

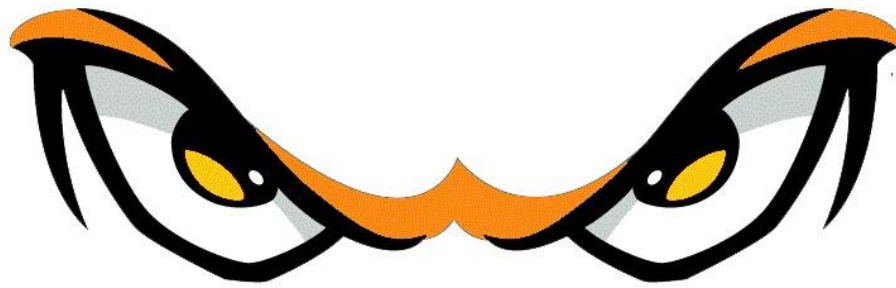
PROJECT   
TSUNAMI

USER



PROJECT   
TSUNAMI

MANUAL



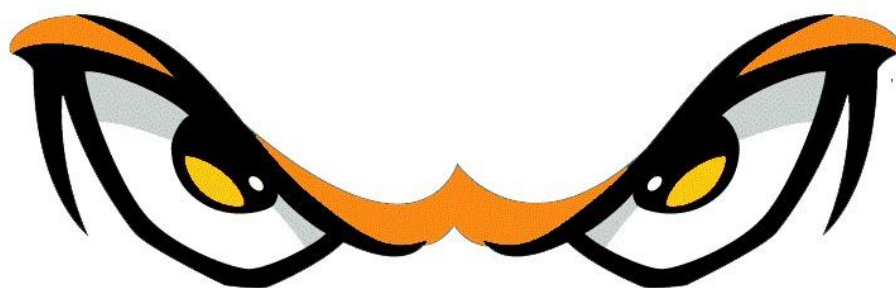
# PREFACE

This user documentation contains details about compiling, executing and using our software that we have developed as our end of semester project of Object Oriented Programming. We chose to develop a spy-ware consisting of a Windows-based Trojan that will act as a Remote Administration Tool. It can be used to remotely connect and manage a single or multiple computers and perform unwanted actions ranging from basic data collection to file erasure and uploading, restart and shutdown etc on it.

## **Developers**

Atiqa Zafar  
Nauman Ali  
Shahid Khaliq  
Zaryab Khan





# TABLE OF CONTENTS



1. Preface
2. Project Overview
3. Compiling
4. Executing
5. User Interface
  - a. Main Window
  - b. Connecting a Victim
  - c. File Manager
  - d. Key Logger
  - e. Screenshot Capture
  - f. Chat
  - g. Power Options
  - h. URL Opener
  - i. Exit
6. About the Developers
7. Contact the Developers



Project Tsunami is a spy-ware consisting of a Windows-based Trojan that will act as a Remote Administration Tool. RAT is used to remotely connect and manage a single or multiple computers and perform unwanted actions ranging from basic data collection to file erasure and uploading, restart and shutdown etc.

Project Tsunami targets the following customers:

- 1) Parents who want to keep a track of their children's activity
- 2) Government Agencies who want to monitor suspicious activities of certain individuals
- 3) Other users who want to gain access to other's computers

It aids in gathering information about a person or organization without their knowledge. It is a non-self-replicating malware which appears to be a game but instead allows unauthorized access to the target's computer.



### Compiling:

The code can be compiled in Qt 5+. Qt can be downloaded from: <http://qt-project.org/downloads>. After you've downloaded it, you've got to install it using the setup. Once installed, you will have to open the .pro file which is the project file. We have uploaded this with our source code. Once the project is open, you can compile it by clicking the build button.



### Executing:

Once we have build the project we'll obtain an exe file deep in the Qt directories. The path can vary but in our case it was:

















**C:\Qt\Qt5.0.2\Tools\QtCreator\bin**

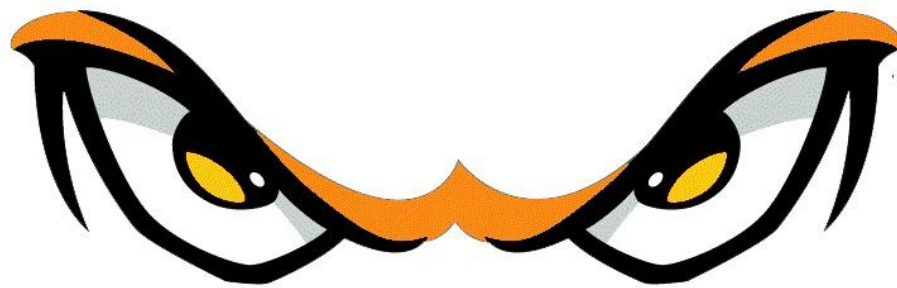
In this bin folder you'll find all the projects you've built using qt creator. Open the folder which matches your projects name. In it there will be two more folder.

1. debug
2. release

You'll find the exe in one of these folders depending on weather your build was debug or release. (Can be set in project options)

This exe will only run in Qt Creator (since the path variables are set by default in Qt). To make this exe standalone, you have to include the dependencies in the folder too. You'll need 3 dlls for Webkit support, 2 for OpenGL support, 4 or 5 of Qts own dlls and a few dlls from Microsoft. In addition you'll need to include a plugins folder too with the required plugins. We will provide all of these files with our exe but here's a screenshot anyways:

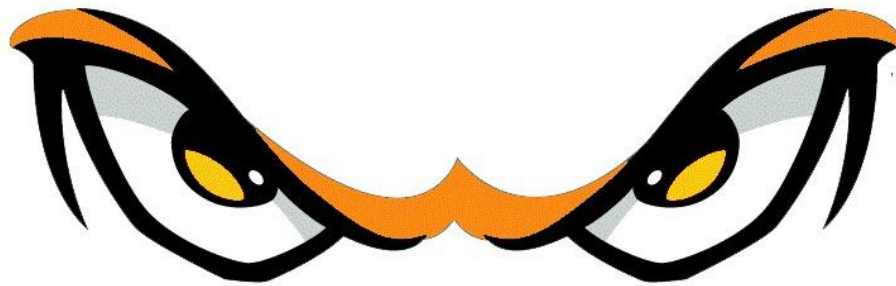
Name	Date modified	Type	Size
 imageformats	25-May-13 10:11 P...	File folder	
 platforms	25-May-13 10:11 P...	File folder	
 Client.exe	26-May-13 7:06 PM	Application	87 KB
 d3dcompiler_46.dll	05-May-13 1:50 PM	Application extens...	3,783 KB
 icudt49.dll	05-May-13 1:50 PM	Application extens...	17,536 KB
 icuin49.dll	05-May-13 1:50 PM	Application extens...	1,523 KB
 icuuc49.dll	05-May-13 1:50 PM	Application extens...	1,245 KB
 libEGL.dll	05-May-13 1:52 PM	Application extens...	66 KB
 libGLESv2.dll	05-May-13 1:52 PM	Application extens...	784 KB
 msvcp110.dll	26-Jul-12 3:22 PM	Application extens...	646 KB
 msvcr110.dll	26-Jul-12 3:22 PM	Application extens...	810 KB
 Qt5Core.dll	05-May-13 1:53 PM	Application extens...	4,178 KB
 Qt5Gui.dll	05-May-13 1:52 PM	Application extens...	3,484 KB
 Qt5Network.dll	05-May-13 1:52 PM	Application extens...	985 KB
 Qt5Widgets.dll	05-May-13 1:52 PM	Application extens...	5,025 KB
 Server.exe	26-May-13 5:05 PM	Application	192 KB



MAIN WINDOW







# CONNECT A VICTIM

The connect screen. First thing's first. We must connect to the client.



Clicking connect we get this screen:

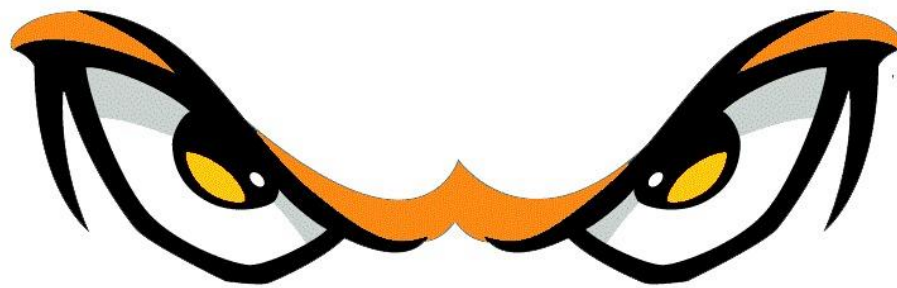


1. All connected clients are displayed.
2. We can choose one by double clicking once selected or clicking connect.

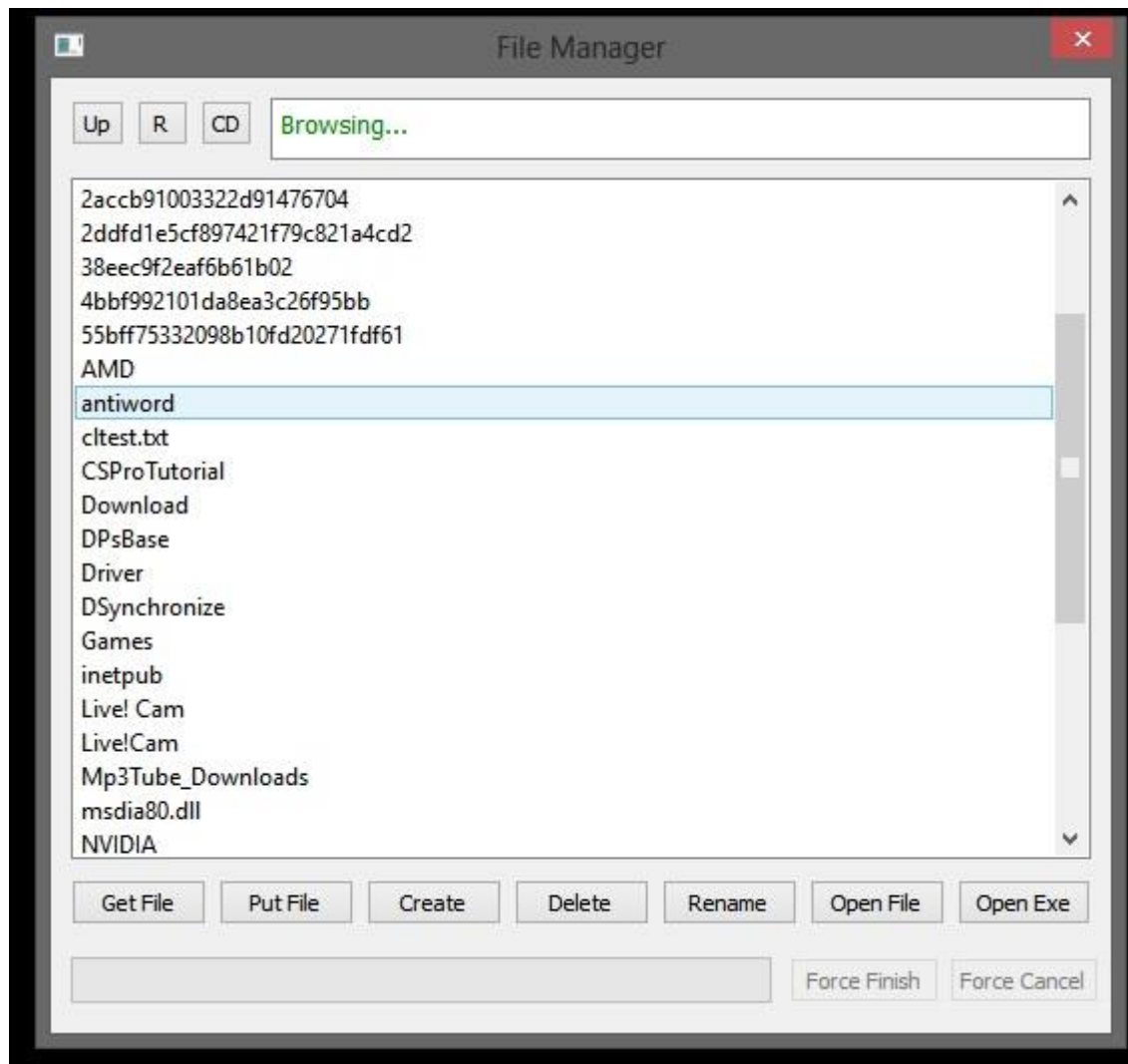
Once connected, we get this screen:



1. Disconnect: Disconnects from the client and pops up the connect screen
2. File Manager: View, edit, get, put files
3. Capture Screen: Get screenshots of victims screen
4. Keylogger: Live keystroke monitoring and we can also get the log, delete it or create a new one
5. We can chat with the victim
6. We can kill processes (like chrome) etc
7. We can open urls
8. We can shutdown their pc, restart it or lock it
9. We can also kill the client process itself



# FILE MANAGER

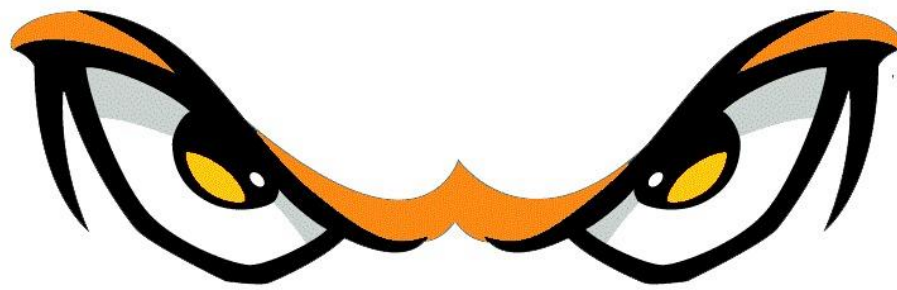


1.) Get files

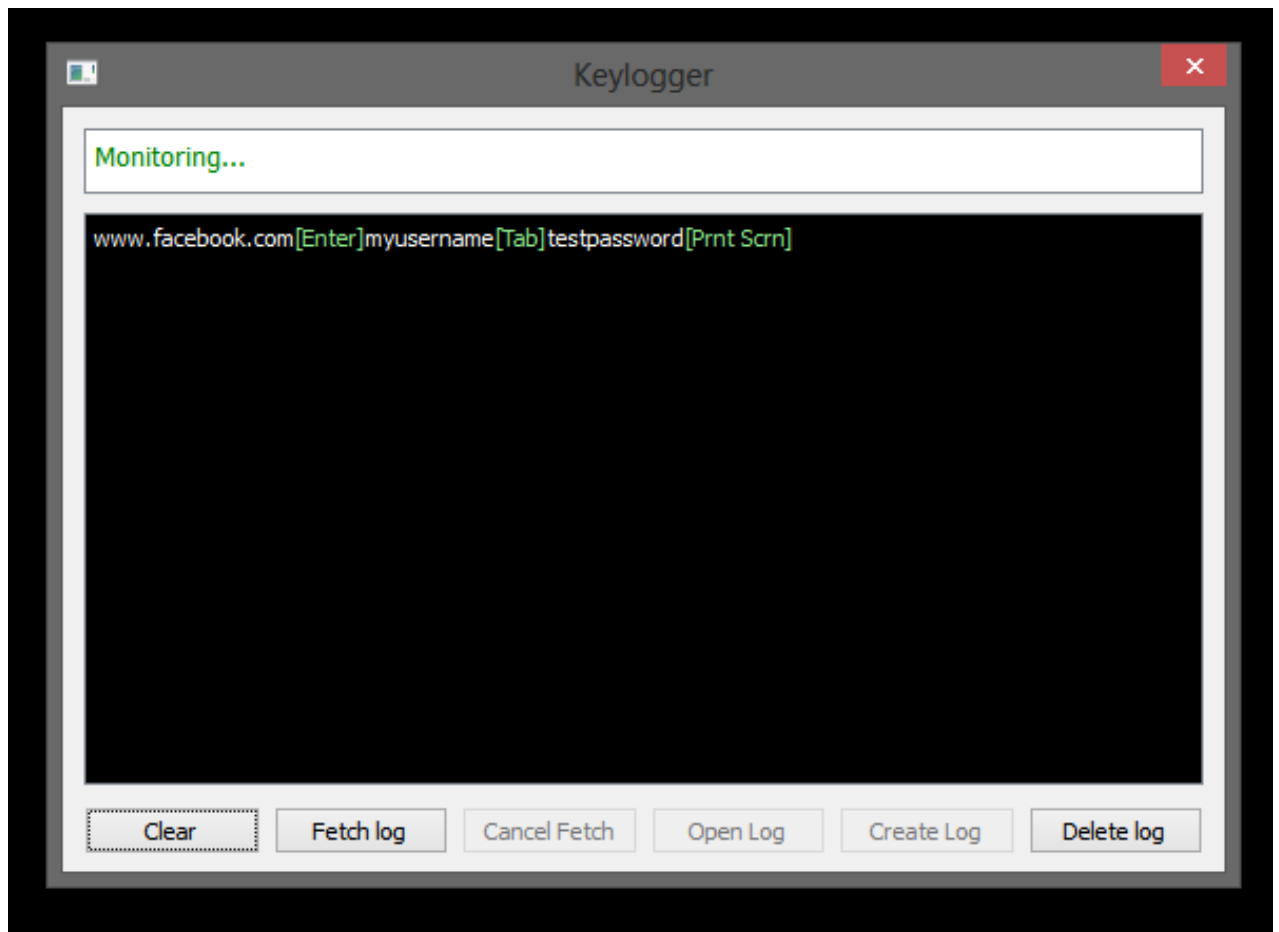
- 2.) Put files
- 3.) Create Folders
- 4.) Delete folders/files
- 5.) Rename folders/files
- 6.) Open files
- 7.) Run exes

In the top left corner we have three buttons

Move up(previous directory), Refresh and Change Directory(Can be done with double click too)

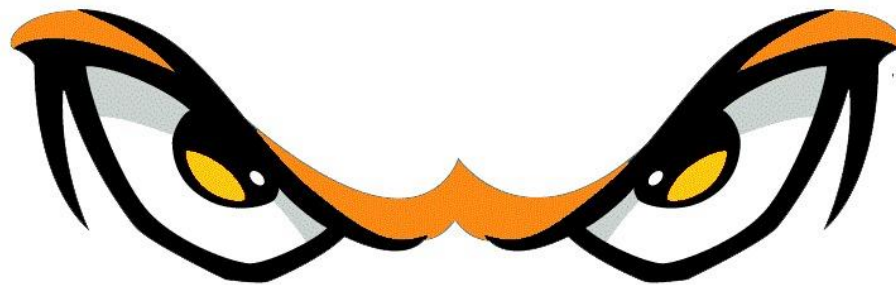


# KEY LOGGER

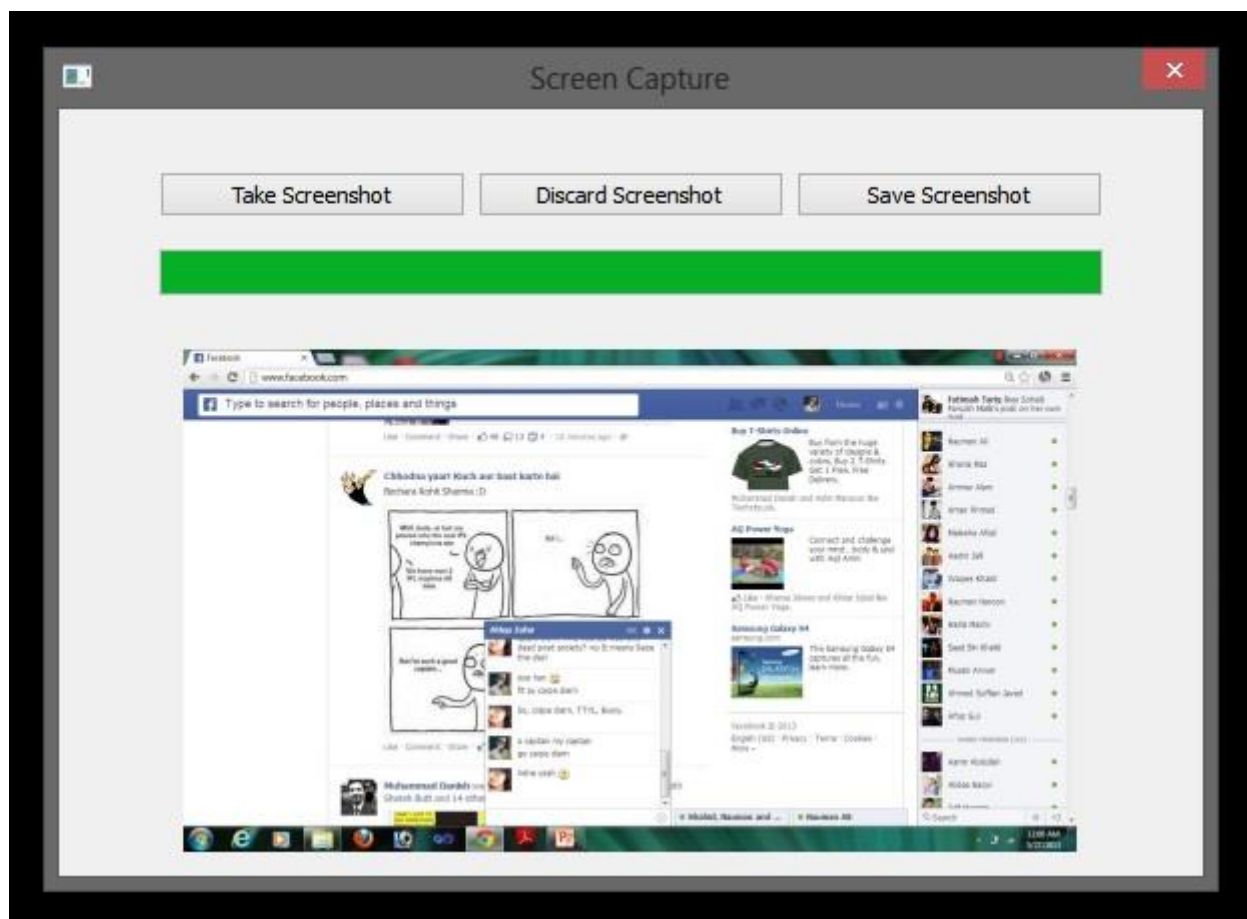


We can view live keystrokes. We can get the stored log from victims pc, delete it or create a new one.

We can also open the log once we fetch it.



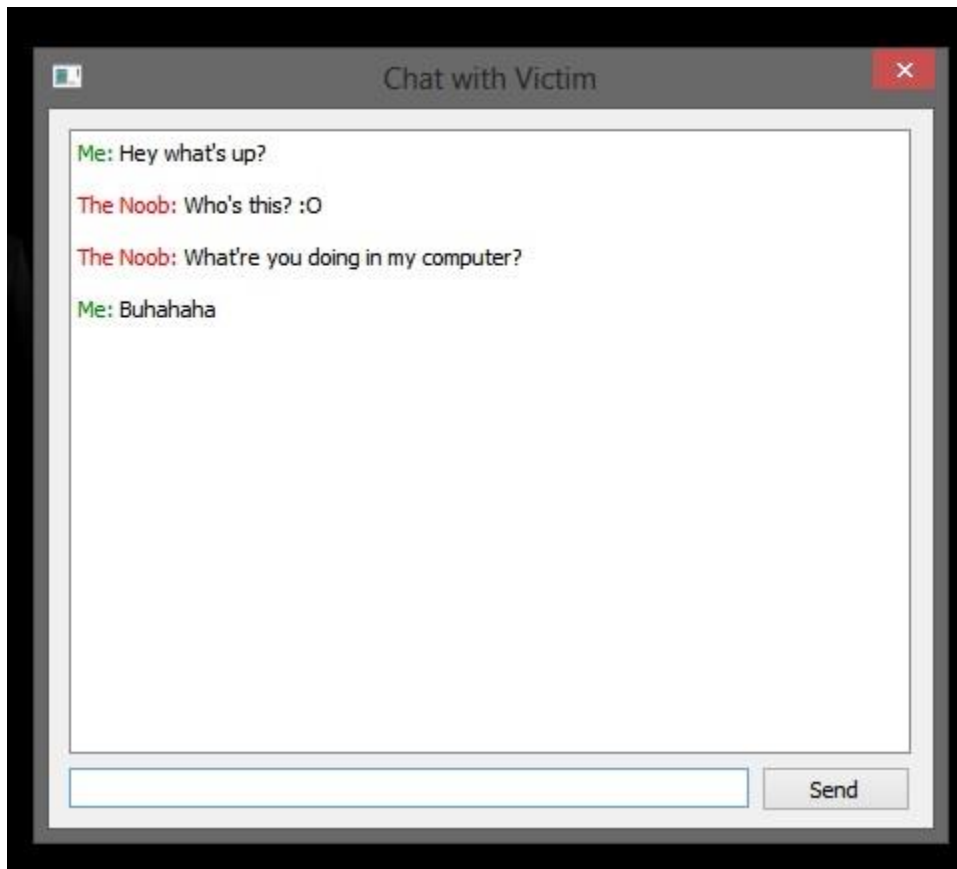
# SCREENSHOT CAPTURE



We can take a screen shot of victims pc and then save it or discard it



We can chat with the victim too... (Server side below)



(Client side below)





This window is full black. It always stays on top and is immovable. Its sticks at the centre of the screen and hasn't got an icon on the task bar.

