu Kenneth	7806545678	Debit	09/05/2013
2	Peter Edet	Mary Jane Okoli	7808549632	Debit	09/05/2013
3	Osakwe Ikenna	Umeh Chinelo	7800545693	Debit	09/05/2013
4	John Ikedi	Ogonhi Isabel	7806645338	Debit	09/05/2013

DEPOSITS

sn	Transaction Personnel	Account Name	Account Number	Transac. Type	Date of Transaction
1	John Makuno	Vincent Yaro	7803423457	Credit	09/05/2013

4.3.3 DATABASE SPECIFICATION

The information required to be stored in the database are specified in Table 4.1 below.

Table 4.1 Database Specification

FIELD NAME	FIELD TYPE	FIELD SIZE	FIELD DESCRIPTION
User ID Char	30	It is the user login identity number	
User password	Char	15	It is the user login password
First name	Char	50	First name of the user
Last name	Char	50	Last name of the user
Phone no	Integer	15	the phone number of the user
E-mail	Char	30	the user e-mail address
Address	Char	70	User address

4.3.4 FLOWCHART OF THE PROPOSED SYSTEM.

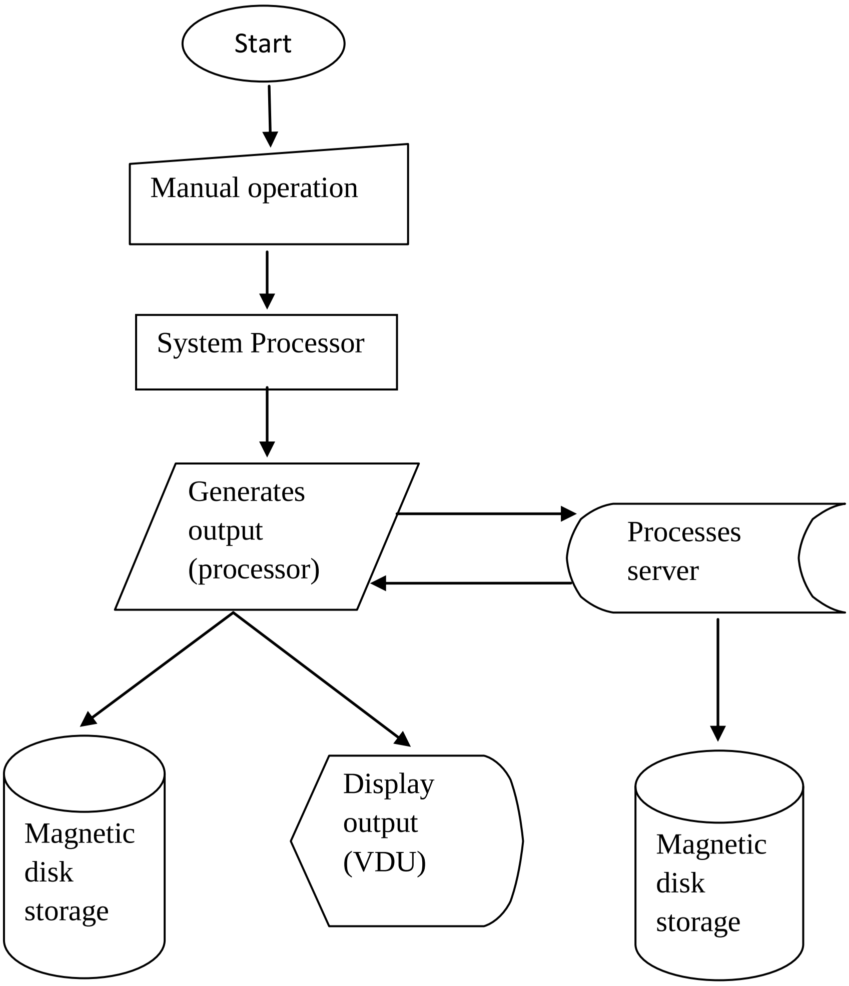
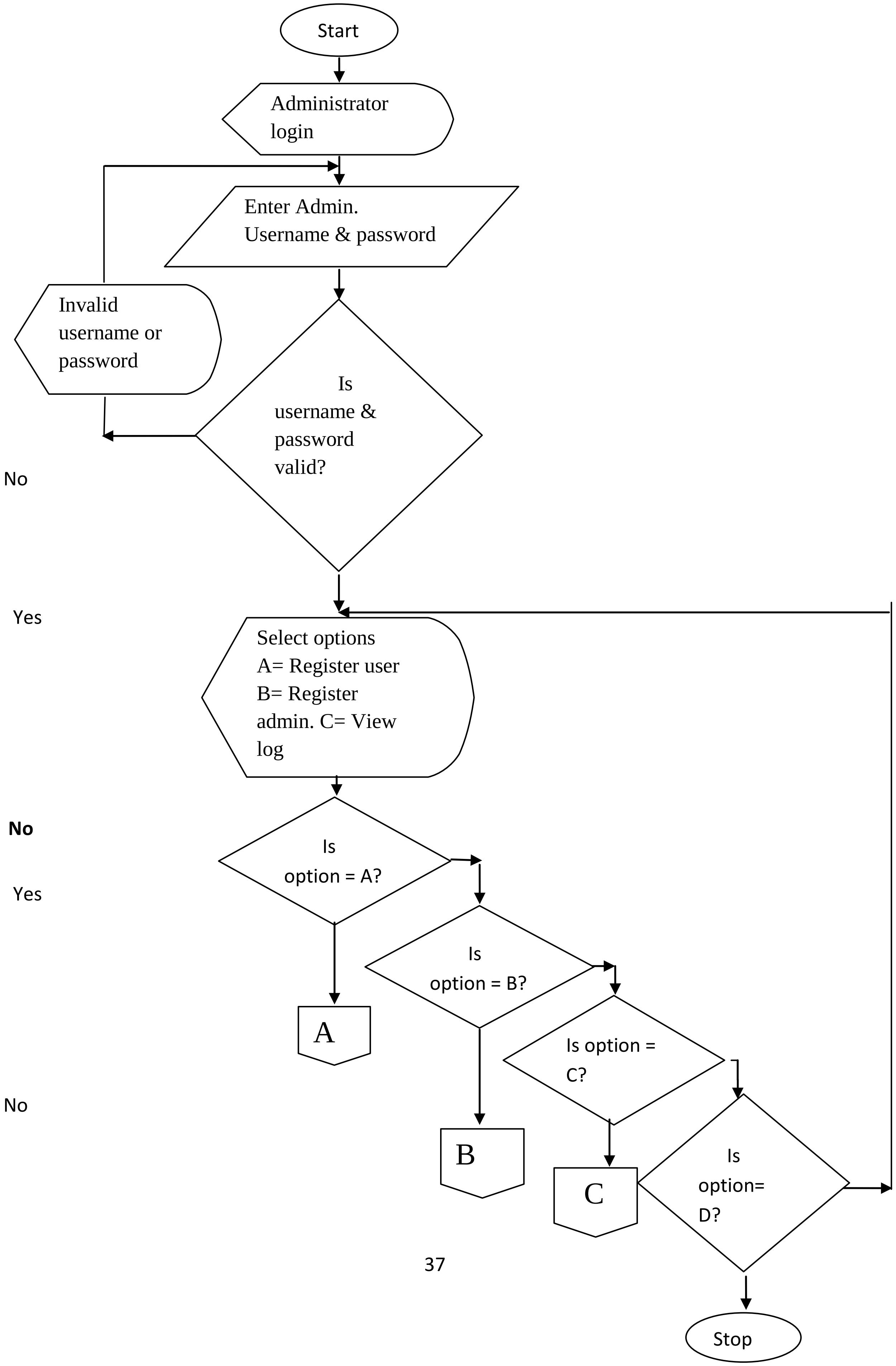
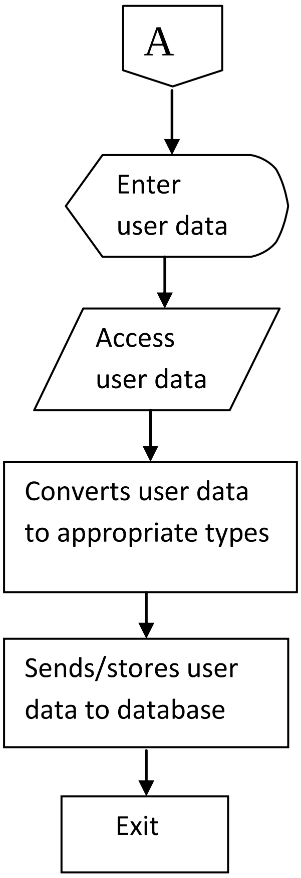
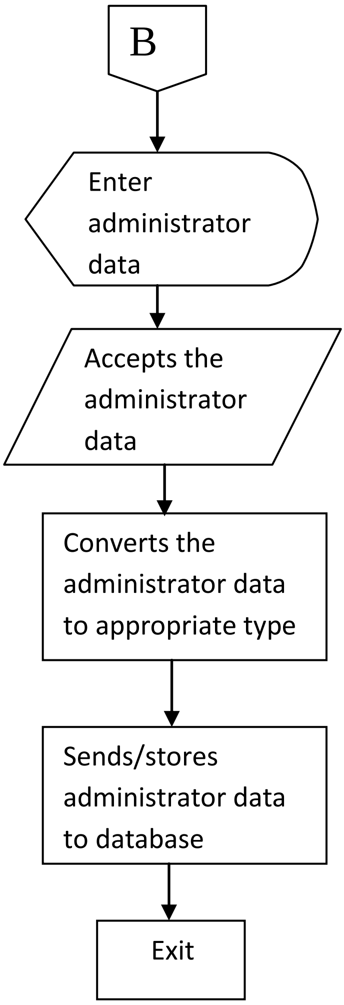


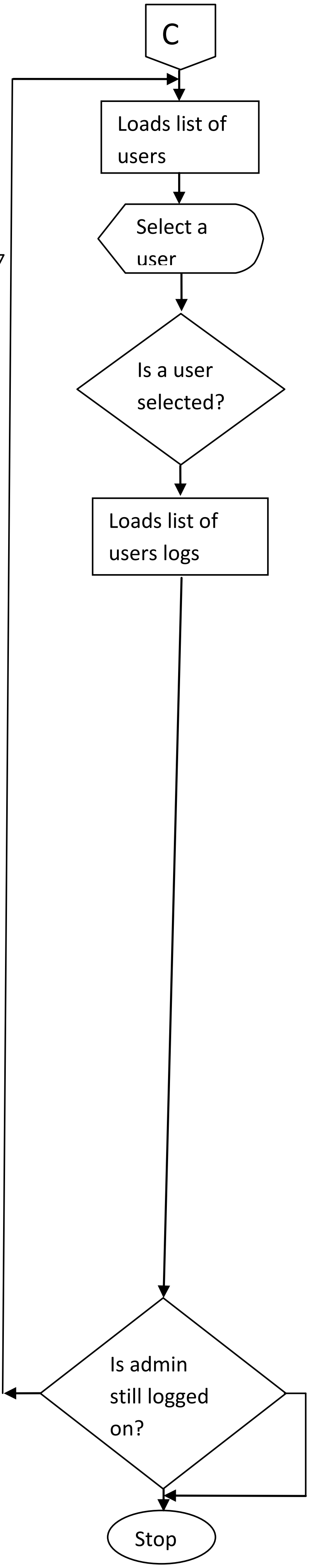
Fig 4.6 System flowchart

4.3.5 ADMIN.FLOWCHART OF THE PROPOSED SYSTEM


Start
Administrator login
Enter Admin. Username & password
Invalid username or password
Is username & password valid?
No
Yes
Select options A= Register user B= Register admin. C= View log
No
Is option = A?
Yes
Is option = B?
A
Is option = C?
No
B
C
Is option= D?
Stop


A
Enter user data
Access user data
Converts user data to appropriate types
Sends/stores user data to database
Exit


B
Enter administrator data
Accepts the administrator data
Converts the administrator data to appropriate type
Sends/stores administrator data to database
Exit


C
Loads list of users
Select a user
Is a user selected?
Loads list of users logs
Is admin still logged on?
Stop

Yes No

4.4 CHOICE AND JUSTIFICATION OF PROGRAMING LANGUAGE

The programming languages used in this project work are PHP and MySQL.

Justifications for using the programming language PHP for this work are as follows

- It is a server site scripting language
- Its open source (i.e. free to use) and cost of hosting a PHP application is less compared with the ASP(Active Server Page) and JSP(Java Server Pages)
- It adds dynamism to a website or web application.

Also MYSQL is used for the following reasons;

- It is preferred because it can execute queries against a database
- SQL can insert records in a database and can set permissions on tables, procedures and database.

It is also preferred because if the back end of the web application. This is because everything that is being done is stored to the database

4.5 SYSTEM REQUIRMENT

The following are the hardware and software requirement of the network activity monitoring system to ensure optimization.

Software Requirements

- Operating system (Windows Xp, windows Vista, windows 7, windows 8, server® 2003 32 or 64 bits)
- PHP program development kit Netbean IDE 6.9.1 or higher
- Database MySQL Server.

Hardware Requirements

- Intel Pentium iv processor/1.5GHZ processor (minimum) recommended.
- 1GB or higher RAM recommended.
- 80GB or higher of HDD recommended. Minimum of 10GB free space required for the windows Java SDK installation.
- Standard mouse for desktop PC's.
- Super visual graphics adapters (SVGA) with 1024*800 resolutions.
- UPS.
- Local area network connection.
- Standard keyboard.

4.6 IMPLEMENTATION PLANS

This procedure involves methods transiting from the old system to the new system. The researcher recommends the parallel changeover procedure because, it allows both the old system to be compared with the new automated system; as it allows the researcher and system designer to prove the efficiency of the new system over existing method of operation.

4.6.1 DOCUMENTATION

Program documentation is an ordered set of information for the computer system to follow and produce a result. These instructions are stored in computer memory to solve problem.

For this to be achieved there must be a procedure involving how to stop and start the system, enter information and must be properly documented.

4.6.2 USER GUIDE

On the client side:

Client logs in by inserting the correct username and password on the corresponding text field and password field.

Server side:

Double click on AMS Admin on the desktop

Admin must log in using the correct user name and password

To register user

1. Go to file
2. Click register user
3. Register user dialog comes up
4. Insert the user details and click the register user button.

To register administration

1. Go to file
2. Click register user
3. Register admin dialog comes up
4. Insert the admin details and click the register admin button

To exit

1. Go to file, then click on exit

To view image log

1. Go to edit, then click view log.
2. The view user log dialog box comes up.

3. On the dialog box, click or select a user and click view to view the user; list of dialog.
4. Click on each item on the list to view a particular image log

4.6.3 INSTALLATION OF THE SOFTWARE

The executable software is stored on a CD ROM or flash disk. Extract the executables;

1. Install the AMS admin first on the drive c: and include it on the system start up Menu followed by the PHP Runtime Environment.
2. Install the MYSQL server and configure the database.
3. To execute the user part of the application, since the AMS is included on the start-up, it will start up menu once the user boots up the system.
4. For the AMS admin, double click on the AMS Admin.php executable located on C:/AMS admin/ dist. to start.

4.7 MAINTENANCE DETAILS

Software needs to be reviewed and maintained at intervals, to ensure proper functioning. Hence there is need to maintain the software at regular interval to make sure that unforeseen problems are solved and ensure that the new system continue to achieve desired results. The following are the ways to maintain the software:

- Backup the image cache folder on bi-weekly bases
- Back up the database tables
- Make sure that all the clients goes off before the service
- The server must have a standby UPS (Uninterrupted Power Supply)
- There may be need to change the capturing time of the software, depending on security levels.

CHAPTER FIVE

SUMMARY AND CONCLUSION

4.1 SUMMARY

The topic of this work was reviewed in chapter one with the view of solving the problems encountered in the Ministry of Federal Inland Revenue Service, Anambra state. During the course of the research, the present system was analysed in other to detect the bottlenecks using Structured System Analysis and Design Methodology. Object oriented analysis and design methodology was found sufficient and efficient in the design of the proposed system.

4.2 REVIEW OF ACHIEVEMENTS

The activity monitoring system was tested and found to achieve the following:

- It monitored the daily activities of the clients.
- Has a great impact on memory management of the server.
- Detected active users.
- Provided accurate evidence on corporate fraud when investigation is being carried out in an organization with regards to date and time.
- Captured and saved screen shots of every user’s daily activities.

4.3 SUGESTIONS FOR FURTHER STUDIES

The developed system can be integrated to monitor micro-programs that can run within the system without actually displaying on the computer screen, or another activity monitoring system that can make use of other means of monitoring the activities on the network apart from screen-capturing can be developed so as to enable monitoring not only the activities that can be displayed on the computer screen but also the ones that can run within the system without actually displaying it on the computer screen.

5.4 AREAS OF APPLICATION

The activity monitoring system can be applied in so many areas where there is need to monitor the clients in a network. Financial institution, private and public sector and so on can benefit from using the software, but with further enhancement it can be used in global organization like the internet service providers, bank etc.

5.5 CONCLUSION

Today, computing system which consists of a broad range of processors, communication network and information repositories are vital to the operations of many sectors in our society, from financial and manufacturing to education and health care.

Network activity monitoring system is a desktop based application, developed to assist organization and institution in monitoring the activities running in their network domain to decrease financial fraud, improve the staff productivity and improve confidentiality of data.

With activity monitoring system as a powerful tool for monitoring activities and hidden data in activity logs, all data and files can be capture and kept securely over the server without tipping of attackers.

The view of this work has shown that monitoring the activities on a network system is efficient because there may not be room for any lapses in delay time in identifying what might have probably gone wrong assuming a problem arises. However implementation of the proposed system will improve the company’s performance in relation to accessing the activity logs. With the necessity of information flow in a network, putting a monitoring mechanism (wired or wireless) in place will go a long way in checkmating hacker authentications into networks.

APPENDIX A (Program Codes)

Admin.php

```
<?php

include('adminlock.php');

include("config.php");

session_start();

if(isset($_POST['view']) || isset($_POST['view2'])){


        $acct_name = trim($_POST['acct_name']);

        $acct_num = trim($_POST['acct_num']);

        if($acct_name == " && $acct_num == "){


                $msg = "Please Insert Acount Name or Number";


                }

                        else{


                        $sql="SELECT * FROM activities WHERE acct_name='$acct_name' or acct_number='$acct_num' ORDER BY sn DESC LIMIT 1";

                        $result=mysql_query($sql);

                        $row=mysql_fetch_array($result);

                        $active=$row['active'];
```

```
            $count=mysql_num_rows($result);


            $_SESSION['acctt']=$row['acct_type'];


    /*      // If result matched $myusername and $mypassword, table row must be 1 row

        if($count > 0){

            session_register("myusername");

            $_SESSION['login_user']=$myusername;


            header ('Location: client.php');

                }

            else {

            $msg="Your Login Name or Password is invalid";

} */

            }

        }

        if(isset($_POST['view3']) || isset($_POST['view4']) ){


    $acct_name2 = trim($_POST['acct_name2']);

    $acct_num2 = trim($_POST['acct_num2']);

        if($acct_name2 == " && $acct_num2 == "){

            $msg = "Please Insert Acount Name or Number";


        }
```

```
            else{


            $sql="SELECT * FROM activities WHERE acct_name='$acct_name2' or acct_number='$acct_num2' ORDER BY sn DESC LIMIT 1";

            $result=mysql_query($sql);

            $row=mysql_fetch_array($result);

            $active=$row['active'];

            $_SESSION['acctt']=$row['acct_type'];


            $count=mysql_num_rows($result);


            }

        }


    if(isset($_POST['transact'])){


        $acct_name = trim($_POST['acct_name']);

        $acct_num = trim($_POST['acct_num']);

        $acct_bal = trim($_POST['acct_bal']);

        $amt_withdrawn = trim($_POST['amt_withdrawn']);


        if($acct_name == '' || $acct_num == '' || $acct_bal == '' || $amt_withdrawn == ''){


            $msg = "Please complete the empty fields";
```

```
                    }
                else{

            if($amt_withdrawn> $acct_bal){

                $msg = "Transaction Cannot be Completed. Insufficient Account
Balance!!";
                        }

                else{

                    $x = 0;
                    $acct_type = $_SESSION['acctt'];
                    $client = $_SESSION['login_user'];
                    $today = date("m/d/y");
                    $new_balance = $acct_bal - $amt_withdrawn;
                    $sql="insert into activities values('$x', '$client', '$acct_num',
                        '$acct_name', 'Withdrawal','$amt_withdrawn',
'$new_balance', '$acct_type', '$today')";
                    $result=mysql_query($sql) or die(mysql_error());
    /* $row=mysql_fetch_array($result);
    $active=$row['active'];

    $count=mysql_num_rows($result); */
                    header("location: account_debited.php");
```

Clientlogin.php

```
<?php


include("config.php");

session_start();


if($_SERVER["REQUEST_METHOD"] == "POST"){

// username and password sent from form


$myusername = trim(addslashes($_POST['username']));

$mypassword = trim(addslashes($_POST['password']));


if($myusername == '' || $mypassword == ''){


        $error="Please Complete the Empty Field";


}


else{

        $sql="SELECT * FROM members WHERE username='$myusername' and 
password='$mypassword'";

        $result=mysql_query($sql);

        $row=mysql_fetch_array($result);

        $active=$row['active'];
```

```
		$count=mysql_num_rows($result);

// If result matched $myusername and $mypassword, table row must be 1 row

if($count > 0){

		session_register("myusername");

		$_SESSION['login_user']=$myusername;

		header ('Location: client.php');

		}

else {


$error="Your Login Name or Password is invalid";


}

}


}//end

?>

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">


<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en">

<head>


<meta name="Description" content="Information architecture, Web Design, Web Standards." />

<meta name="Keywords" content="your, keywords" />
```

```
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />

<meta name="Distribution" content="Global" />

<meta name="Robots" content="index,follow" />


<link rel="stylesheet" href="images/HarvestField.css" type="text/css" />


<title>Network Activity Monitoring System - Login Page</title></head>


<body>

<!-- wrap starts here -->

<div id="wrap">


        <!--header -->

        <div id="header">


                <h1 id="logo-text"><a href="client.php" title="">Network Activity</a></h1>


                <h2 id="slogan">Monitoring System</h2>

        <!--header ends-->

        </div>


        <!-- navigation starts-->

        <div  id="nav">
```

```
                <div id="light-brown-line"></div>

        <!-- navigation ends-->

        </div>



        <!-- content-wrap starts -->

        <div id="content-wrap">

        <div id="main">

<h1>Client Login Page          </h1>

<form action="" method="post">

        <table width="100%" border="0">

        <tr>

        <td colspan="2"><?php echo $error; ?></td>

        </tr>

        <tr>

        <td width="18%"><strong>Username:</strong></td>

        <td width="82%"><label>

        <input type="text" name="username" id="username" />

        </label></td>

        </tr>

        <tr>

        <td width="18%"><strong>Password:</strong></td>

        <td width="82%"><label>

        <input type="password" name="password" id="password" />

        </label></td>
```

```
          </tr>

          <tr>

          <td width="18%">&nbsp;</td>

          <td width="82%"><label>

          <input type="submit" name="login" id="login" value="Login" />

          </label></td>

          </tr>

          </table>

          <p><br />

          </p>

                    </form>

                              <br />



                    <!-- main ends -->

                    </div>



          <!-- content-wrap ends-->

          </div>



          <!-- column starts -->

          <div id="column-wrap">

          <!-- column-wrap ends-->

</div>
```

```
        <!-- footer starts -->
        <div id="footer">


                <p>
                &copy; 2013 <a href="client.php" title="">Network Activity Monitoring System</a>
                <!-- footer ends -->
        </p>
        </div>


<!-- wrap ends here -->
</div>


</body>
</html>
```

Openaccount.php

```
<?php


include('clientlock.php');
include("config.php");
session_start();


if($_SERVER["REQUEST_METHOD"] == "POST"){
// username and password sent from form
```

```
$acct_type = trim(addslashes($_POST['acct_type']));

$acct_name = trim(addslashes($_POST['acct_name']));

$acct_number = trim(addslashes($_POST['acct_number']));

$transaction = trim(addslashes($_POST['transaction']));

$acct_bal = trim(addslashes($_POST['acct_bal']));



if($acct_type == '' || $acct_name == '' || $acct_number == '' || $transaction == '' || $acct_bal == '' ){


        $error="Please Complete the Empty Field";


}



else{


        $x = 0;

        $client = $_SESSION['login_user'];

        $today = date("m/d/y");

        $sql="insert into activities values('$x', '$client', '$acct_number', '$acct_name', '$transaction',
'$acct_bal', '$acct_type', '$today')";

        $result=mysql_query($sql);

        /* $row=mysql_fetch_array($result);

        $active=$row['active'];
```

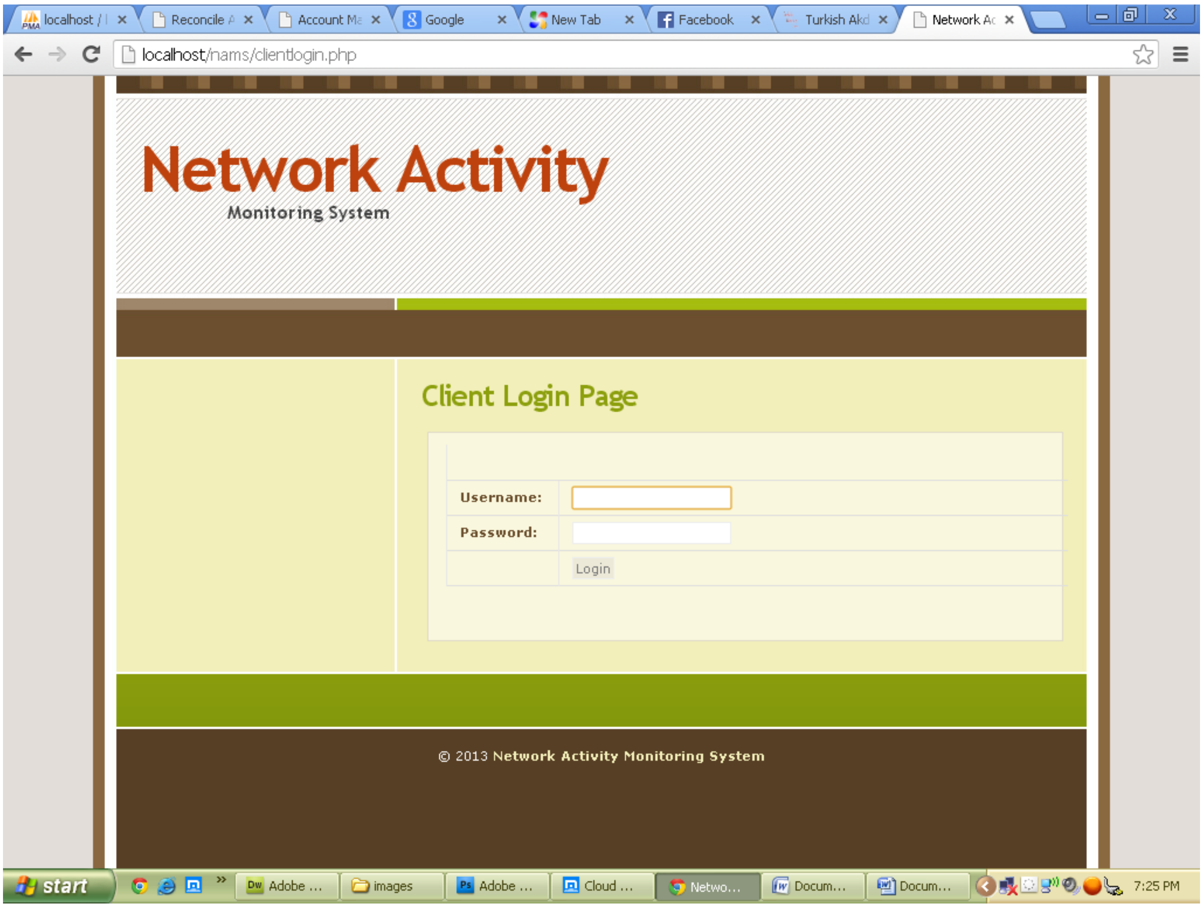
```
	$count=mysql_num_rows($result); */

	header("location: thanks.php");


}


}//end

?>

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">


<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en">
```

Regadmin.php

```
<?php


include("config.php");

session_start();


if($_SERVER["REQUEST_METHOD"] == "POST"){

// username and password sent from form

$username = trim(addslashes($_POST['username']));

$password = trim(addslashes($_POST['password']));
```

```
$cpassword = trim(addslashes($_POST['cpassword']));

$fullname = trim(addslashes($_POST['fullname']));

$age = trim(addslashes($_POST['age']));

$gender = trim(addslashes($_POST['gender']));

$address = trim(addslashes($_POST['address']));

$email = trim(addslashes($_POST['email']));

$phone = trim(addslashes($_POST['phone']));


if($username == " || $password == " || $cpassword == " || $fullname == " || $age == " || $gender == " ||
$address == " || $email == " || $phone == "){


        $error="Please Complete the Empty Field";


}

else{


        if( $password !=  $cpassword){


                $error="Passwords does not match";

                                }

                                else{

                $x = 0;

        $sql="insert into admin values('$x', '$username', '$cpassword', '$fullname', '$age', '$gender',
'$address', '$email', '$phone')";

        $result=mysql_query($sql);
        /* $row=mysql_fetch_array($result);

        $active=$row['active'];



        $count=mysql_num_rows($result); */

        header("location: thanks.php");



}

}



}//end
```

APPENDIX B (Sample, Output forms)



Network Activity

Monitoring System

Client Login Page

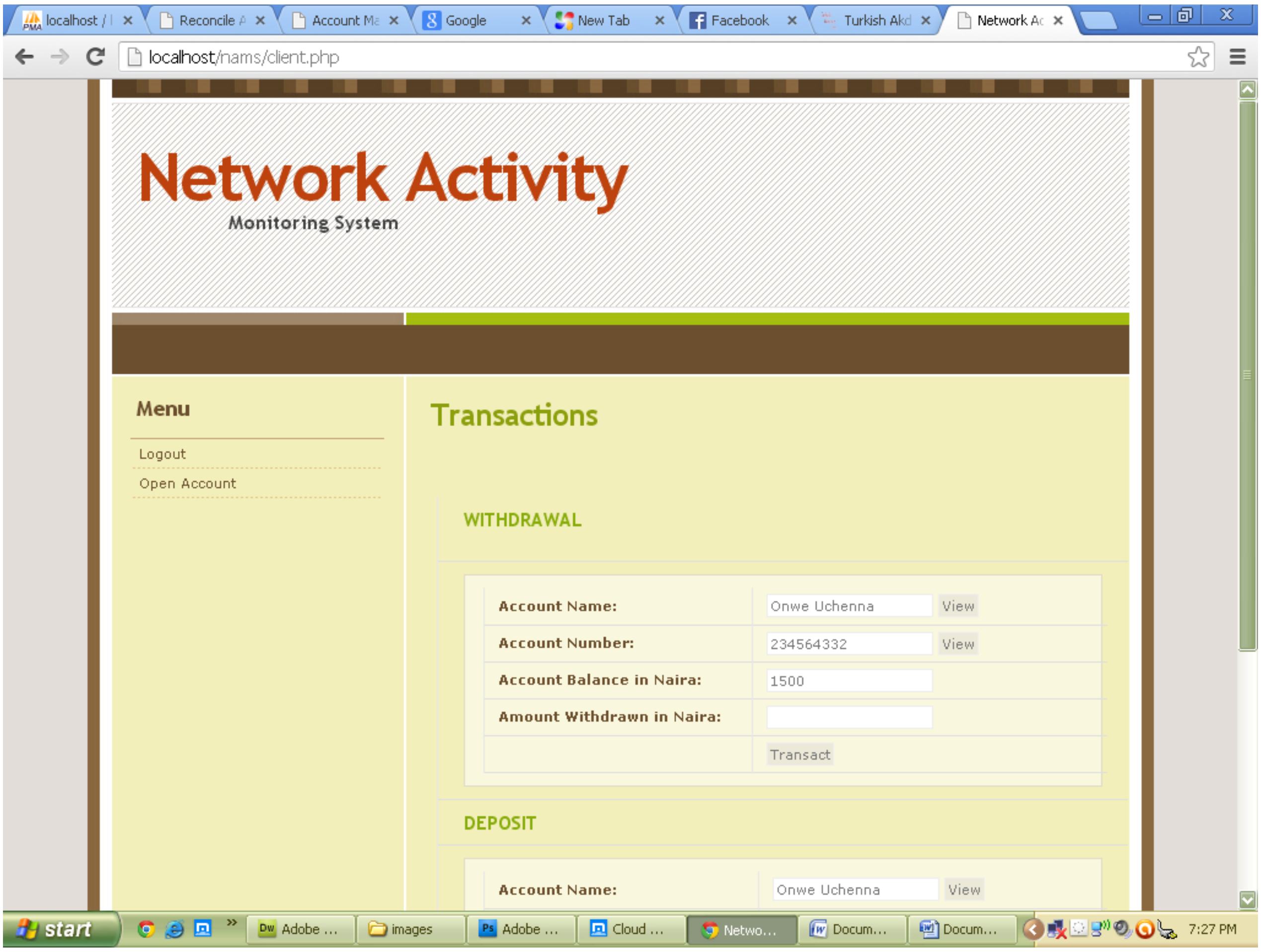
Username:

Password:

Login

© 2013 Network Activity Monitoring System

Client login page



Network Activity

Monitoring System

Menu

- Logout
- Open Account

Transactions

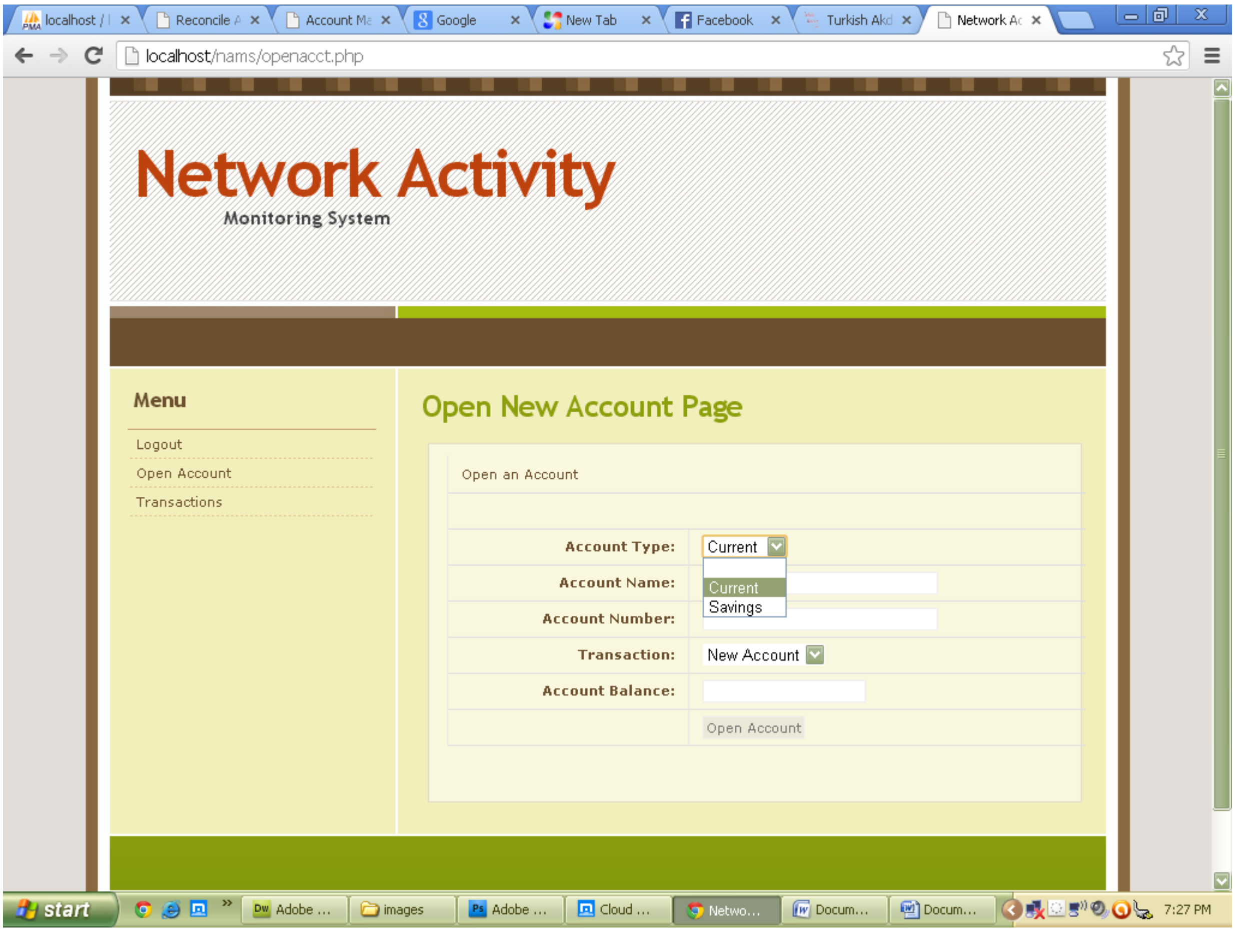
WITHDRAWAL

Account Name:	Onwe Uchenna	View
Account Number:	234564332	View
Account Balance in Naira:	1500	
Amount Withdrawn in Naira:		
	Transact	

DEPOSIT

Account Name:	Onwe Uchenna	View

Transactions page



localhost/nams/openacct.php

Network Activity

Monitoring System

Open New Account Page

Open an Account

Account Type: Current (Current, Savings)

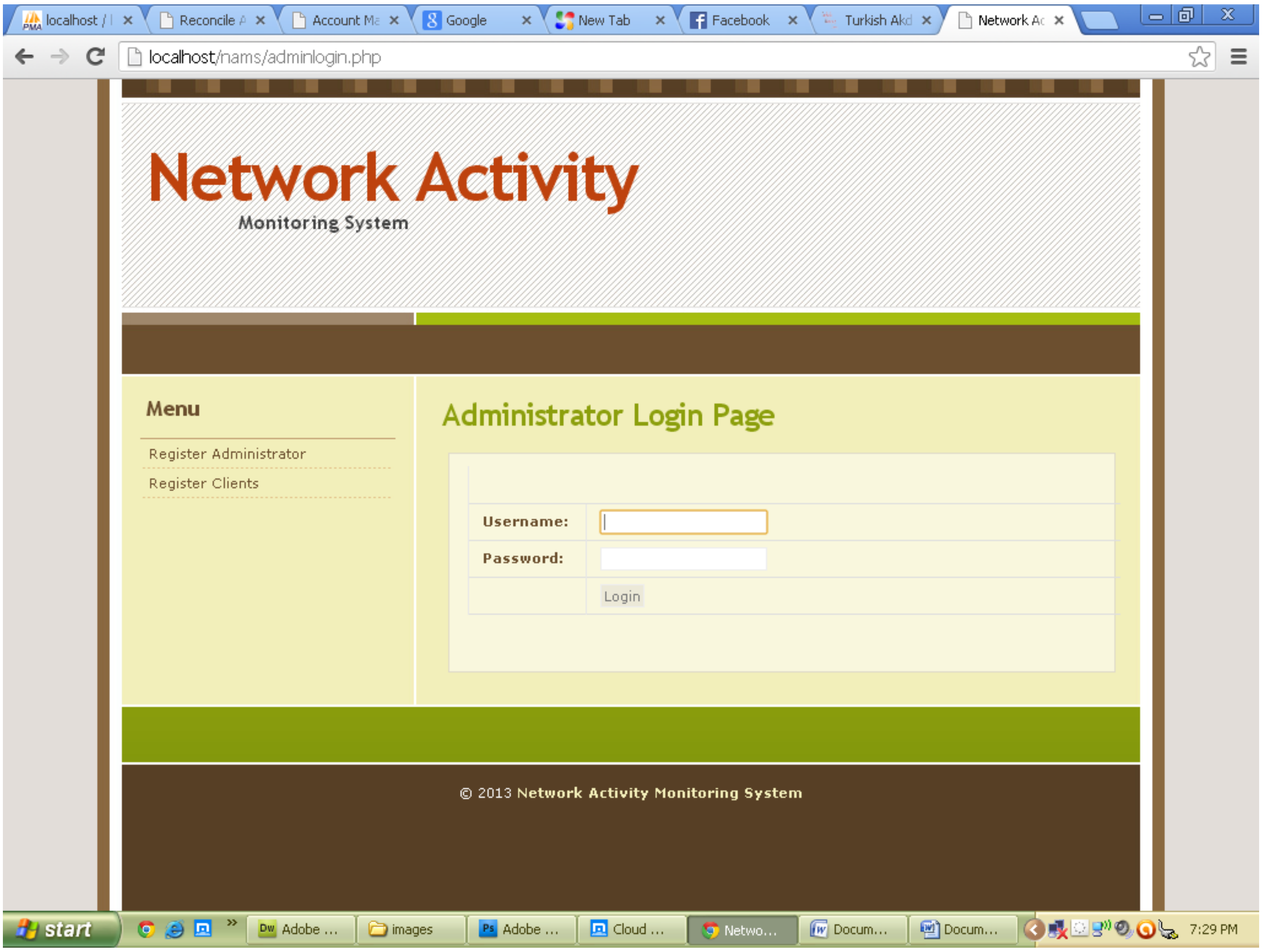
Account Name:

Account Number:

Transaction: New Account

Account Balance:

Open new bank account page



Network Activity

Monitoring System

Menu

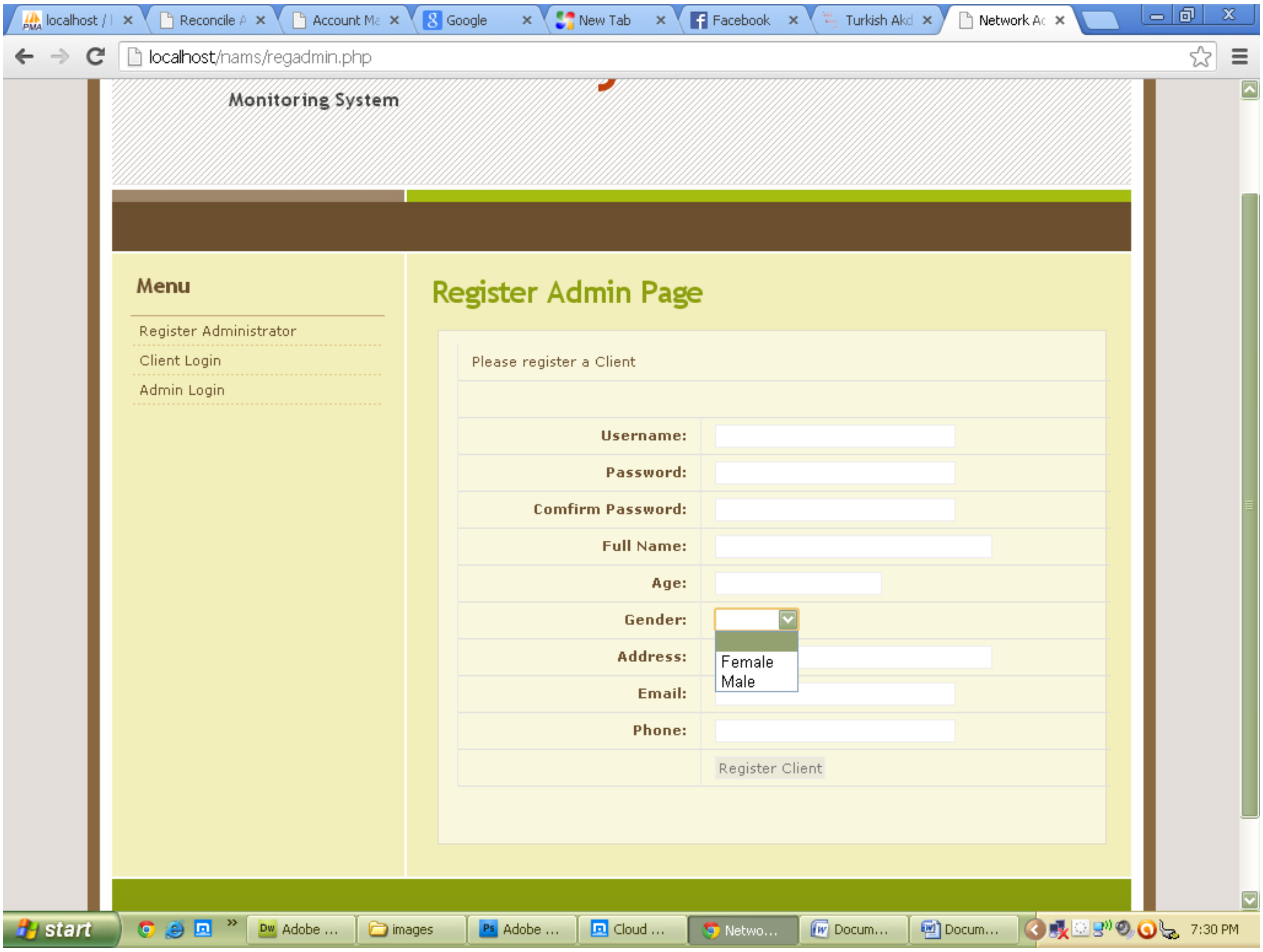
- Register Administrator
- Register Clients

Administrator Login Page

Username:	|
Password:	
	Login

© 2013 Network Activity Monitoring System

Admin Login Page

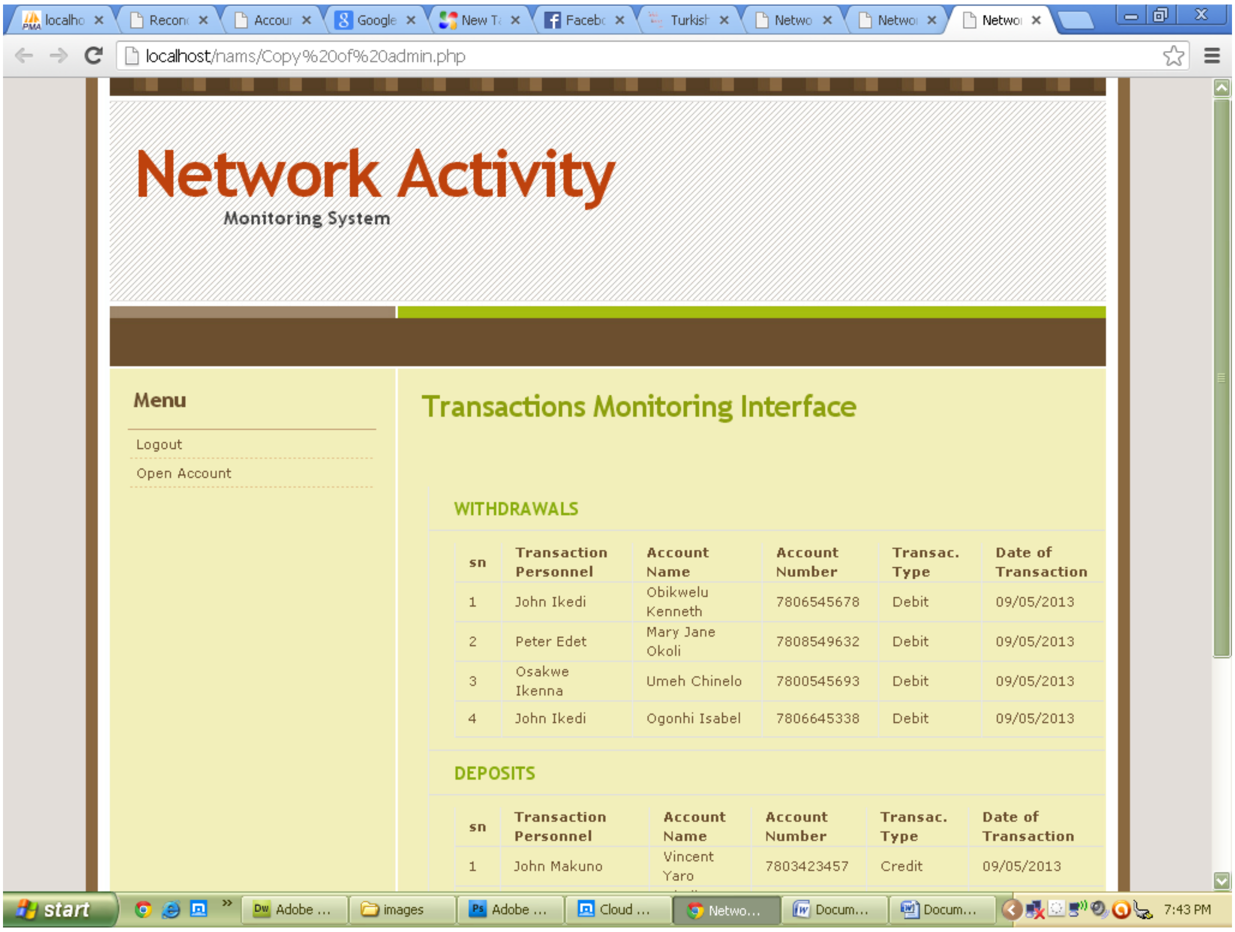


Register Admin Page

Please register a Client

Username:	
Password:	
Comfirm Password:	
Full Name:	
Age:	
Gender:	Female Male
Address:	
Email:	
Phone:	

Register Admin Page



Network Activity

Monitoring System

Menu

Logout

Open Account

Transactions Monitoring Interface

WITHDRAWALS

sn	Transaction Personnel	Account Name	Account Number	Transac. Type	Date of Transaction
1	John Ikedi	Obikwelu Kenneth	7806545678	Debit	09/05/2013
2	Peter Edet	Mary Jane Okoli	7808549632	Debit	09/05/2013
3	Osakwe Ikenna	Umeh Chinelo	7800545693	Debit	09/05/2013
4	John Ikedi	Ogonhi Isabel	7806645338	Debit	09/05/2013

DEPOSITS

sn	Transaction Personnel	Account Name	Account Number	Transac. Type	Date of Transaction
1	John Makuno	Vincent Yaro	7803423457	Credit	09/05/2013

Transactions Monitoring Interface