CHAPTER 1

INTRODUCTION

This Chapter gives an overview of the project LAN CLIENT ANALYSER and about the tools and technologies used.

1.1 ABOUT THE PROJECT:

Multiple Clients Computers controlled by a Single server via LAN. Network monitoring provides the information necessary for network management. It is important to find network trends and locate network problems quickly.

Server can able to find client machine activities like login, logout, current working status of the user. Implement the project in order to find some unauthorized access by the client machine.

From this method, avoid Resource theft as well as possible to keep monitoring the client tasks.

Servers wan have a Domain Controller to provide Authorization and Authentication of client machines which are presenting the LAN.

1.2 SYSTEM STUDY:

- The Admin can easily Track User's details by using "LAN Client Analysis Tools".
- Main Scope of the Project is to keep tracking client activities by the Admin
- Easily identified Resource theft
- Malpractice identification is more efficient

1.3 HARDWARE REQUIREMENTS:

Processor	: Dual core and above
Hard Disk	: 50 GB
RAM	: 2 GB

1.4 SOFTWARE REQUIREMENTS:

Operating System	: WINDOWS SERVER R2 2012, WINDOWS 8.1
Language	: JAVA

1.5 TOOLS AND TECHNOLOGIES USED:

1.5.1 JAVA

In the early days of the web, a server could dynamically construct a page by creating a separate process to handle each client request. The process would open connection to one or more databases in order to obtain the necessary information. It communicated with the web server via an interface known as the Common Gateway Interface (CGI) .CGI allowed the separate process to read data from HTTP request and write data to the HTTP response. A variety of different languages were used to build CGI programs including C, C++ and Perl.

JAVA'S MAGIC: THE BYTE CODE

The key that allows java to solve both the security and the portability problems just described is that, the output of the java compiler is not an executable code. Rather, it is Byte Code. Byte Code is a highly optimized set of instructions designed to be executed by virtual machine that the java Run-time system emulates. However, the fact that a java program is interpreted helps solve the major problems associated with downloading the program over the Internet.

Here is why java was designed to be interpreted language. Because java programs are interpreted rather than compiled .It is easier to run them in wide variety of environments. Only the java runtime system needs to be implemented for each platform. Once the runtime package exists for a given system any java program can run on it. If java were a compiled language then different versions of the same program will have to exist for each type of CPU connected to the Internet.

Thus interpretation is the easiest way to create truly portable programs. Although java was designed to be interpreted, there is technically nothing about java that prevents on the fly compilation of Byte Code into native code. However, even if dynamic compilation were applied to Byte Code, the portability and safety would still apply, because the run time system would still be in change of the execution environment.

FEATURES OF JAVA

- Division into Functions
- Problems with Structured Programming
- Relationship to the Real World
- New Data Types
- The object oriented approach
- Classes
- Abstraction
- Encapsulation
- Inheritance

CHAPTER 2

SYSTEM ANALYSIS

This chapter gives an overview of the system design, working method to evaluate network systems. Recommend network and Data communications, hardware and software required are also discussed here.

2.1 EXISTING SYSTEM:

The administrator has to take all the trouble of going to a particular system to access a file that is needed by him. The processes that are running in a particular system can be viewed only in that system itself by using the present generation software's.The security was not the primary objective. Restorable capabilities were not a big issue.

Access Management process to provide Admin privileges to selected personnel. It becomes very important for the organizations to know if a server is down or non-functional and take corrective action immediately

- Previous network monitoring tools are not user friendly.
- The security was not the primary objective.
- Restorable capabilities were not a big issue.
- Traffic rerouting was not a prominent feature in their inventory.

2.2 PROPOSED SYSTEM:

The disadvantages present in the existing systems can be overcome using the proposal systems. Using The LAN CLIENT ANALYSER Tool the administrator can control the operations of the Client system from his system itself.

- The administrator can get the configuration of the remote system from the server system itself using this software.
- In order to Maintain User details of Client machine as Log Files
- In order to terminate the operations on the remote systems, the administrator can obtain the current process details of the remote systems from the server itself.
- This monitoring piece of the application keeps pinging each of the servers at the specific intervals.

CHAPTER 3

DOMAIN CONTROLLAR

This chapter gives an overview of the Domain Controller, Active Directory and group polices, client machine interaction

3.1 DEFINITOIN:

A domain controller (DC) is a server that responds to security authentication requests within a Windows Server domain. It is a server on a Microsoft Windows or Windows NT network that is responsible for allowing host access to Windows domain resources.

A domain controller is the centre piece of the Windows Active Directory service. It authenticates users, stores user account information and enforces security policy for a Windows domain.

A server running Active Directory Domain Services (AD DS) is called a domain controller. It authenticates and authorizes all users and computers in a Windows domain type network—assigning and enforcing security policies for all computers and installing or updating software.

For example, when a user logs into a computer that is part of a Windows domain, Active Directory checks the submitted password and determines whether the user is a system administrator or normal user.

Also, it allows management and storage of information, provides authentication and authorization mechanisms, and establishes a framework to

deploy other related services: Certificate Services, Federated Services, Lightweight Directory Services and Rights Management Services.

On Microsoft Servers, a domain controller (DC) is a server computer that responds to security authentication requests (logging in, checking permissions, etc.) within a Windows domain. A *domain* is a concept introduced in Windows NT whereby a user may be granted access to a number of computer resources with the use of a single username and password combination.

3.2 INSTALL ACTIVE DIRECTORY DOMAIN SERVICES ON WINDOWS SERVER 2012 WITH SERVER MANAGER:

1. Open Server Manager, then select Manage and click on "Add Roles and Features".
2. Click next on the "Before you begin" window.
3. Select Role-based or feature-based installation and then click next.
4. Click Select a server from the server pool, click the name of the server to install Active Directory Domain Services to, and then click Next (If you wanted to install this on a remote server, you have to first create a server group containing the remote server).
5. Click Active Directory Domain Services. When the Add Roles and Features Wizard dialog box opens, select Add Features, then Next.
6. On the Active Directory Domain Services page, review the information and then click next.
7. On the Confirm installation selections page, click Install.

8. On the Results page, verify Installation succeeded, and click Promote this server to a domain controller to start the Active Directory Domain Services Configuration Wizard.

The nice part about using the Server Manager method is that it takes you directly into running the Active Directory Domain Services Configuration Wizard, which is the utility which replaced the deprecated DC promo.

Now that you've installed the features, you will need to promote the server into a domain controller.

3.3 PROMOTE A SERVER TO A DOMAIN CONTROLLER:

1. Choose your Deployment Configuration.
2. To install a domain controller to an existing domain, specify the domain name**.**
3. To install a new domain in existing forest, choose "Child" or "Tree" domain, then browse for forest structure.
4. To install a new forest, specify the new forest name. Then click next.
5. Choose your Domain Controller Options**.**
6. To create a new forest or domain, select the functional levels, click Domain Name System (DNS) server, specify the Directory Services Restore Mode password, and then click next.
7. To add a DC to a domain, choose Domain Name System (DNS) server**,** Global Catalog (GC)**,** or Read Only Domain Controller (RODC) as needed, choose the site name, and type the Directory Services Restore Mode password and then click next.

8. If installing a DNS Server, you may need to Update DNS delegation**.** To update, enter credentials with permission to create DNS delegation records in the parent DNS zone. (To help determine if you need to update DNS delegation, see the Microsoft TechNet article Understanding Zone Delegation. For more information on any errors that may be generated by updating DNS delegation, see DNS Options.
9. If installing a Read Only Domain Controller (RODC), specify the group that will manage the RODC. Add or remove accounts to the Allowed or Denied password replication groups. Click Next.
10. On the Additional Options page, choose one of the following options:
11. To create a new domain, type or verify the NetBIOS name of the domain.
12. To add a DC to a domain, select a domain controller to replicate the AD DS installation data from (or the wizard can select "any").
13. Specify where the directories for the Active Directory database, the log files, and the SYSVOL folder will be. Click Next. Warning: Do not attempt to store any of the above on a Resilient File System data volume.
14. You may need to specify alternate credentials to run adprep on the Preparation Options page.
15. If you want to reuse these steps again, click View Script, and copy the text of the Power Shell script.
16. Verify your server was successfully promoted on the results page,then click Close**.**
17. A reboot is required and it happens automatically by default.
18. You can also automate this process with Power Shell.
19. Install-ADDS Domain Controller.
20. Install-ADDS Domain,
21. Install-ADDS Forest

3.4 USE OF DOMAIN CONTROLLER:

Though Windows Server 2012 removes the DC promo that system engineers have been using since 2000, they have not removed the functionality. If a GUI is preferred by an active directory engineer, they may still have much of the look and feel provided through Server Manager. If a script or a command line interface is preferred, new cmdlets in PowerShell provide all of the flexibility of the GUI, with the added benefit or scalability and reusability.

CHAPTER 4

SYSTEM DESIGN

A system design shows the components and wiring in a network of computers and other devices. Design is the place where quality is fostered in software development. Design provides us with representations of software that can assess for quality

4.1 DATA FLOW DIAGRAM:

The Figure 4.1 shows the DFD used for the system.

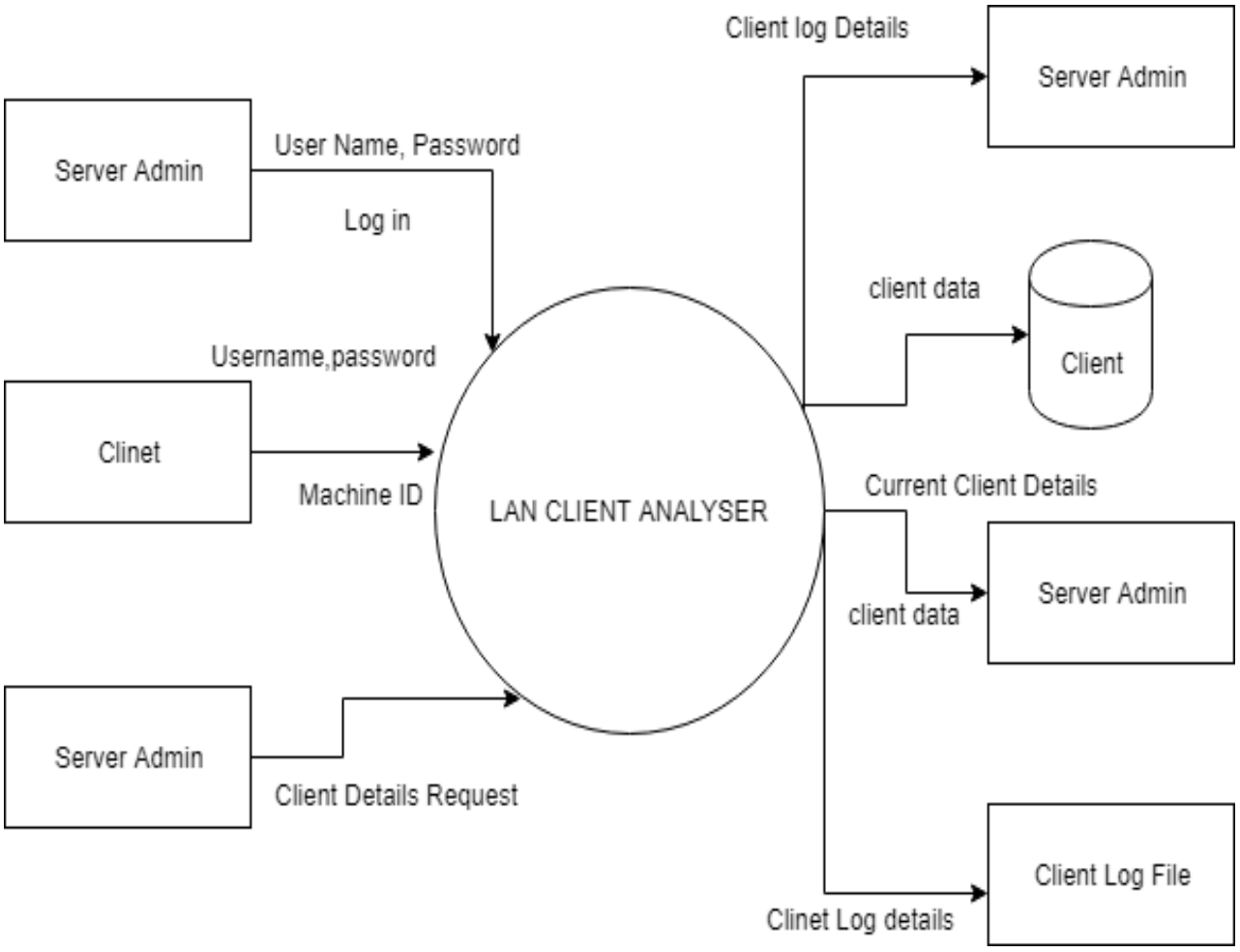

Fig 4.1 DFD

CHAPTER 5

MODULES

This chapter gives an overview of the modules which are implemented in this project also discussed here. The **LAN CLIENT ANALYSIS** Tool is divided in to four modules based on their functionalities. These modules are as follows.

- Active Machines
- Current Task List
- Event Log file
- Remote Capturing
- Socket Implementation

5.1 ACTIVE MACHINES:

Using Active Machines module, we can easily identified which are systems are currently logged in by user along with System name and IP Address. This Module get input as any serious of IP Address like 000.000.000.000 in this format. By Clicking Enter Button in tool we can able to see the currently working machine name along with IP Address.

Normally in a local area network, most of the workstations or remote computers use dynamic IP addresses assigned by the DHCP service. It is possible but very tedious work to check which computer is up and running on the network by using the PING command from command prompt. Lots of computers connected to a network could be sharing resources such as printers or files and folders, and it's sometimes useful to get a list of what is being shared across the network.

One of the options that you have is using the -P0 flag which skips the host discovery process and tries to perform a port scan on all the IP addresses (In this case even vacant IP addresses will be scanned). Obviously this will take a large amount of time to complete the scan even if you are in a small (20-50 hosts) network. But it will give you the results

5.2 CURRENT TASK LIST:

A task list is actually a prioritized list of all the tasks and responsibilities that need to be performed at a certain amount of time. The list will contain everything that needs to be done and obviously, the tasks that have the nearest deadline are given priorities.

When you create task lists for your projects, it’s equivalent to drawing up a specific plan on how you want to carry out your business. If there are "big tasks" that you need to perform, divide them into smaller tasks or even subtasks.

Task lists also create short term and long term goals for the employees and companies. When each goal is accomplished (or ticked off because you're done with it), then you're not simply finishing tasks but inspiring employees to achieve higher goals because they can evidently see their progress.

This too displays a list of currently running process on either a local or remote machine. It is available in the below Microsoft operating Systems as tasklist.exe. This Module Used to get Client machines Current working files, In Task list we can able to find which process are currently running in client machine. Also shows user name and time of the process begin and what program in currently running.

5.3 EVENT LOG FILE:

- Event Log files are used to find what is current status of user, like currently working file, When The User logged inetc.
- The Event Viewer is a tool in Windows that displays detailed information about significant events on your computer.
- Examples of these are programs that don't start as expected or automatically downloaded updates.
- Event Viewer is especially useful for troubleshooting Windows and application errors.

EVENT VIEWER DISPLAYS THESE TYPES OF EVENTS

Error: A significant problem, such as loss of data or loss of functionality. For example, if a service fails to load during startup, an error will be logged.

Warning: An event that is not necessarily significant, but may indicate a possible future problem. For example, when disk space is low, a warning will be logged.

Information: An event that describes the successful operation of an application, driver, or service. For example, when a network driver loads successfully, an Information event will be logged.

Success Audit: An audited security access attempt that succeeds. For example, a user's successful attempt to log on to the system will be logged as a Success Audit event.

Failure Audit: An audited security access attempt that fails. For example, if a user tries to access a network drive and fails, the attempt will be logged as a Failure Audit event.

The Event Log service starts automatically when you start Windows. Application and System logs can be viewed by all users, but Security logs are accessible only to administrators

5.4 REMOTE CAPTURING:

With Remote Desktop Connection, you can connect to a computer running Windows from another computer running Windows that's connected to the same network or to the Internet.

For example, you can use all of your work computer's programs, files, and network resources from your home computer, and it's just like you're sitting in front of your computer at work.

To connect to a remote computer, that computer must be turned on, it must have a network connection, Remote Desktop must be enabled, you must have network access to the remote computer (this could be through the Internet), and you must have permission to connect.

For permission to connect, you must be on the list of users. Before you start a connection, it's a good idea to look up the name of the computer you're connecting to and to make sure Remote Desktop connections are allowed through its firewall.

HOST

Enter the IP address or host name of the target platform where the Remote Packet Capture Protocol service is listening. The drop down list contains the hosts that have previously been successfully contacted. The list can be emptied by choosing “Clear list” from the drop down list.

PORT

Set the port number where the Remote Packet Capture Protocol service is listening on. Leave open to use the default port (2002).

NULL AUTHENTICATION

Select this if you don’t need authentication to take place for a remote capture to be started. This depends on the target platform. Configuring the target platform like this makes it insecure.

PASSWORD AUTHENTICATION

This is the normal way of connecting to a target platform. Set the credentials needed to connect to the Remote Packet Capture Protocol service.

DO NOT CAPTURE OWN RPCAP TRAFFIC

This option sets a capture filter so that the traffic flowing back from the Remote Packet Capture Protocol service to Wire shark isn’t captured as well and also send back. The recursion in this saturates the link with duplicate traffic.

USE UDP FOR DATA TRANSFER

Remote capture control and data flows over a TCP connection. This option allows you to choose an UDP stream for data transfer.

SAMPLING OPTION NONE

This option instructs the Remote Packet Capture Protocol service to send back all captured packets which have passed the capture filter. This is usually not a problem on a remote capture session with sufficient bandwidth.

SAMPLING OPTION 1 OF X PACKETS

This option limits the Remote Packet Capture Protocol service to send only a sub sampling of the captured data, in terms of number of packets. This allows capture over a narrow band remote capture session of a higher bandwidth interface.

SAMPLING OPTION 1 EVERY X MILLISECONDS

This option limits the Remote Packet Capture Protocol service to send only a sub sampling of the captured data in terms of time. This allows capture over a narrow band capture session of a higher bandwidth interface.

MICROSOFT WINDOWS ONLY

This dialog and capability is only available on Microsoft Windows. On Linux/Unix you can achieve the same effect (securely) through an SSH tunnel.

5.5 INTRODUCTION TO RMI:

` Remote Method Invocation (RMI) facilitates object function calls between Java Virtual Machines (JVMs). JVMs can be located on separate computers - yet one JVM can invoke methods belonging to an object stored in another JVM. Methods can even pass objects that a foreign virtual machine has never encountered before, allowing dynamic loading of new classes as required. Remote method invocation allows applications to call object methods located remotely, sharing resources and processing load across systems.

Unlike other systems for remote execution which require that only simple data types or defined structures be passed to and from methods, RMI allows any Java object type to be used - even if the client or server has never encountered it

before. Any object that can be invoked this way must implement the Remote interface.

When such an object is invoked, its arguments are “marshalled” and sent from the local virtual machine to the remote one, where the arguments are “unmarshalled”. When the method terminates, the results are marshalled from the remote machine and sent to the caller's virtual machine. If the method invocation results in an exception being thrown, the exception is indicated to caller.

RMI ARCHITECTURE

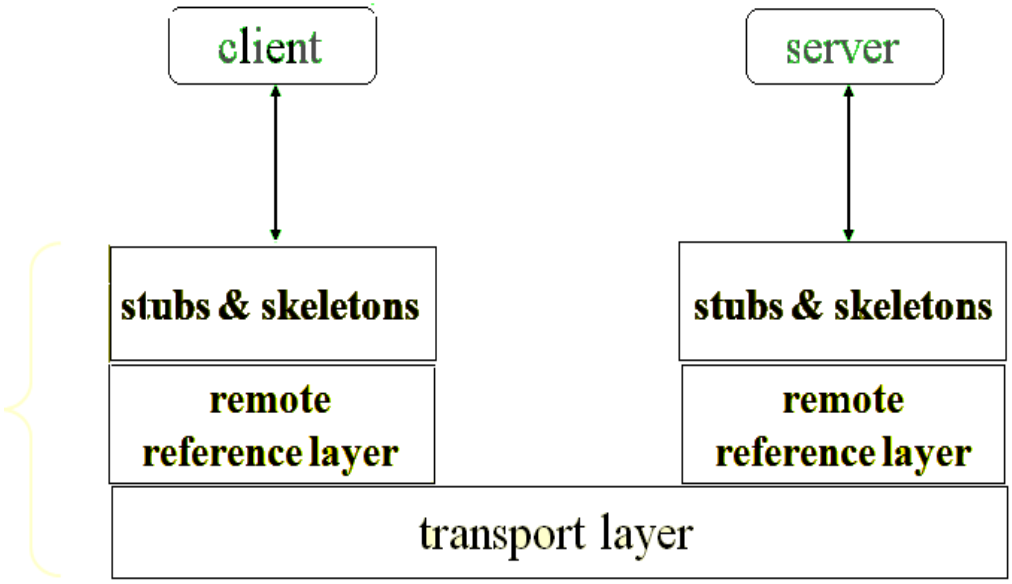

Fig 5.1 RMI Architecture

LOCATE REMOTE OBJECTS

Applications can use one of two mechanisms to obtain references to remote objects. An application can register its remote objects with RMI's simple naming facility, the RMI registry, or the application can pass and return remote object references as part of its normal operation.

COMMUNICATE WITH REMOTE OBJECTS

Details of communication between remote objects are handled by RMI; to the programmer, remote communication looks like a standard Java method invocation.

LOCAL CLASS BYTE CODES FOR OBJECTS THAT ARE PASSED

Because RMI allows a caller to pass objects to remote objects, RMI provides the necessary mechanisms for loading an object's code, as well as for transmitting its data. The server calls the registry to associate (or bind) a name with a remote object. The client looks up the remote object by its name in the server's registry and then invokes a method on it.

ADVANTAGES OF RMI

One of the important features of RMI is its ability to download the byte codes (or simply code) of an object's class even though the class is not defined in the receiver's virtual machine. The type and behaviour of an object, previously available only in a single virtual machine, can be transmitted to another, virtual machine. RMI passes objects by their true type, and hence the behaviour of those objects is not changed, when they are sent to another virtual machine. This allows

new types to be introduced into a remote virtual machine, thus extending the behaviour of an application dynamically.

RMI is made up of interfaces and classes. The methods used in RMI are defined using the interfaces which are implemented by the classes. In a distributed application some of the implementations are assumed to reside in different virtual machines.

Objects that have methods that can be called across virtual machines are remote objects. An object becomes remote by implementing a remote interface, which has the following characteristics. A remote interface extends the interface java.rmi.Remote. When the object is passed from one virtual machine to another, Instead of making a copy of the implementation object in the receiving virtual machine, RMI passes a remote stub for a remote object. The stub acts as the local representative, or proxy.

The caller invokes a method on the local stub, which is responsible for carrying out the method call on the remote object. A stub for a remote object implements the same set of remote interfaces that the remote object implements. This allows a stub to be cast to any of the interfaces that the remote object implements. However, this also means that only those methods defined in a remote interface are available to be called in the receiving virtual machine.

DEFINING REMOTE INTERFACE

A remote interface specifies the methods that can be invoked remotely by a client. Clients program to remote interfaces, not to the implementation classes of those interfaces. Part of the design of such interfaces is the determination of any local objects that will be used as parameters and return values for these

methods. In case of any of these interfaces or classes being not available, the user has to define them

IMPLEMENTING THE REMOTE OBJECTS

Remote objects must implement one or more remote interfaces. The remote object class may include implementations of other interfaces (either local or remote) and other methods (which are available only locally). If any local classes are to be used as parameters or return values to any of these methods, they must be implemented as well.

IMPLEMENTING THE CLIENTS

Clients that use remote objects can be implemented at any time after the remote interfaces are defined, including after the remote objects has been deployed.

WORKING OF AN RMI APPLICATIONS

The working of RMI applications is based on accessing the remote object. A remote object can be defined as an object associated with methods hat can be called from another java virtual machine. In this mechanism the application that access to the remote object is treated as client application and the application that implements that object is treated as a server application. Thus an RMI application can be satirized into two parts.

1. Server side application
2. Client side application

SERVER SIDE APPLICATION

The first file is an interface that declares the methods, which are accessed remotely. The purpose of making an interface is to enable the client to access the methods of an interface with the help of its reference. The second file creates a class and the binds that object in RMI registry. An RMI registry is the naming server, which allows the remote request to be redirected to an object, which is bind inside it.

CLIENT SIDE APPLICATION

On a client side, a file is created that creates a class access that remote object through RMI registry and invokes the remote methods.

CREATING RMI SERVER

The first side to create an RMI application is to create server side application. For server side application, the first thing to create is an interface that defines the methods, which are accessed by the remote clients.

COMPILE SOURCES AND GENERATE STUBS

This is a two-step process. In the first step the user uses the javac compiler to compile the source files, which contain the implementation file, interfaces, the server program and the client program. In the second step you use the rmic compiler to create stubs for the remote objects. RMI uses a remote object's stub class as a proxy in clients so that clients can communicate with a particular remote object.

5.6 SCREENSHOTS:

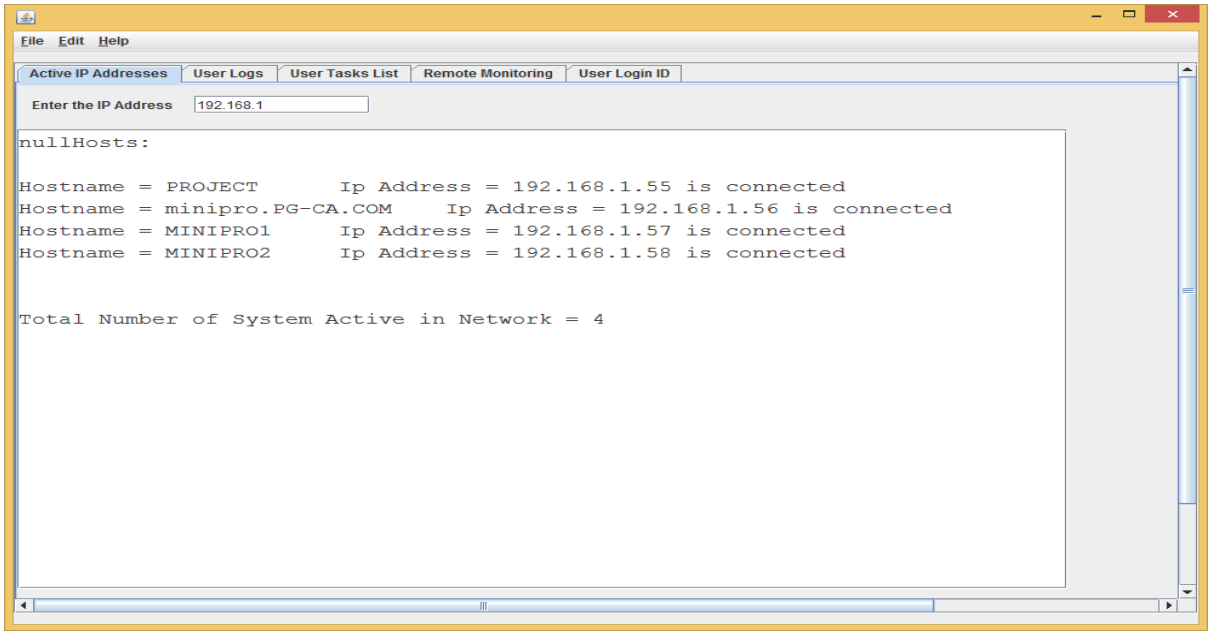

Fig 5.2 Active Client machines

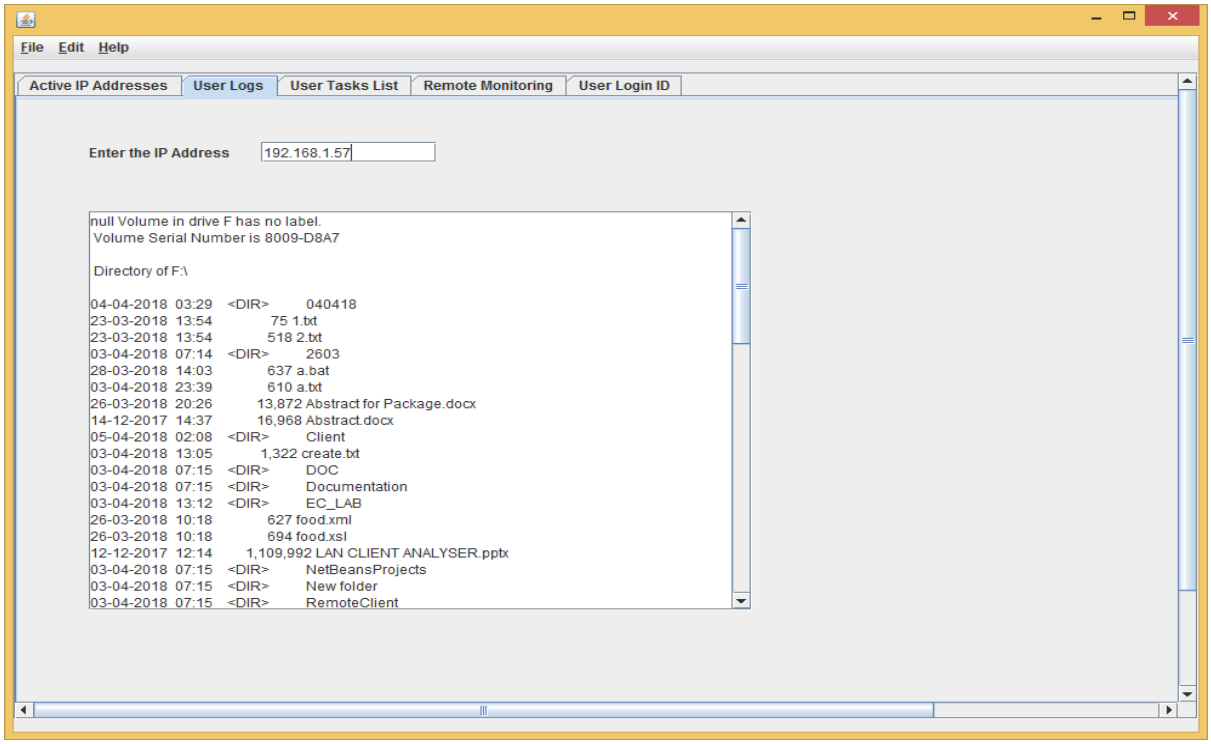

Fig 5.3 User Logs

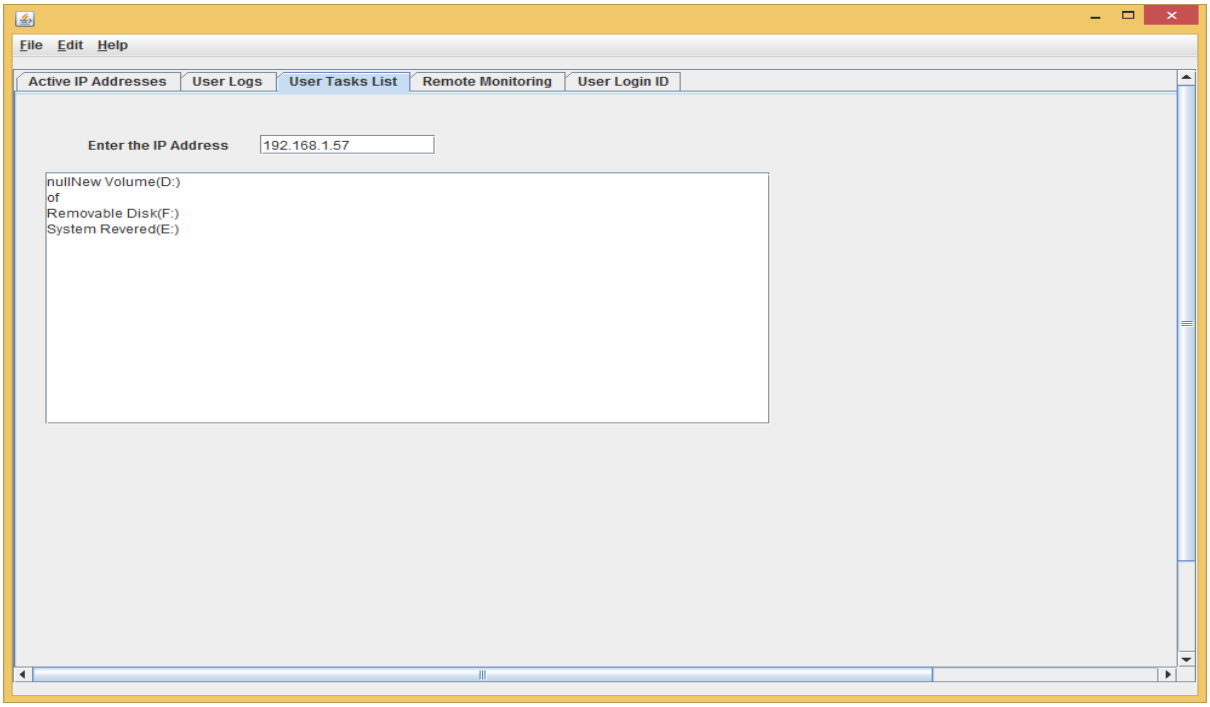

Fig 5.4 User Task List

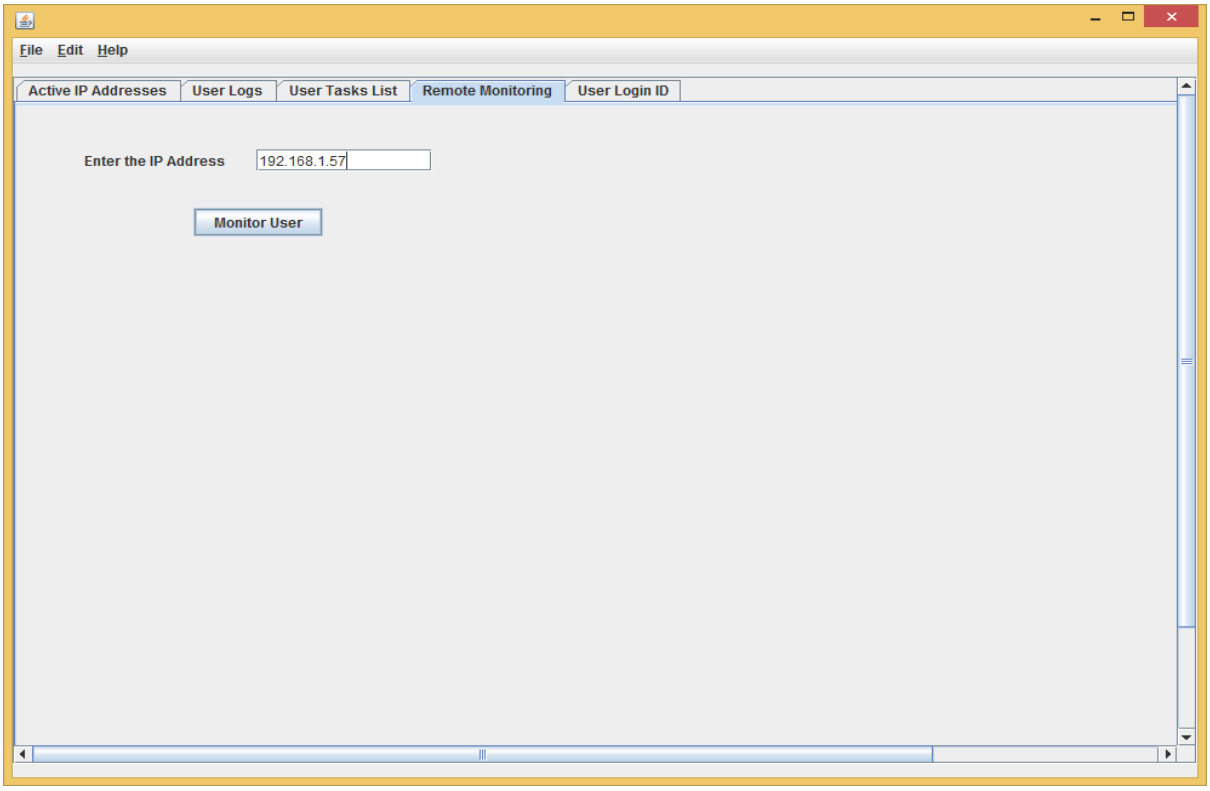

Fig 5.5 Remote Method Invocation

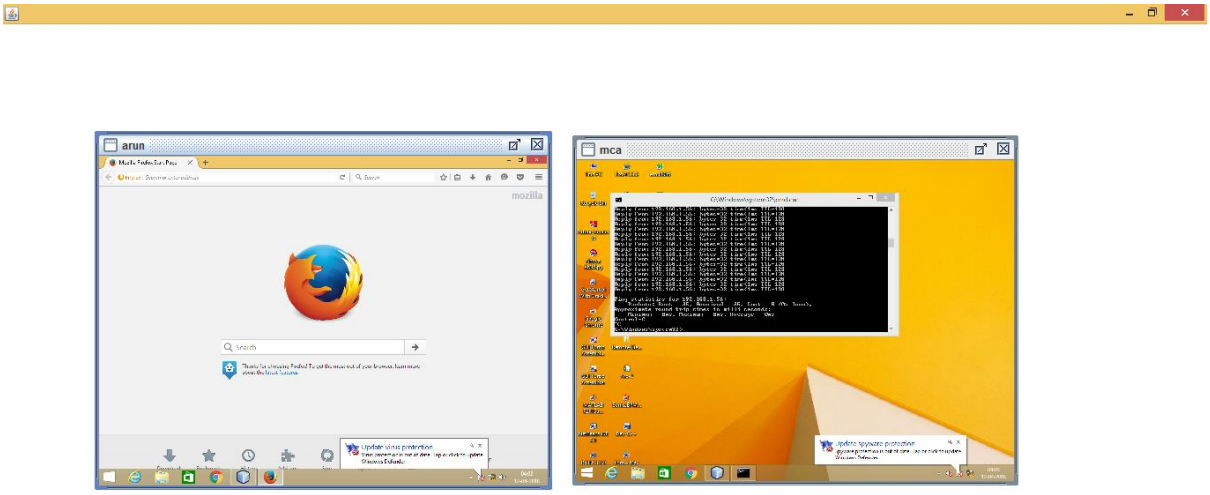

Fig 5.6 Remote Monitor Capture

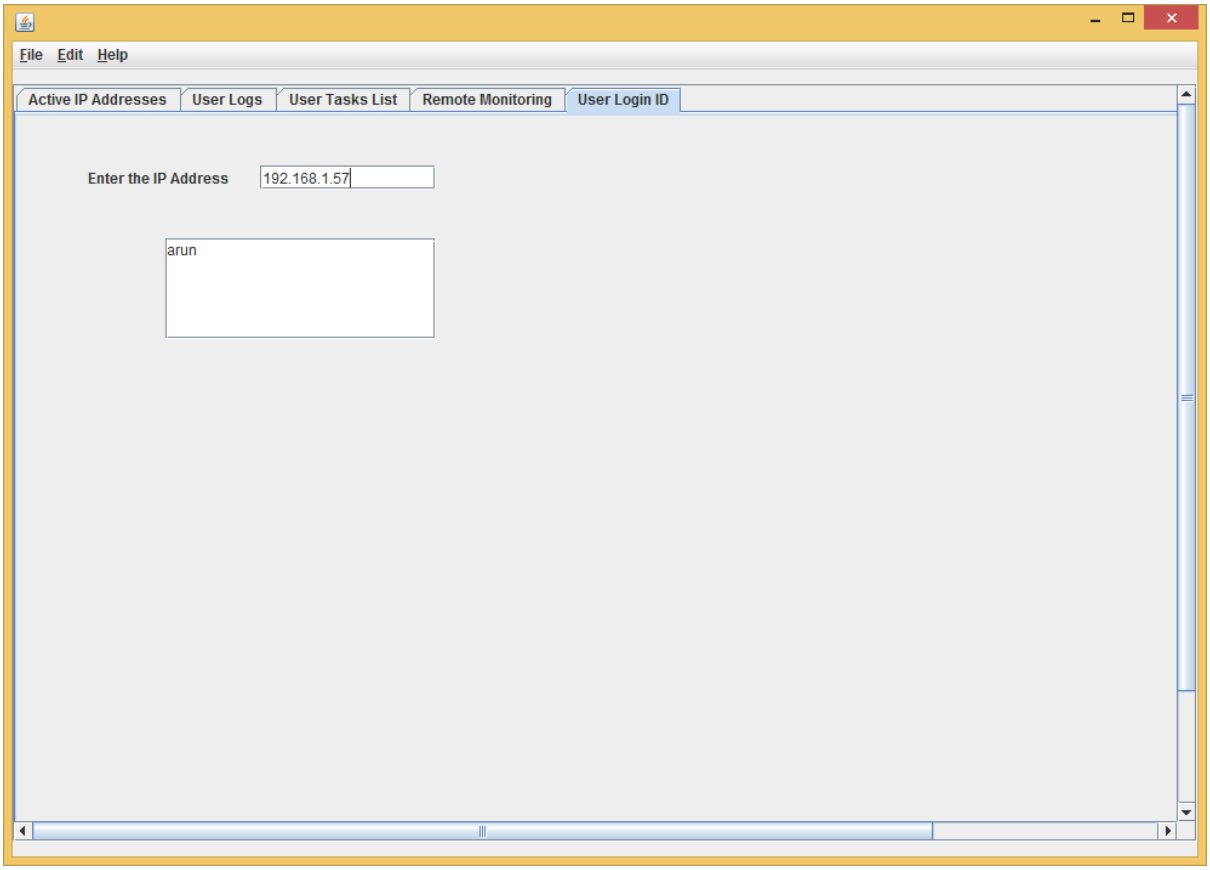

Fig 5.7 User Login ID

CHAPTER 6

CONCLUSION

This Project is used to monitor client activities within Network. Administrator can view the client machine details like username, current working status, on screen. This tool is used to identify malpractice activities and Log files. In Future, It also provides knowledge about client server technology that will be great demand in future. Based on this project better opportunities and guidance in future in developing projects independently.

CHAPTER 7

BIBLIOGRAPHY

https://www.wireshark.org/docs/wsug_html_chunked/ChCapInterfaceRemoteSection.html

https://www.microsoft.com/en-in/download/details.aspx?id=5842

https://www.microsoft.com/en-us/download/confirmation.aspx?id=269

https://en.wikipedia.org/wiki/Windows_Server_2012

http://virtualrouter.codeplex.com/

https://www.microsoft.com/en-us/evalcenter/evaluate-windows-server-honolulu

https://www.petri.com/windows-server-2012-as-domain-controller