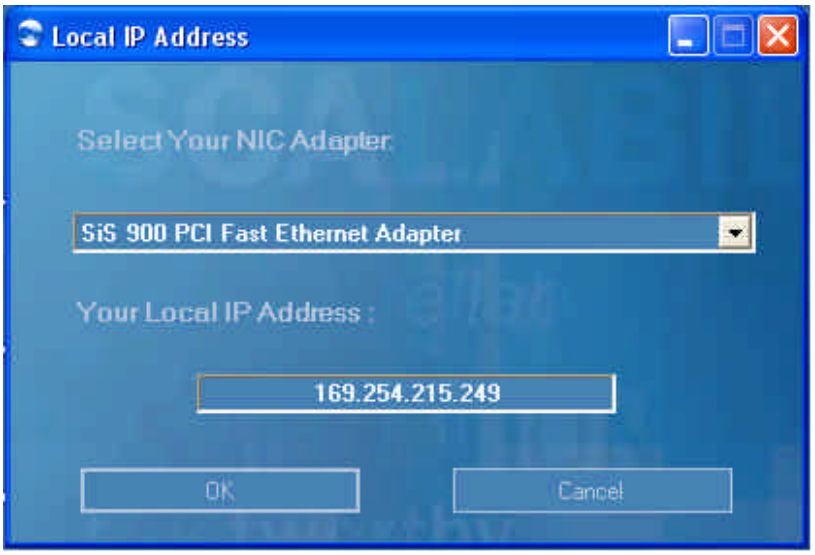
Chat Client Help Document

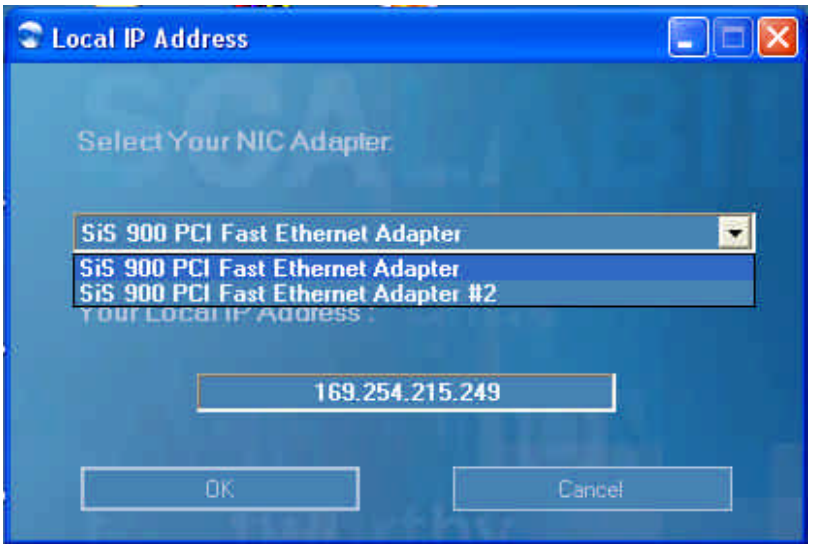
- Login Forms
  - Select Local IP Address
  - Login Form
- File Menu
  - Encrypted Dialog
  - Options Form
- Connection Menu
  - Establish Connection
  - End Connection
  - Show Connected Terminals
- Private Menu
  - Private Message
  - Send File
- Sniffer Menu
  - Simple Sniffer
  - Command Line Sniffer

Local IP Address Form :

When you start the program, it will ask you to determine the IP address you want to bind your program to.



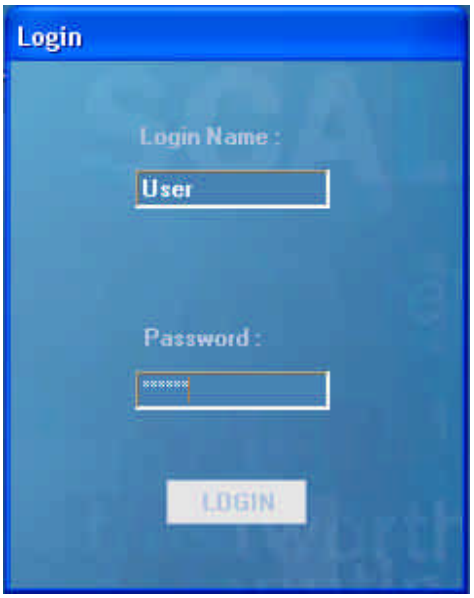
Choose from the NIC adapters available to you, once you choose one, the associated IP address to that NIC will be shown in the IP address text box.



If you do not want to bind to this IP, or your IP is not shown in the list you can add it manually. But remember that you must enter it in the right form.

Login Form :

After choosing the IP address, a Login form will pop up. as the figure below :

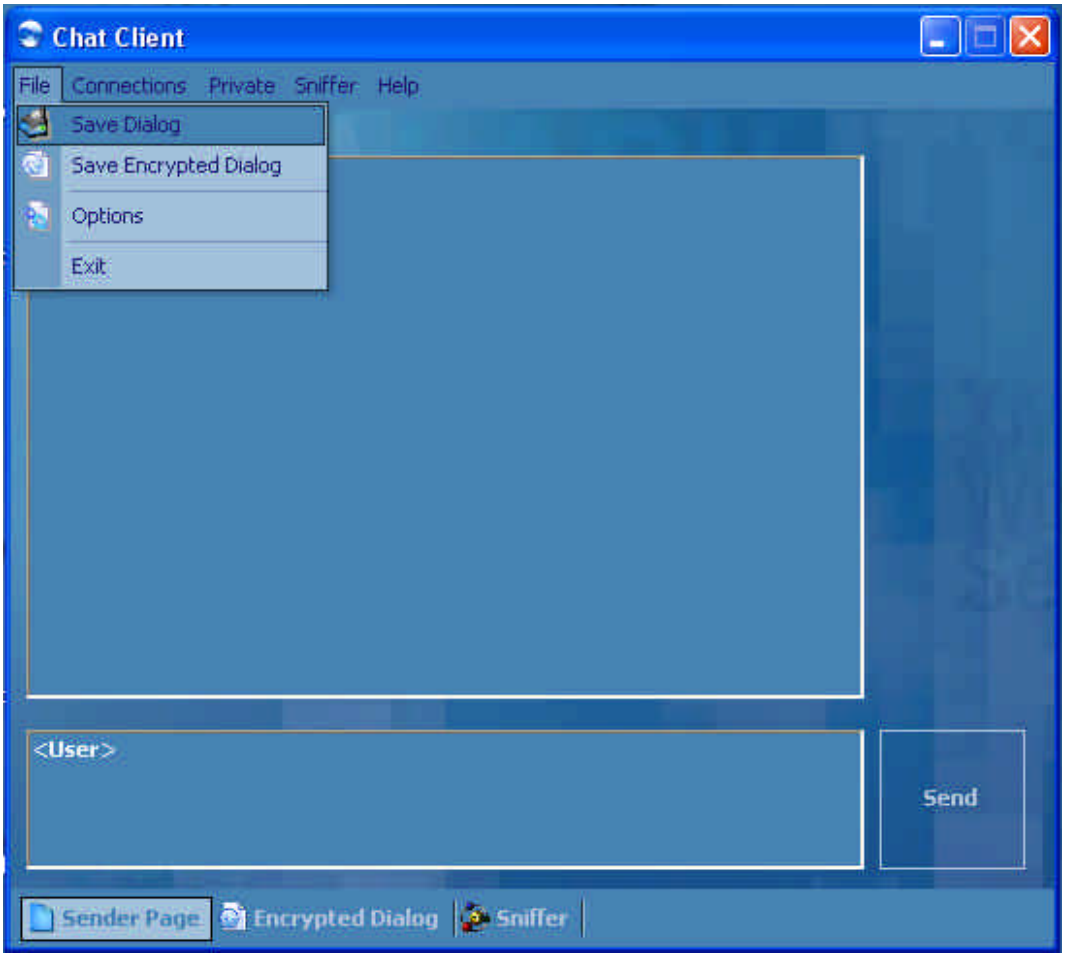


You can choose any Login Name you want, this will be used as your nick name in the chat environment.

After choosing the Login Name, enter a password to be used for encrypting your data. By default this will be used as a seed for auto generated secret key, but as you will see in the option form you will be able to use this password string as your secret key.

File Menu :

In the main form for the program, the first menu group is the file menu as shown below:



This menu group contains the following menu commands :

- **Save Dialog .**

  This command allow you to save your dialog in .txt and .rtf formats file.

- **Save Encrypted Dialog**

Each dialog has its encrypted version which allow the user to see how his dialog was sent and received using ARTProtocol.

Click Here for more information about encrypted dialog.

- **Options**

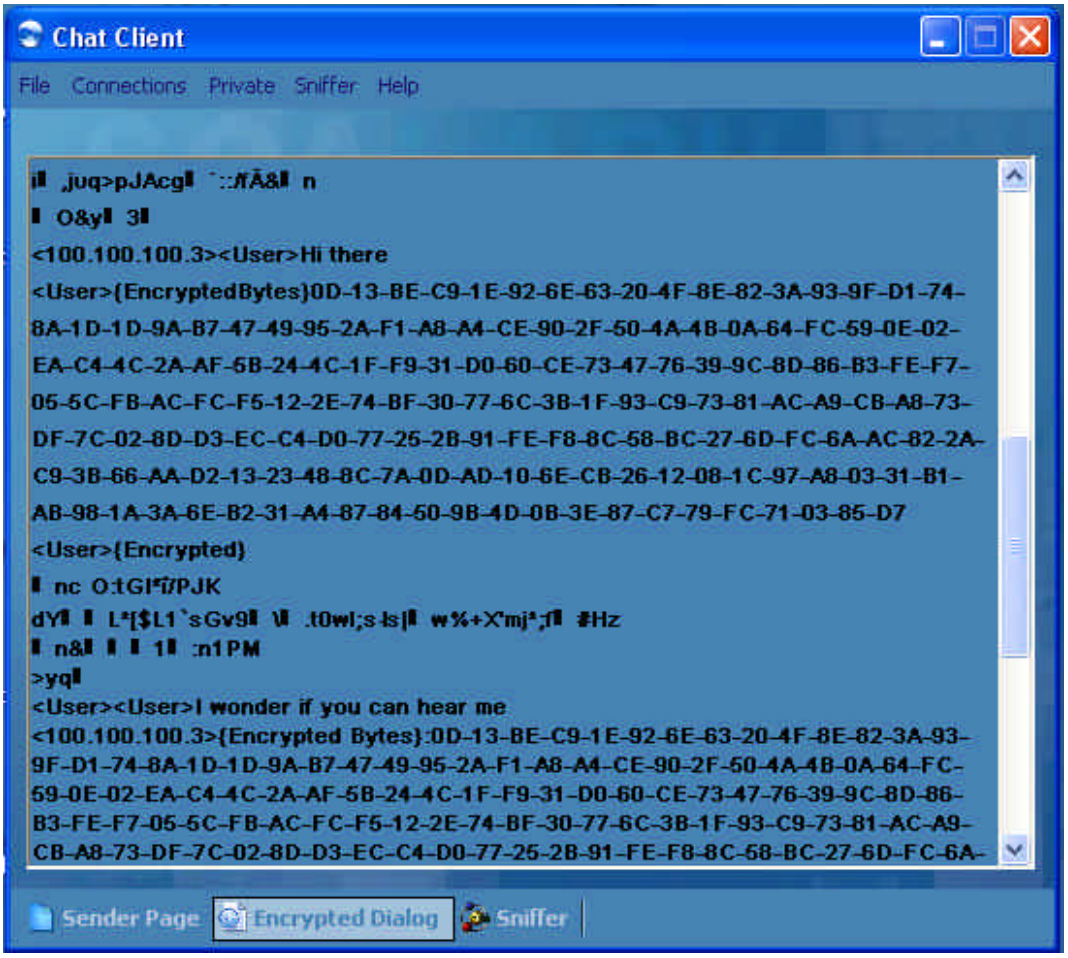
You can using this command to open a form which allow you to change your settings . For more Click Here.

- **Exit**

To exit the program, all the connected terminals will be notified that you have terminated the connections with them.

Encrypted Dialog :

Encrypted Dialog tab show the user how its normal dialog is sent out in the network.



The output is in three forms :

- **Encrypted Bytes**

  Shows a sequence of bytes that represents the encrypted data.

- **Encrypted Data**

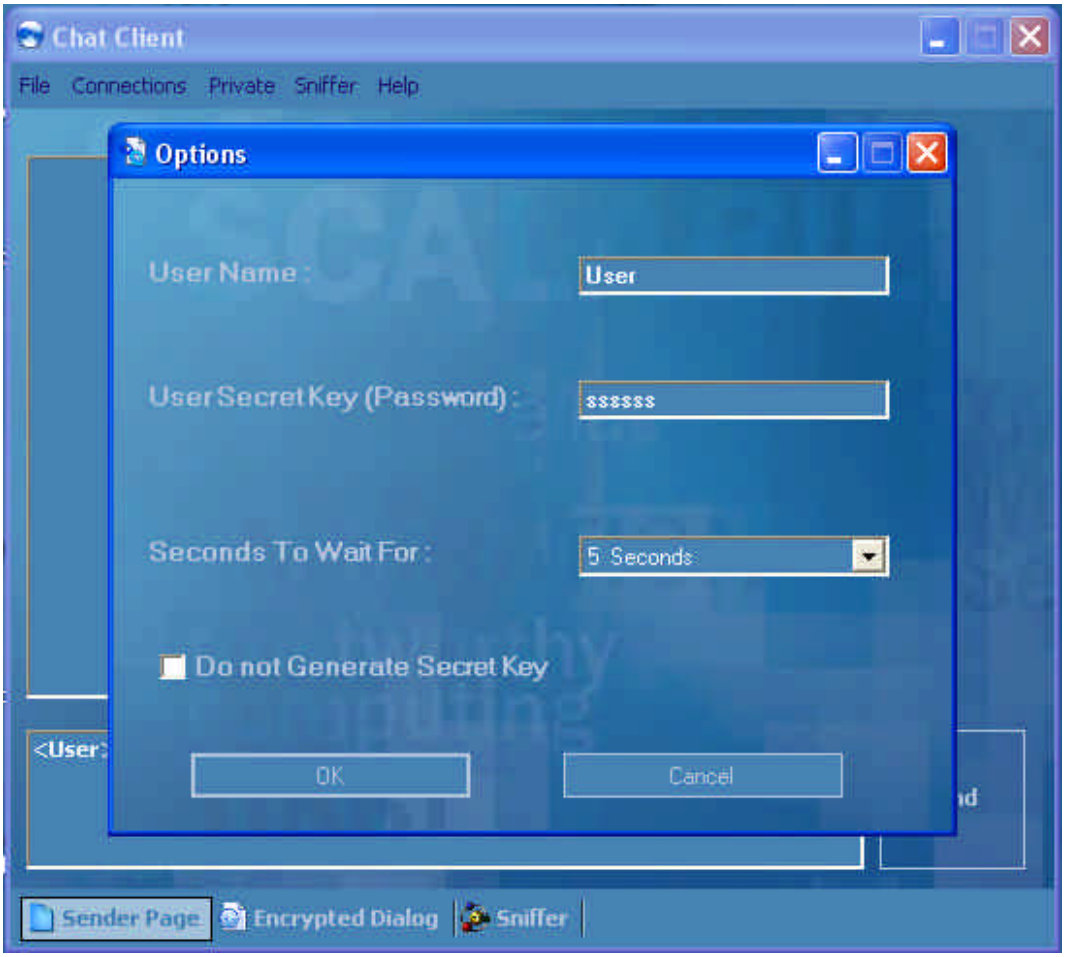
  Show the encrypted data as a string.

- **Data**

  Data after decryption.

Options Form :

In this form, the user has the ability to change his/her settings. Lets take a look at this form:



As you can see you have the following abilities :

- **Change your User Name**

This is the same Login Name you have entered in the Login Form.

- **Change your Secret Key**

Change your Password, either for changing the seed for the auto generated Secret Key, or changing you real Secret Key depending on your settings.

- **Change Seconds To Wait For Variable**

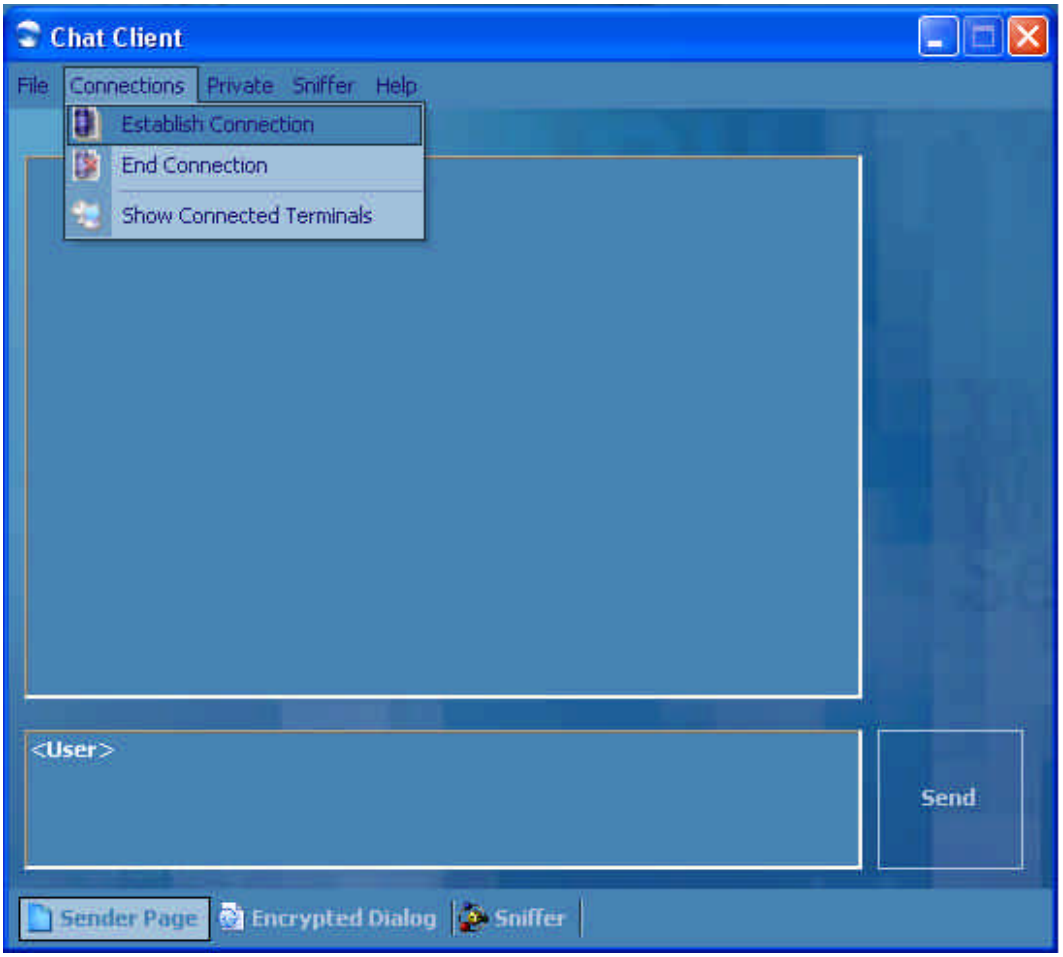
This variable is used for Establishing connections and Receiving connections, and it represents the time the terminal wait for other terminal response before deciding that the connection is broken. This help for low bandwidth connection situation. The default Number of Seconds is 5 and the maximum is 60 (1 Minute).

- **Check or Uncheck "Do not Generate Secret Key" box**

If this box is checked the program will use your User Password as a Secret Key in the encryption process. If not, User Password will be used as a seed for 128 Bytes long auto-generated password. The default setting is Unchecked.

Connections Menu :

The second group of commands menu is Connections Menu.



As shown in the figure above it has three menu commands

- **Establish Connection**

Used to establish connection with other terminals by providing its IP address.

- **End Connection**

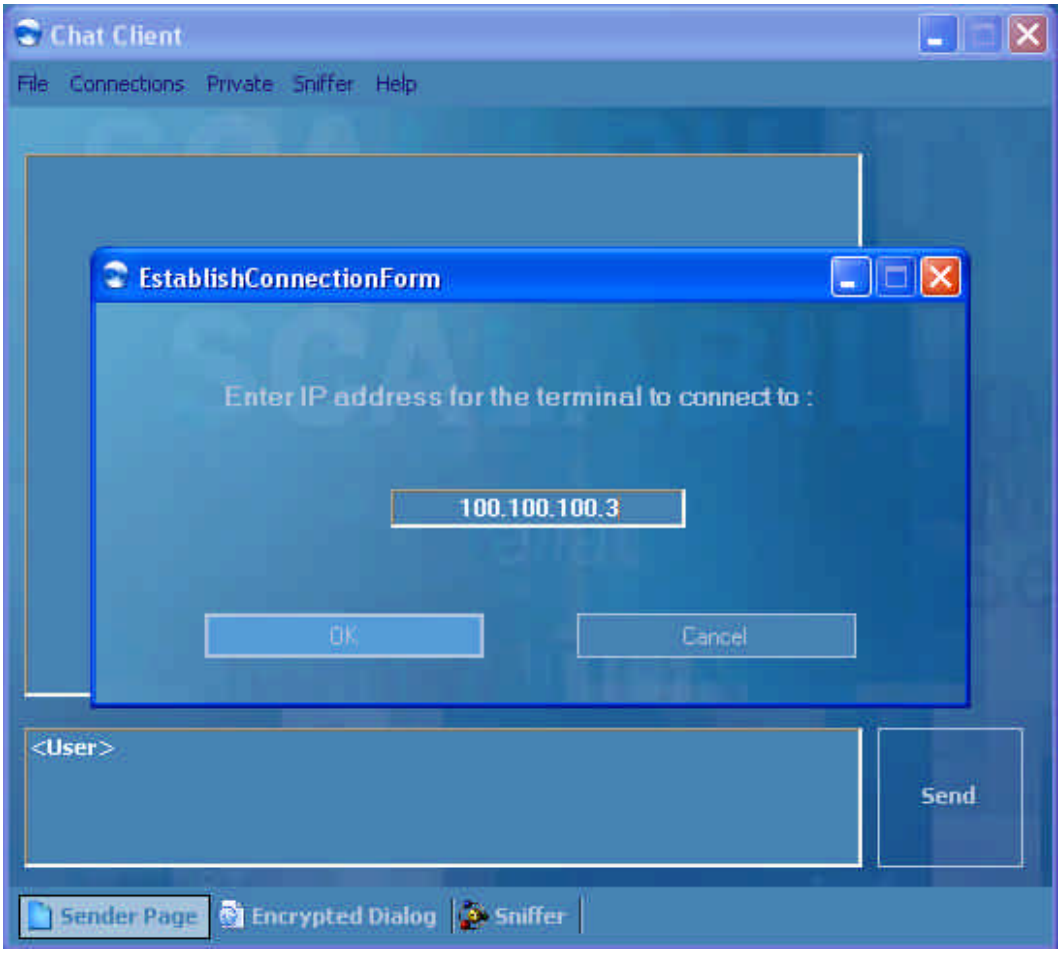
Used to end connection with a terminal.

- **Show Connected Terminals**

This option is used to display the connected terminals to the user terminal.

Establish Connection :

This option is essential to connect to other terminals by providing their IP addresses.

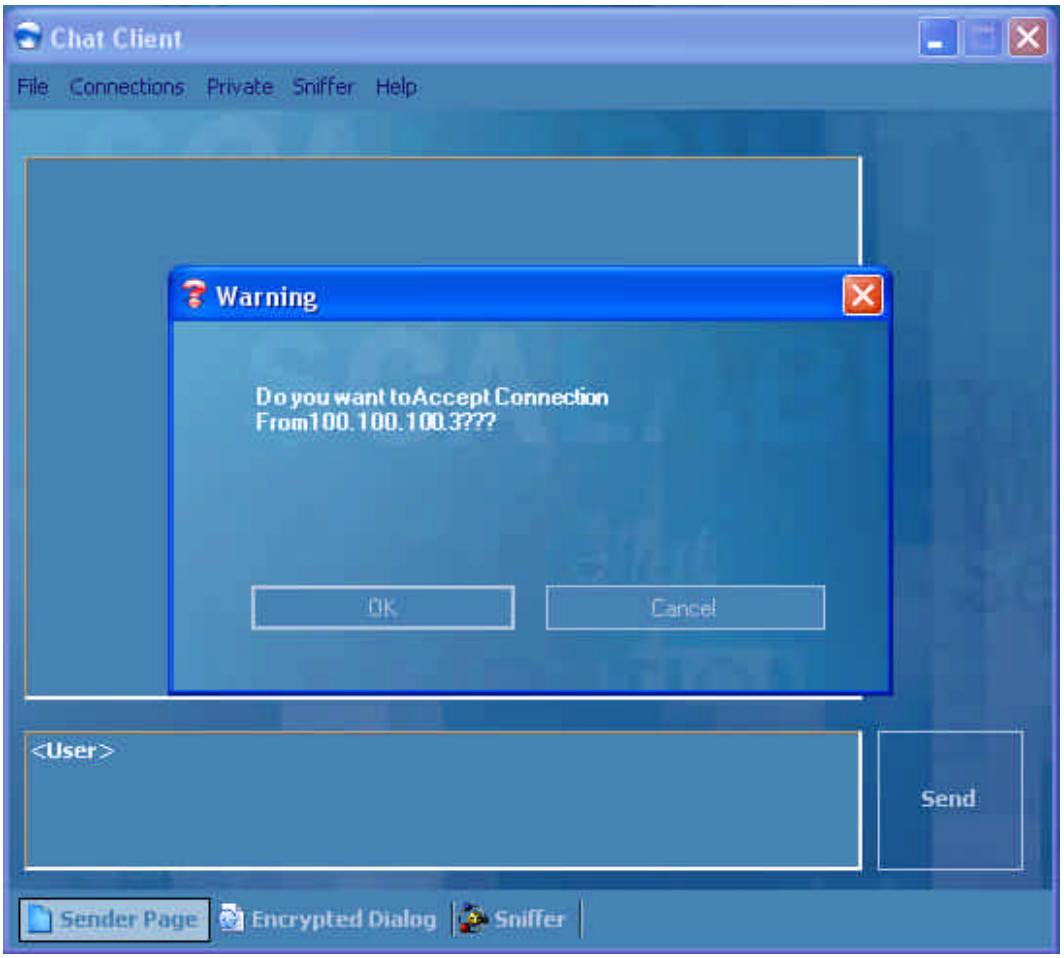


Note: you must enter the IP address in the right format.

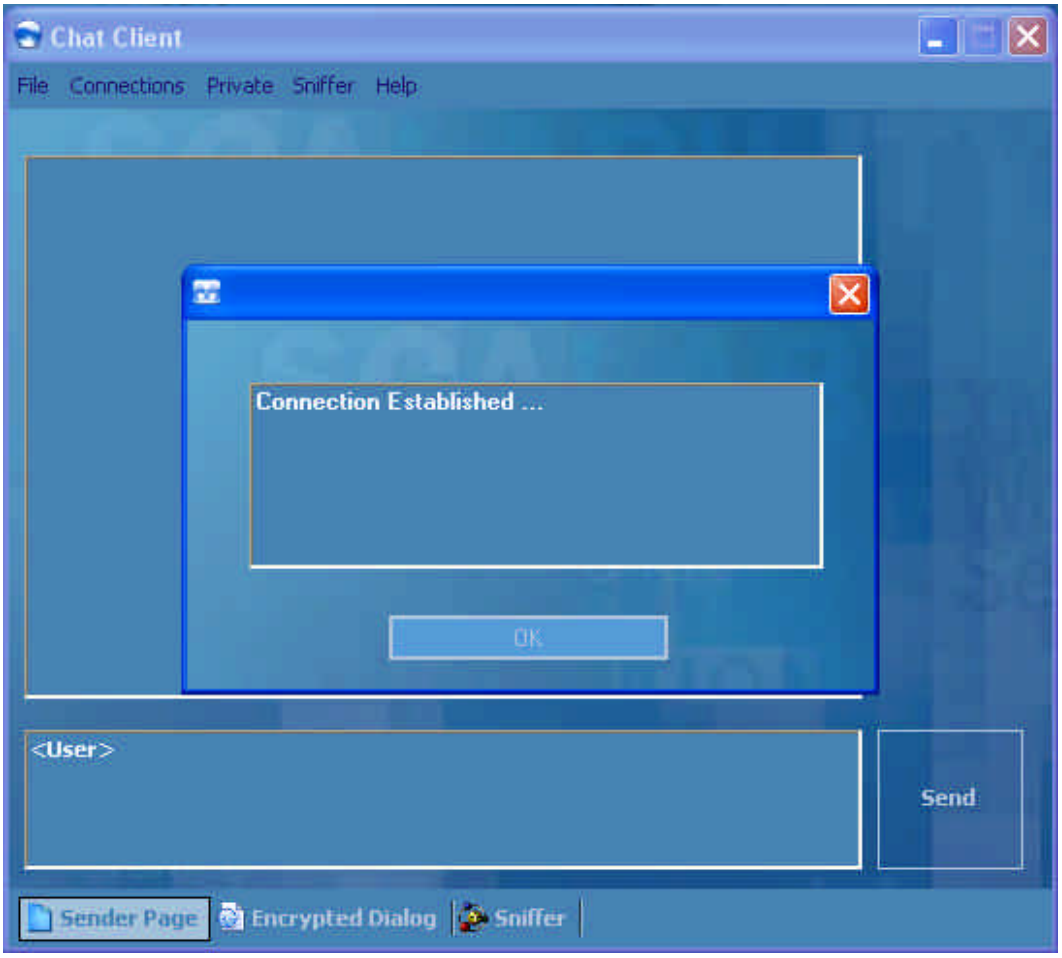
After entering the IP address of the destination terminal, two scenarios are possible :

Successful operation.

This case happens if the destination terminal is running this program, then it will get a message just like the below one:



if the destination terminal choose to accept the connection, you will get a message box as in the figure below:



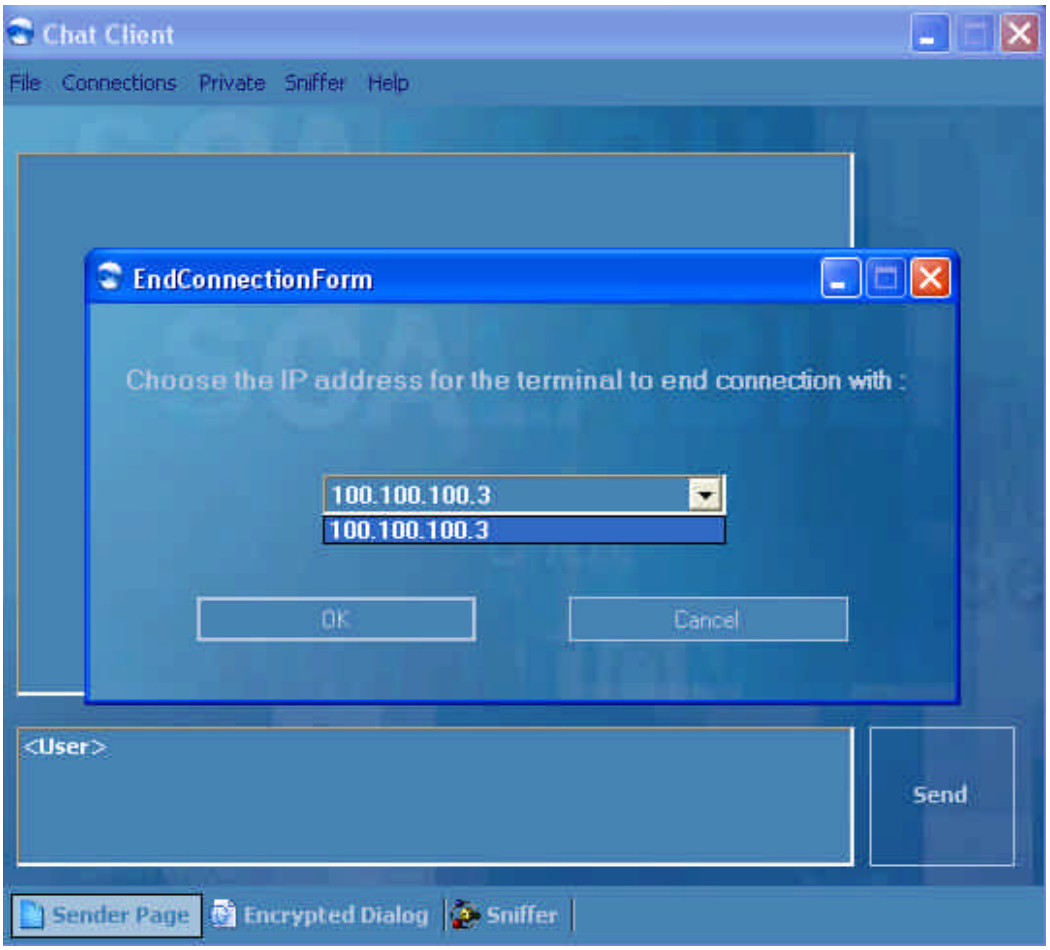
Failed Operation

Else, if it did not choose to accept the connection then an error message will be shown to indicate that the connection failed and it will ask you if you want to retry the connection process.

End Connection Form :

Obviously, this option is used to end connection with one of the terminals that is connected to the user terminal.

A form will be displayed as the following one to ask you to chose the terminal you wish to end connection with :

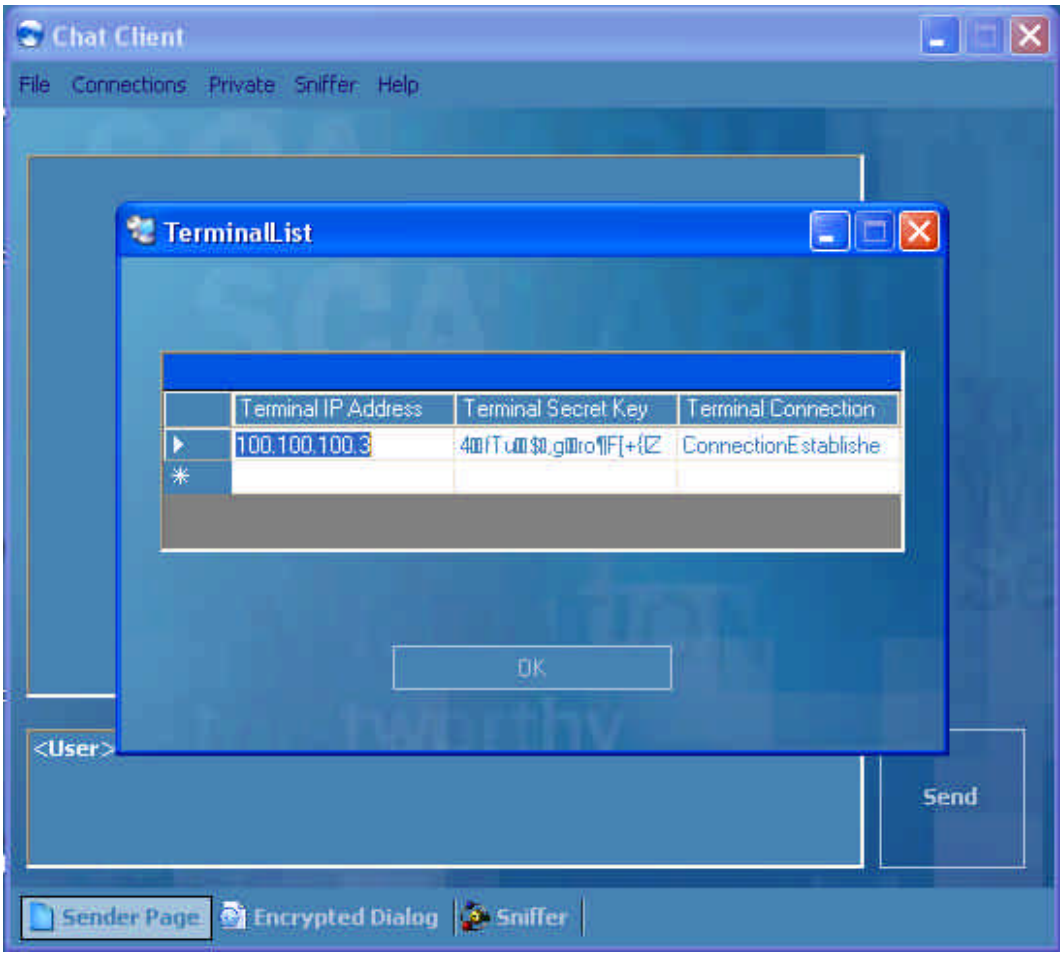


Once you choose the terminal IP address, an EndConnection message will be sent to the terminal to tell it that you has ended the connection with it.

Show Connected Terminals Form :

This form will show the user the connected terminals to its terminal. and the Connection state of this terminal along with its secret key if it is available.

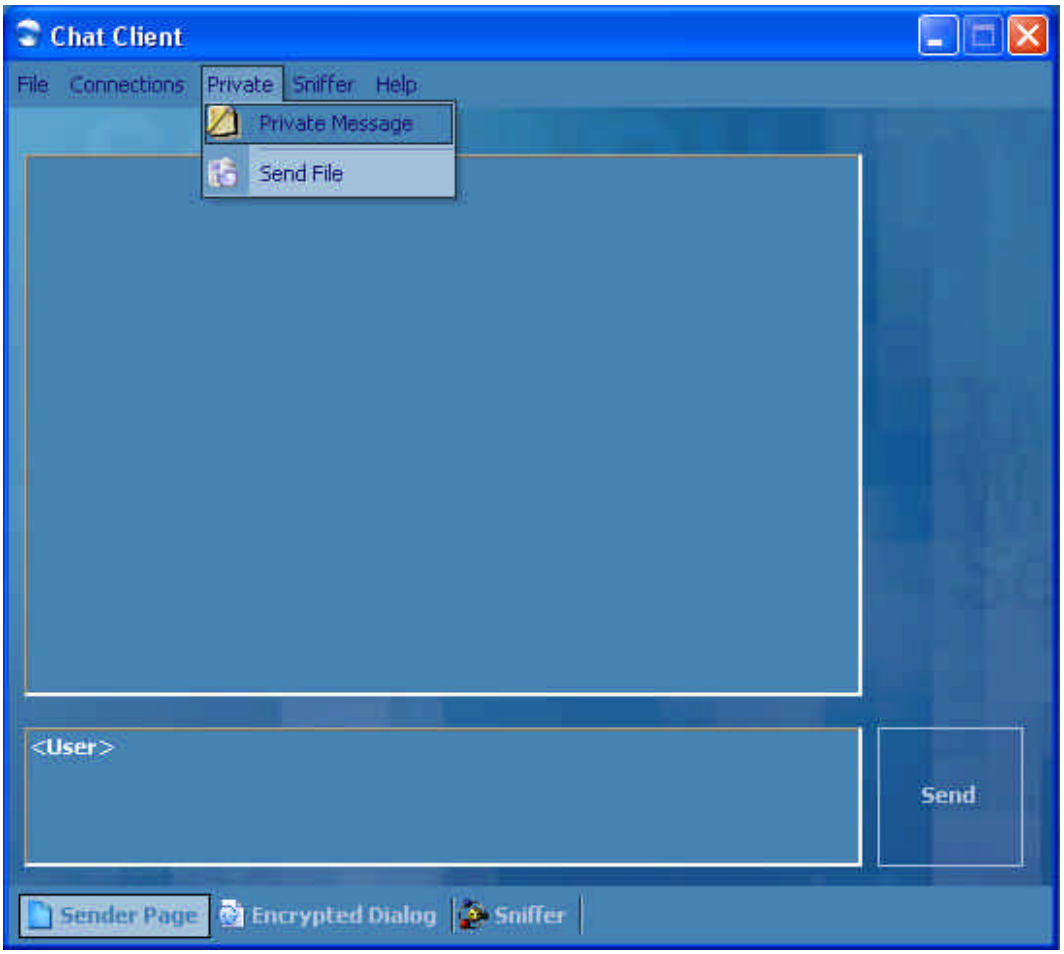
See the figure below :



As you can see form the figure, the terminal with address 100.100.100.3 is connected to you since it has Connection Established state. And this terminal is using the Secret Key shown in the column "Terminal Secret Key" to exchange encrypted data.

Private Menu :

This group of menu command give the user the ability to send data to a specific user (i.e. it dose not send the data to all connected user like normal chat message controller do).



This menu consists of two menu commands:

- **Private Message**

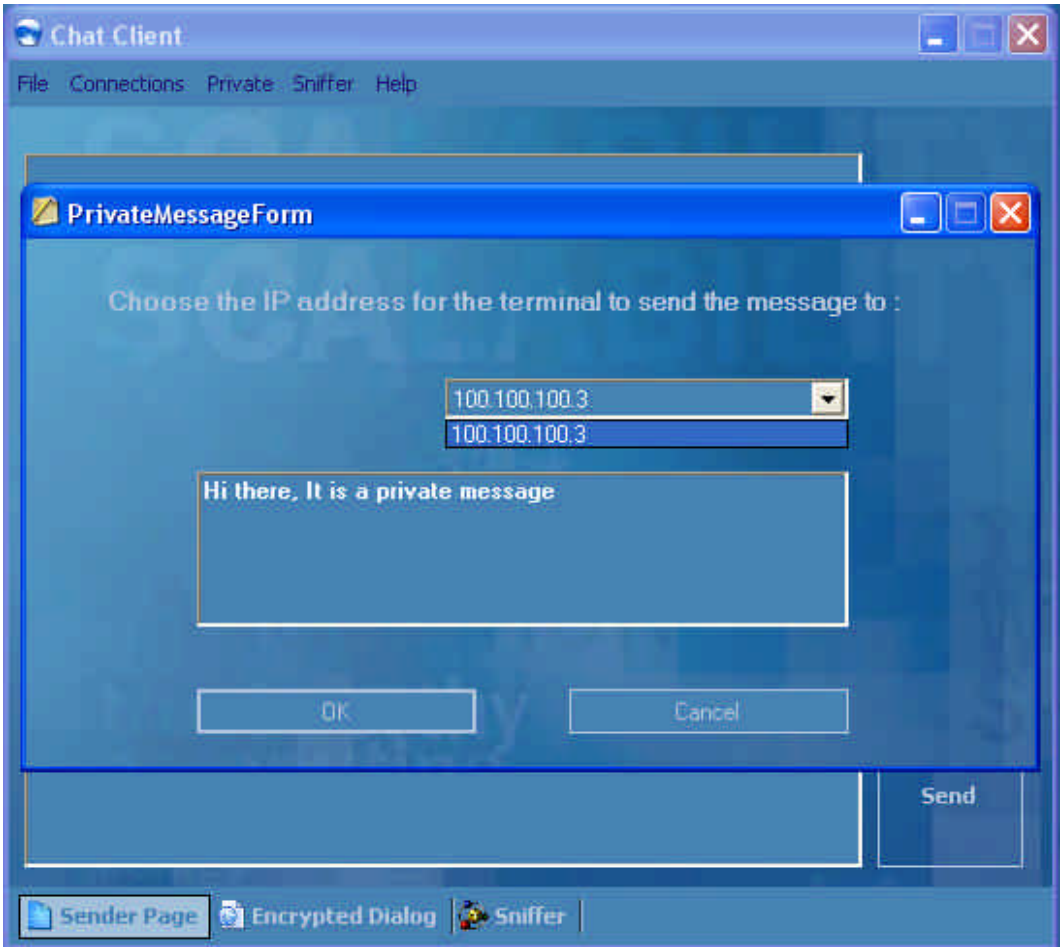
  This option allows the user to send private message to a specific user only.

- **Send File**

  This option allows the user to send a file to a specific user (File size should not exceed 64 KB).

Private Message :

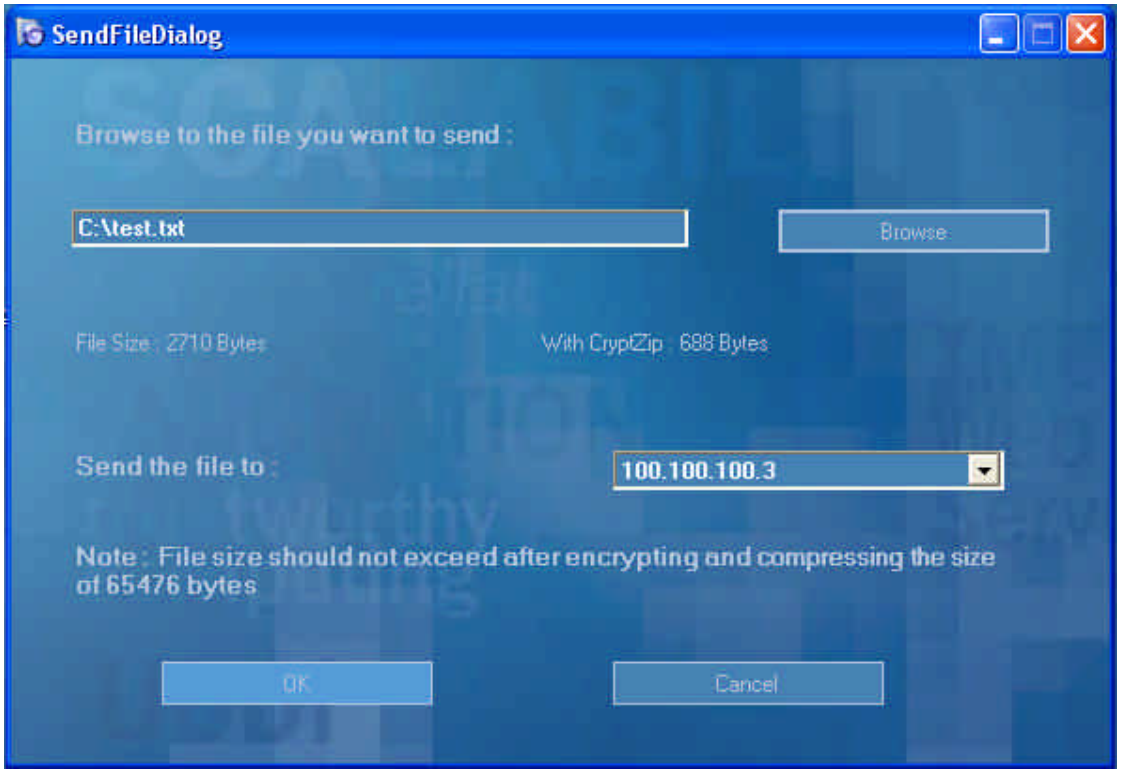
This facility allows the user to send private message to a specific user . See the figure below.



Send File :

Sender Side

This option is used to send files between connected terminals. Now lets take a look at the figure below :

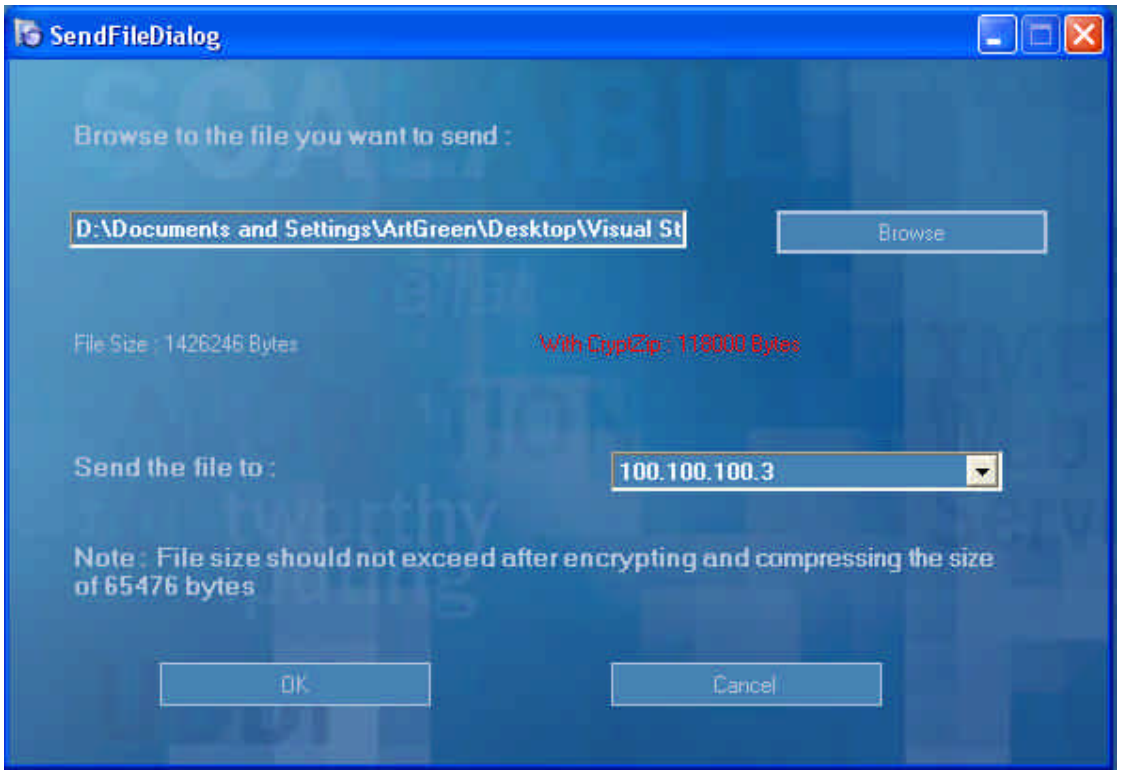


AS you can see; to select the file you want to send you can either type its full path directly in the text box or use the browse button to browse to the desired file.

File size should not exceed 65476 bytes after encryption. For the figure above the actual file size is 2710 bytes, but with CryptZip it is only 688 bytes.

This will give you the probability to send files up to 800 KB.

Yet if your chosen file is large than the limit, the size label will become red to notify you.

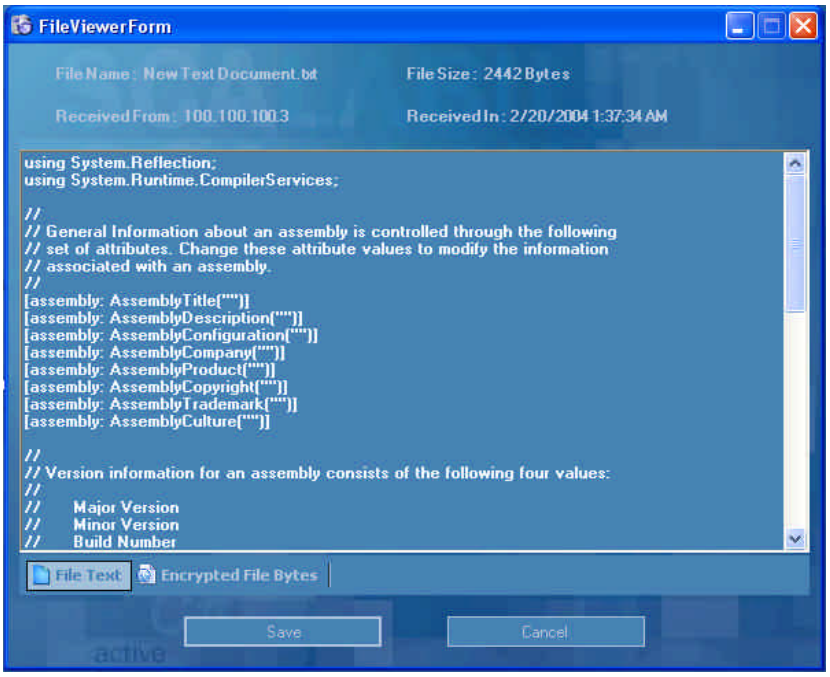


Even if you proceed and ignore the notification the program will not send the file and an error will be shown.

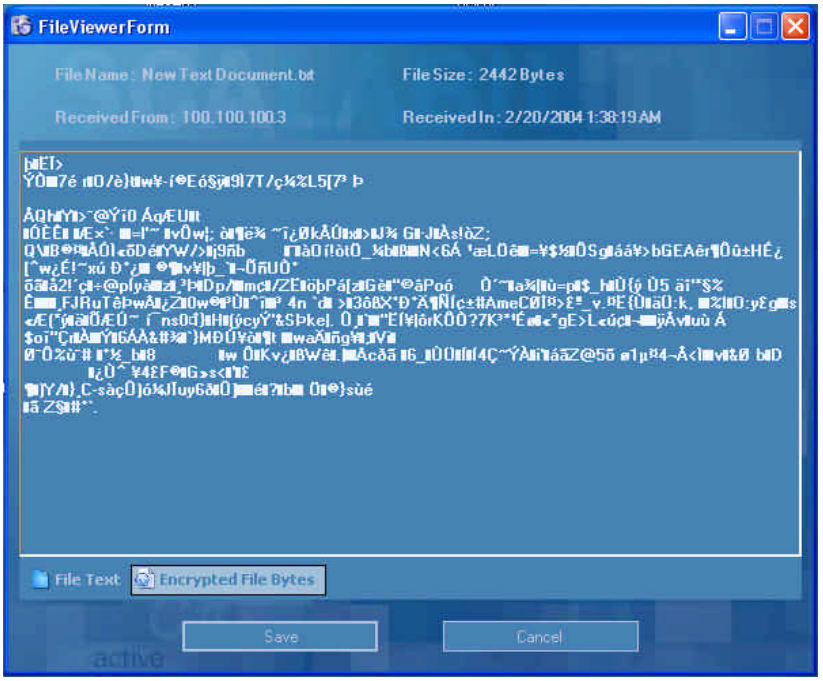
Recipient Side

The recipient of the file will get a file viewer that will allow him to:

- Browse the content of the file if it is viewable. And save it.

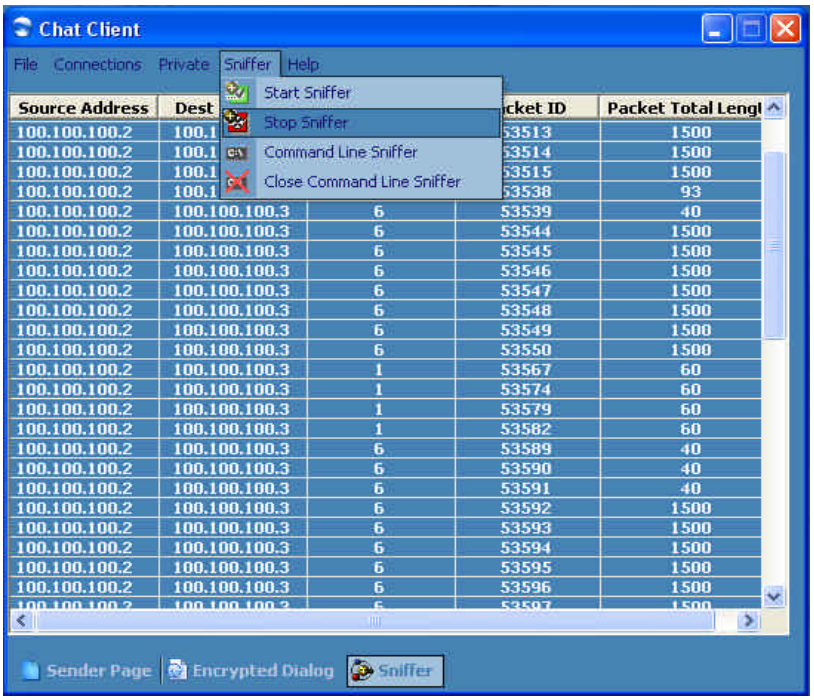


- See the encrypted content of the file.



Sniffer Menu :

Although it is not a major part in the chat program, this menu and its contents was added to show a simple use of the well-known sniffer programs.



Menu options are :

- **Start Sniffer**

Start a simple sniffer for network administration purposes. Click Here for more.

- **Stop Sniffer**

Stop the simple sniffer.

- **Command Line Sniffer**

Start a command line sniffer with more features than the simple sniffer. Click Here for more.

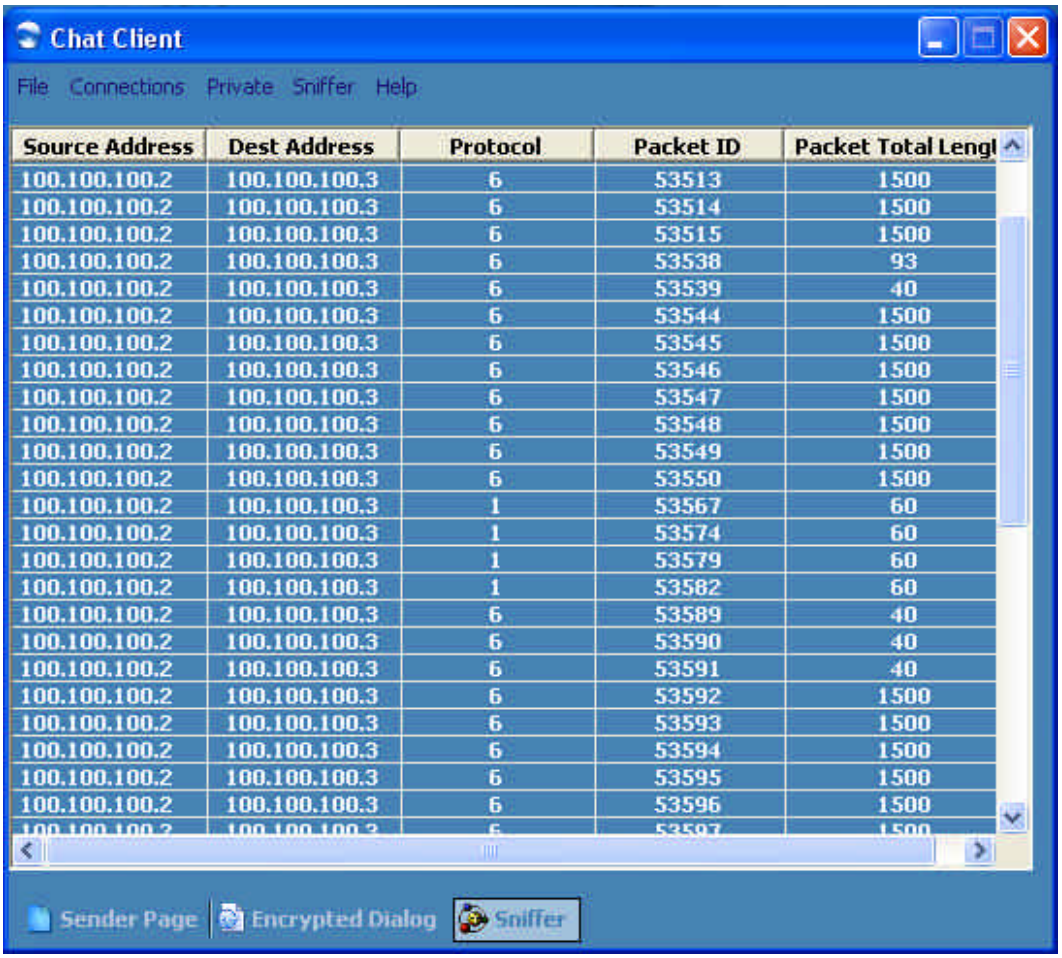
- **Stop Command Line Sniffer**

Stop command line sniffer program.

Simple Sniffer :

This is a simplified output of the sniffer program, used to the incoming IPv4 packets to the user device.

Figure below shows a simple output to the program.



The output columns are :

Source Address : Packet source address

Dest Address : Packet destination address.

Protocol : Packet upper protocol.

Packet ID : Packet Identification Number.

Total Packet Length : Total Packet length including the Header and the data.

Command Line Sniffer :

This program is a powerful sniffer that shows all the content of the incoming IPv4 packets headers and data.

Figure below shows how its output looks like.

