KING FAHD UNIVERSITY OF PETROLEUM AND MINERALS
COLLEGE OF COMPUTER SCIENCE & ENGINEERING

User Manual

Of

“Denial of Service Attack Detector and Tracer”

Done by

Ahmad Salam AlRefai 208602

For

Dr. Mohammed H. Sqalli

15-May-07

Table of Content

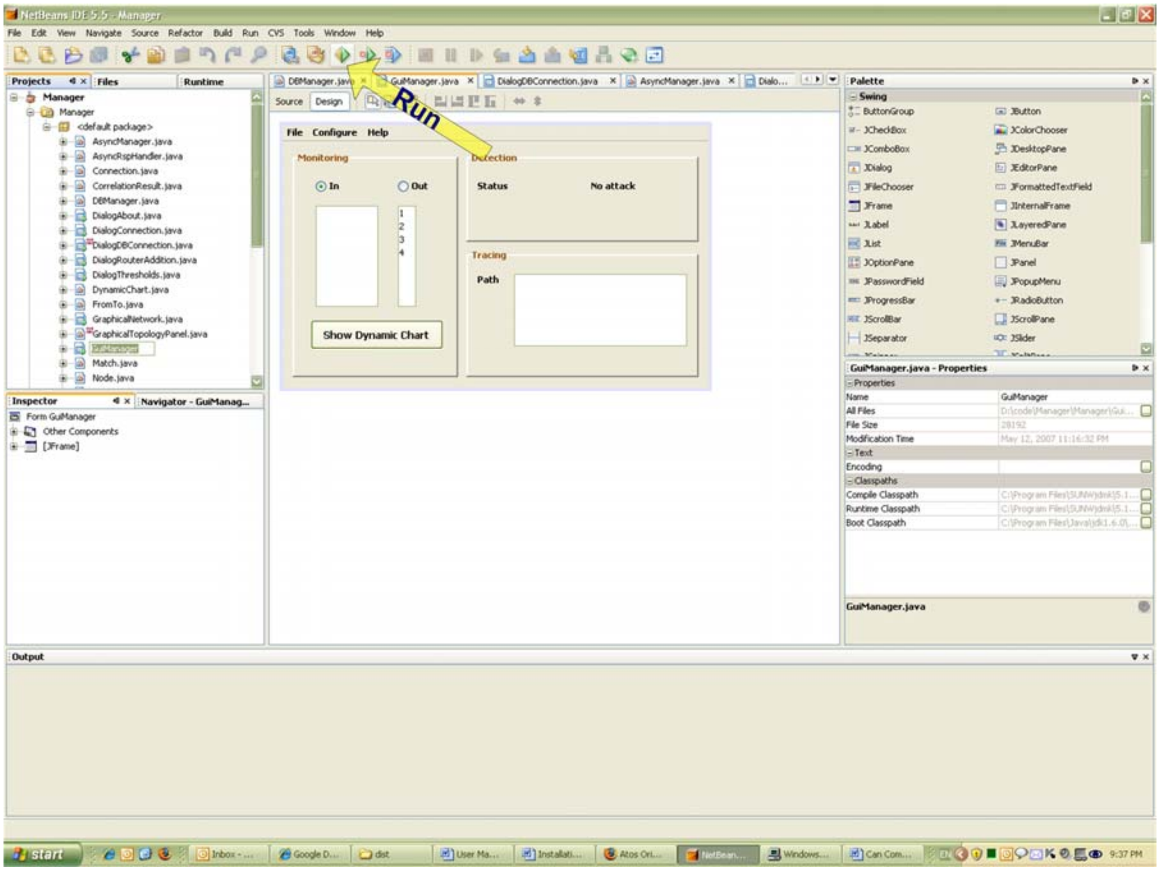
1. How to install the application?

Review the installation guide to see how to see how to install “Denial of Service Attack Detector & Tracer (DoSAT)” and all the required software and libraries.

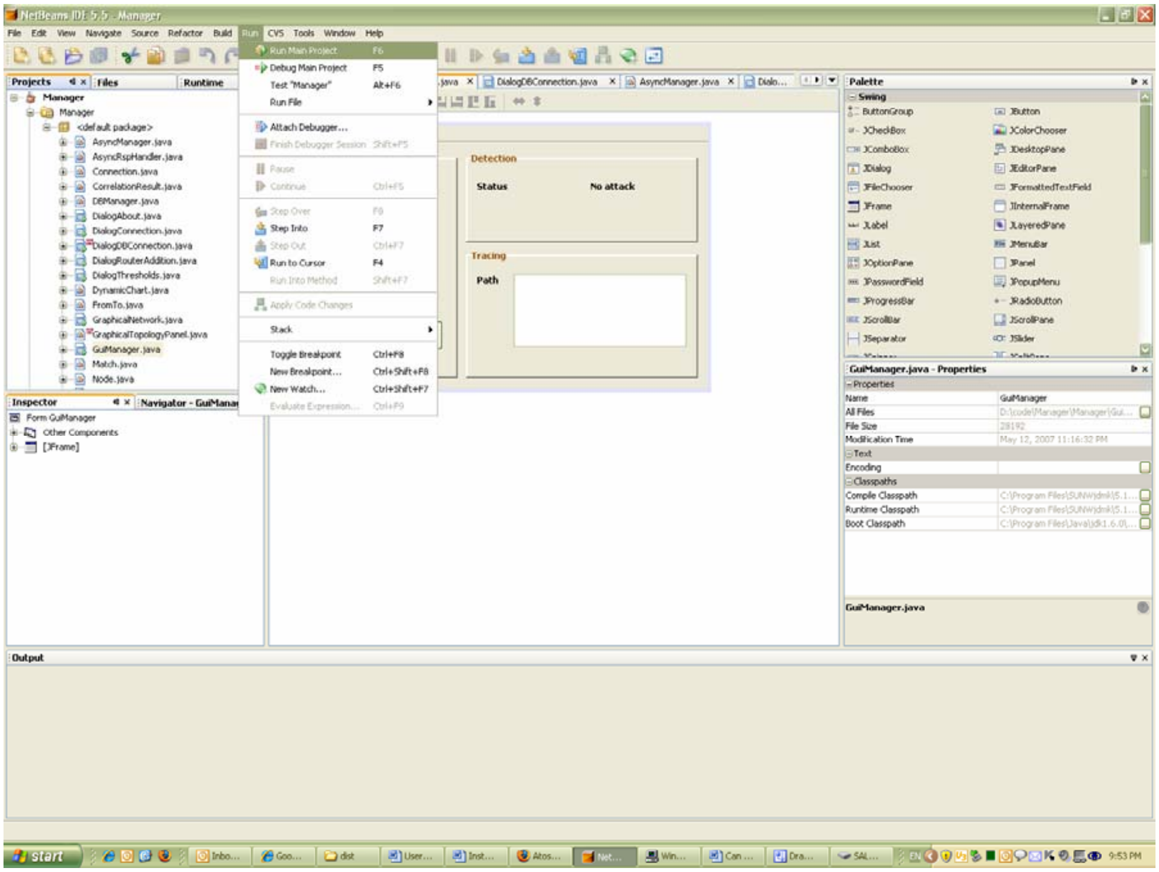
2. How to run the application?

2.1 Run From the Source Code (NetBeans Application).

Either by clicking run button as shown below.



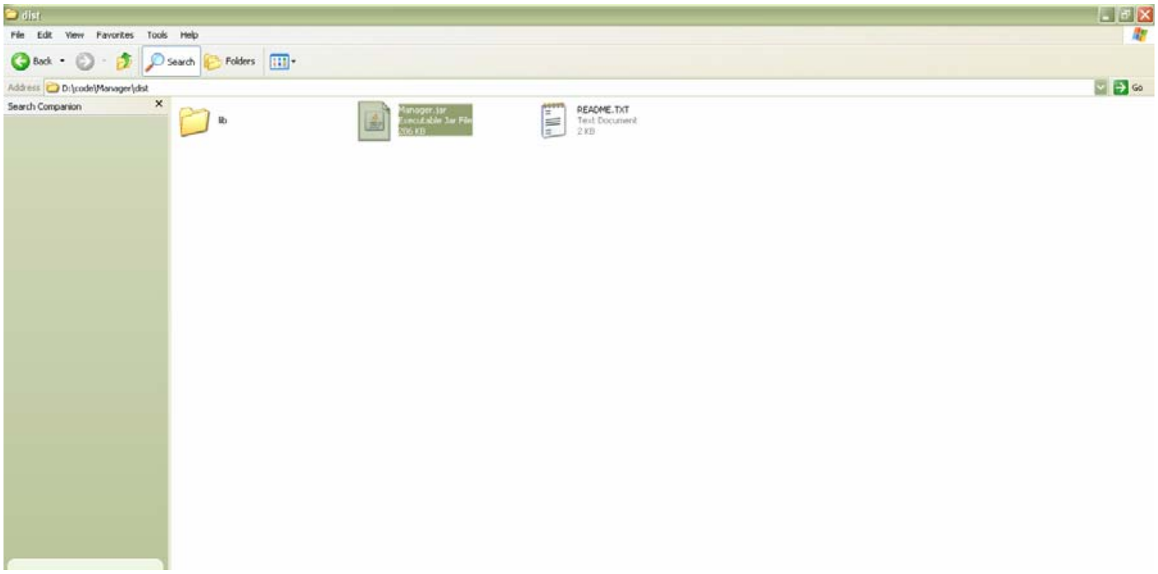
Or from the Run Menu, choose “Run Main Project” Menu Item as shown below:



Properties
Name GuiManager
All Files D:\code\Manager\Manager\Gui...
File Size 28192
Modification Time May 12, 2007 11:16:32 PM
Text
Encoding
Classpaths
Compile Classpath C:\Program Files\SUNW\jdmk\5.1...
Runtime Classpath C:\Program Files\SUNW\jdmk\5.1...
Boot Classpath C:\Program Files\Java\jdk1.6.0\...

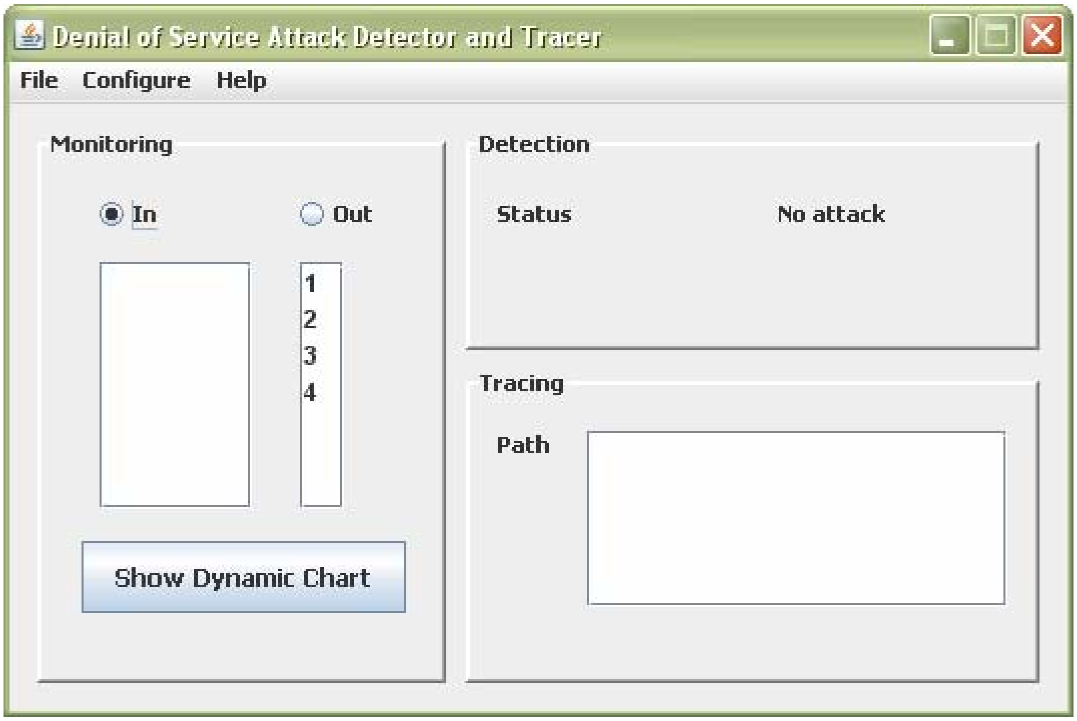
2.2 Run From the Jar File

Or just by double clicking the manager.jar file and the application will run. This is shown next.



Address D:\code\Manager\dist

The program starts with the following screen



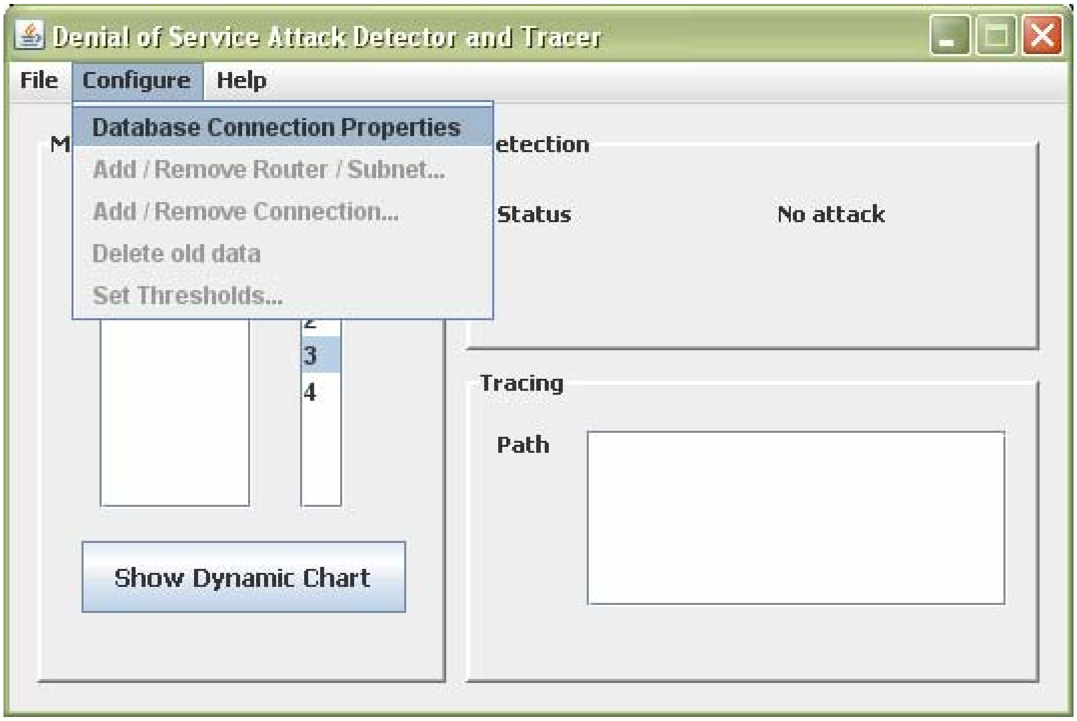
● In ○ Out

Status No attack

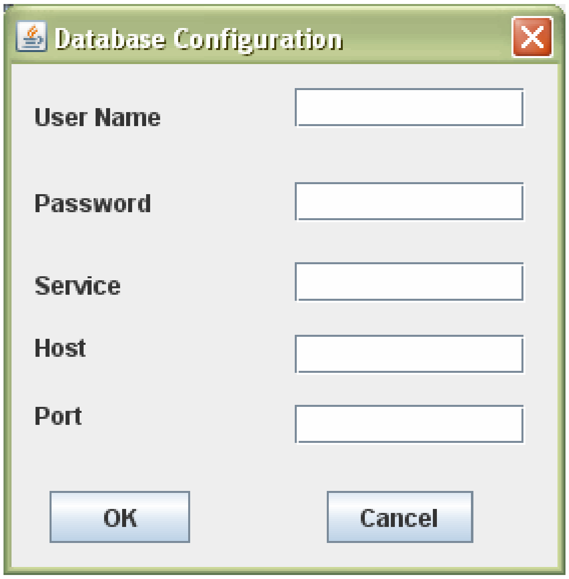
3. How to configure database connection?

First thing, you should do, if you are using the application for the first time, is to enter the database parameters. These are the parameters about the database you have already installed in your system and you also have the database tables running there.

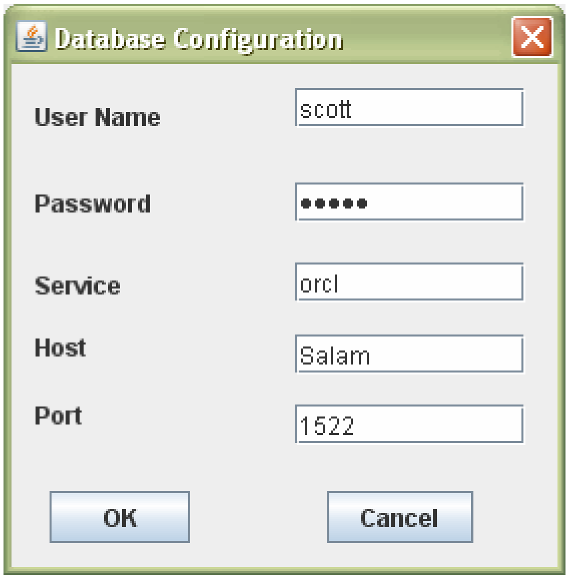
From the configure menu, in DoSAT application, choose “Database Connection Properties” menu item. This is shown in the next diagram.


Denial of Service Attack Detector and Tracer
File
Configure
Help
Database Connection Properties
Add / Remove Router / Subnet...
Add / Remove Connection...
Delete old data
Set Thresholds...
M
etection
Status
No attack
3
4
Tracing
Path
Show Dynamic Chart

A dialog box will appear. This is show in the following diagram.



The user can enter the username, password, service, host and port number, i.e. all the information required to connect to specific database. The system will remember the old configuration of the database. This is shown below.



User Name: scott

Password: •••••

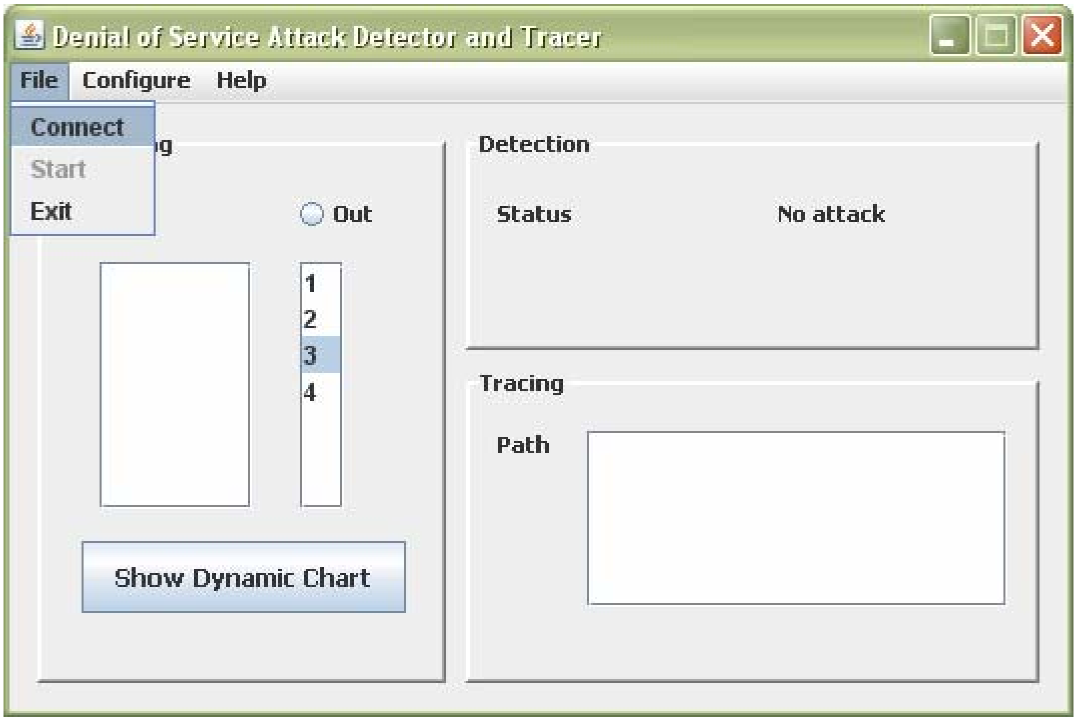
Service: orcl

Host: Salam

Port: 1522

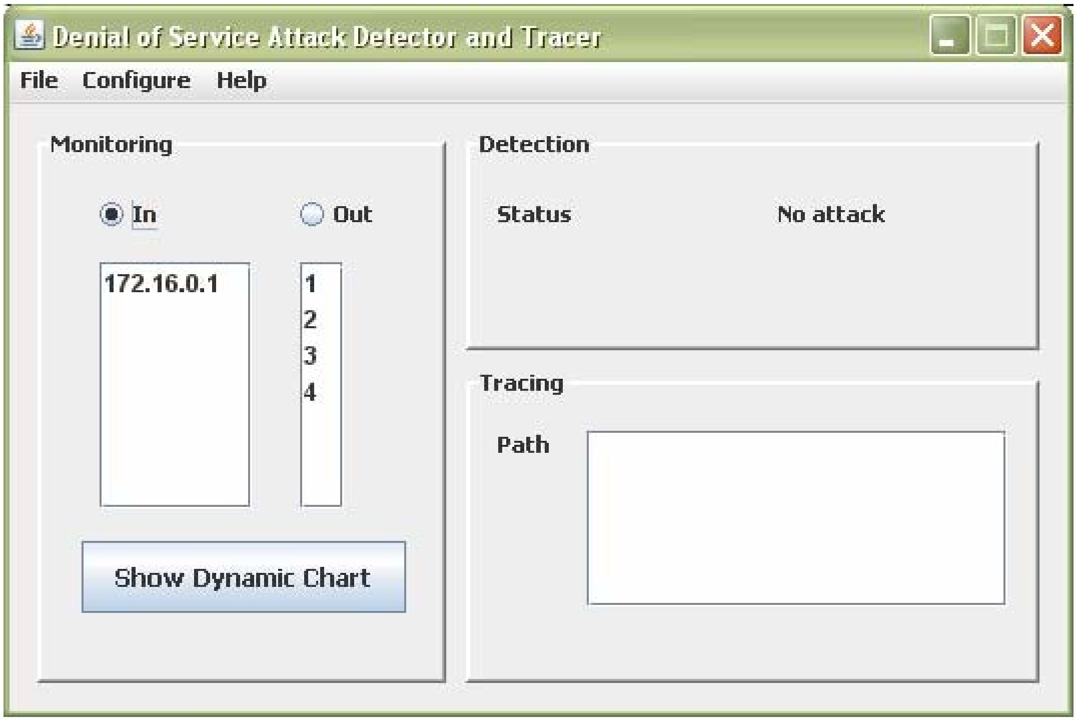
4. How to connect to database?

After you have configured your database, you can connect to it by choosing “Connect” menu item from the “File” menu. This is shown below.



Status: No attack

If it connects successfully, it just displays the routers stored before in the database and you can continue working with the application.



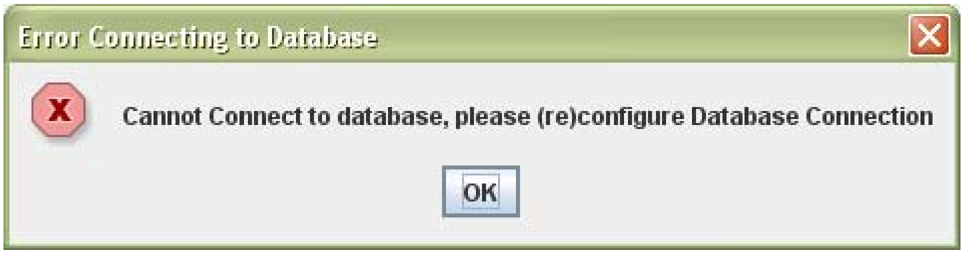
● In ○ Out

172.16.0.1

1
2
3
4

Status No attack

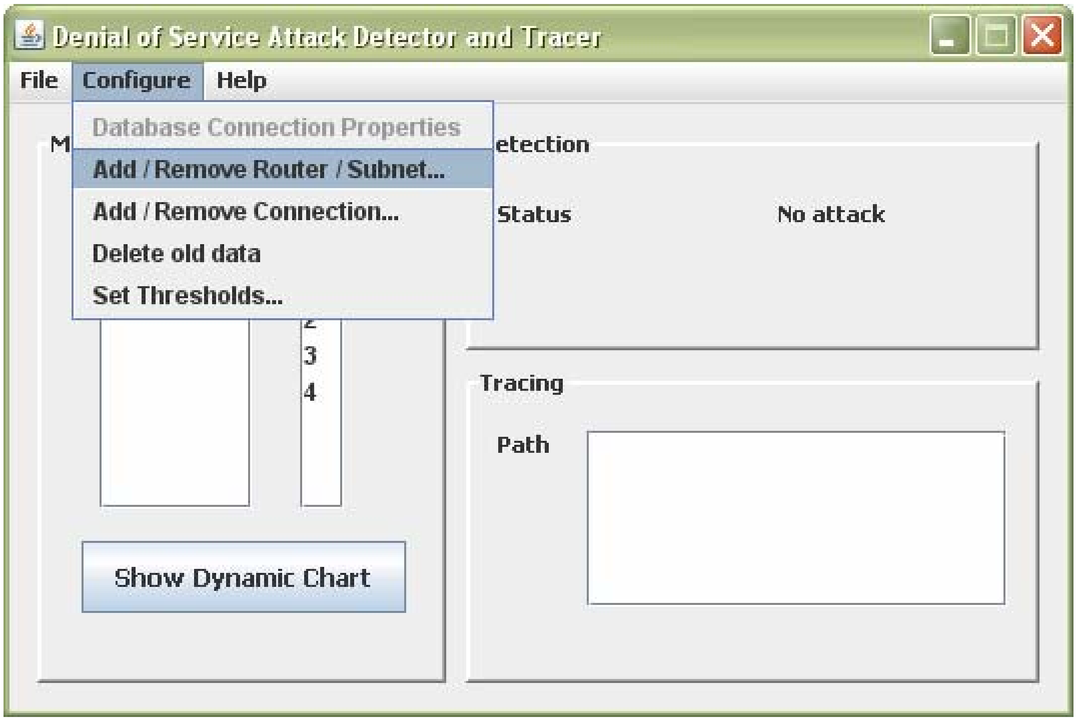
If you have entered wrong parameters in the database configuration, and the system is not able to connect to the database, the system will display a message that it cannot connect to the database.



Cannot Connect to database, please (re)configure Database Connection

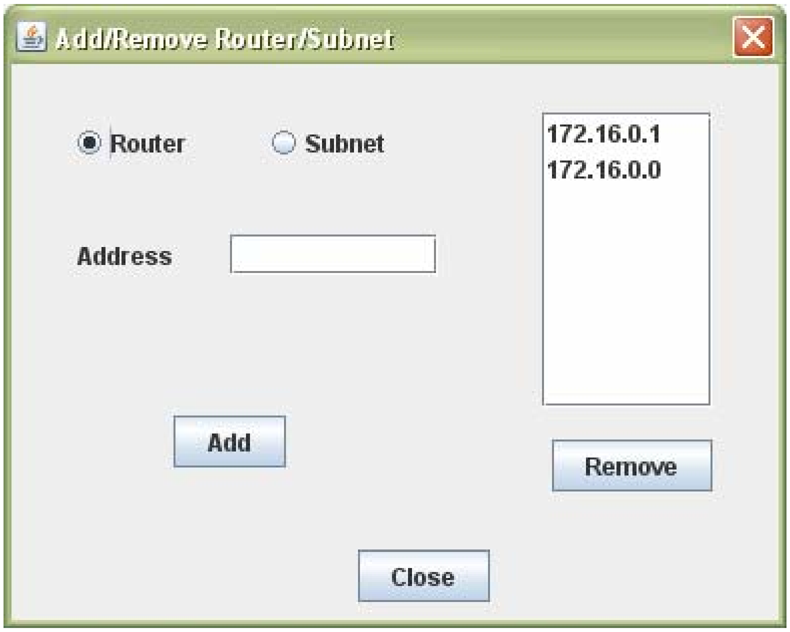
5. How to add a node?

To add a node whether it is router or subnet, go to “Add/Remove Router/Subnet” menu item from the “Configure” menu as shown below:


Denial of Service Attack Detector and Tracer
File
Configure
Help
Database Connection Properties
Add / Remove Router / Subnet...
Add / Remove Connection...
Delete old data
Set Thresholds...
M
etection
3
4
Show Dynamic Chart
Tracing
Path

Status No attack

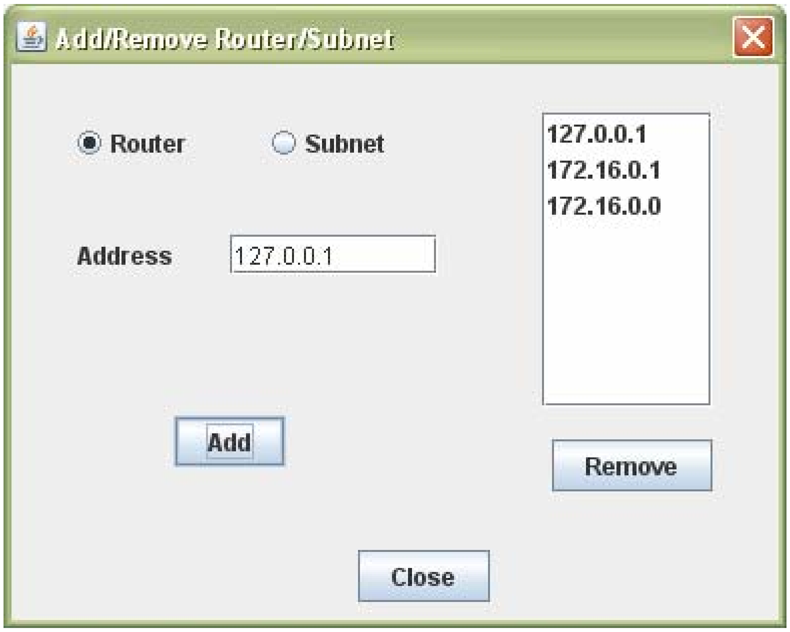
The following dialog will appear



● Router ○ Subnet

172.16.0.1
172.16.0.0

To add a router just choose Router radio button and enter the address (identity) of the router which is one of the IPs of its interface and then click the add button. This is shown below.



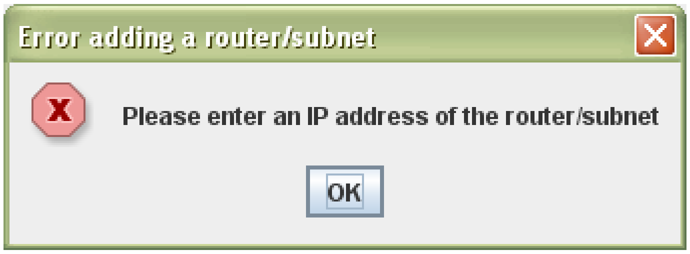
● Router ○ Subnet

Address 127.0.0.1

127.0.0.1
172.16.0.1
172.16.0.0

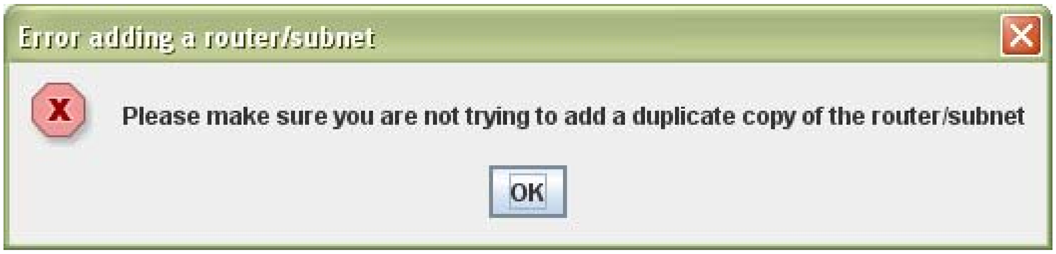
Then you can choose the close button to dispose this dialog.

If you try to add a router/subnet without entering the address, the following error message appears.



Please enter an IP address of the router/subnet

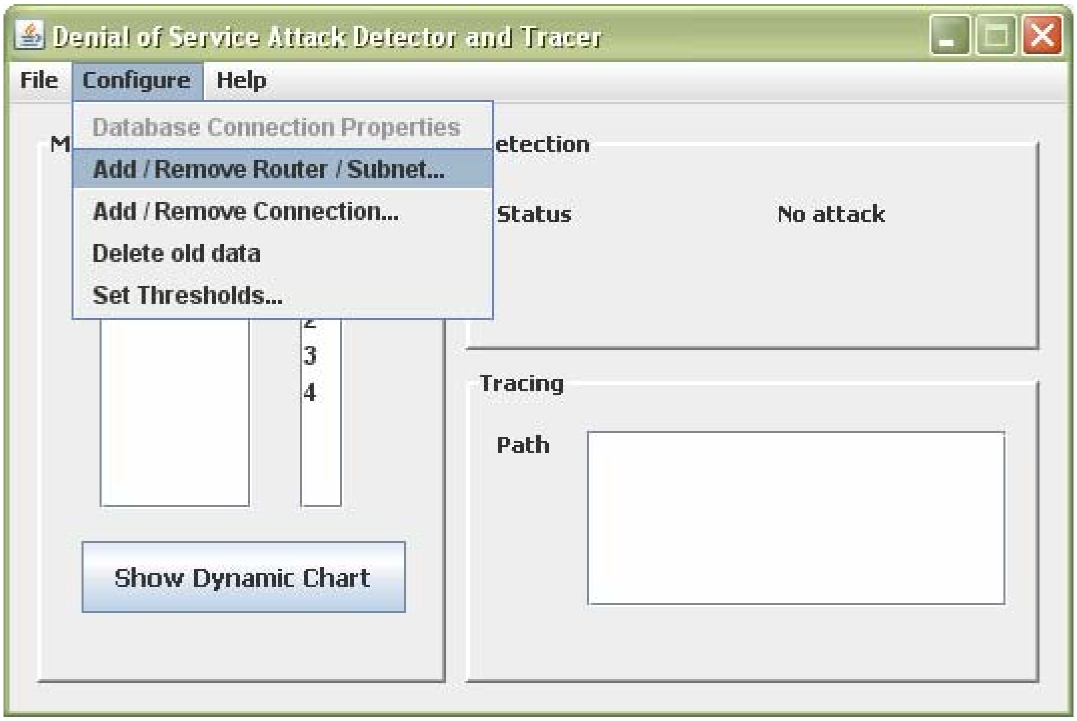
If you try to add the a router/node more than once, the following error appears



Please make sure you are not trying to add a duplicate copy of the router/subnet

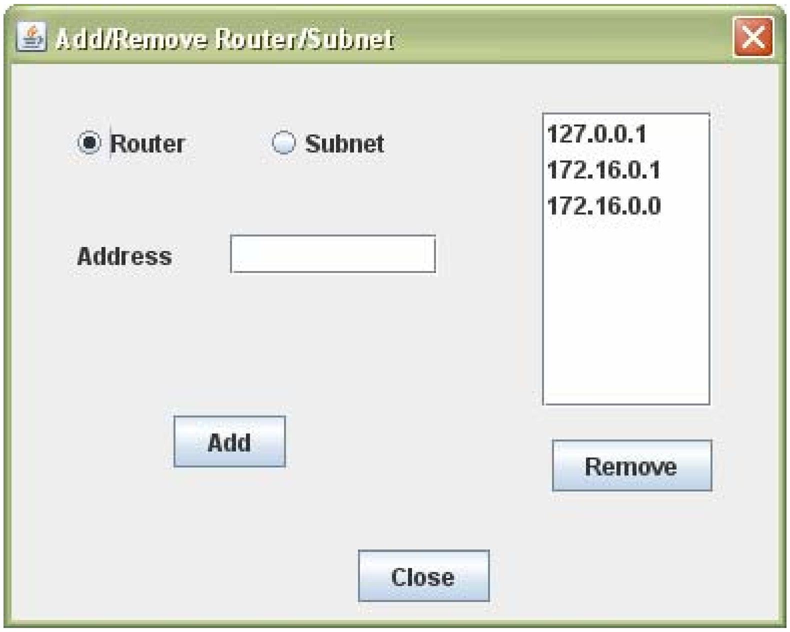
6. How to remove a node?

To remove a node whether it is router or subnet, go to “Add/Remove Router/Subnet” menu item from the “Configure” menu as shown below.


Denial of Service Attack Detector and Tracer
File
Configure
Help
Database Connection Properties
Add / Remove Router / Subnet...
Add / Remove Connection...
Delete old data
Set Thresholds...
M
etection
Tracing
Path
3
4
Show Dynamic Chart

Status No attack

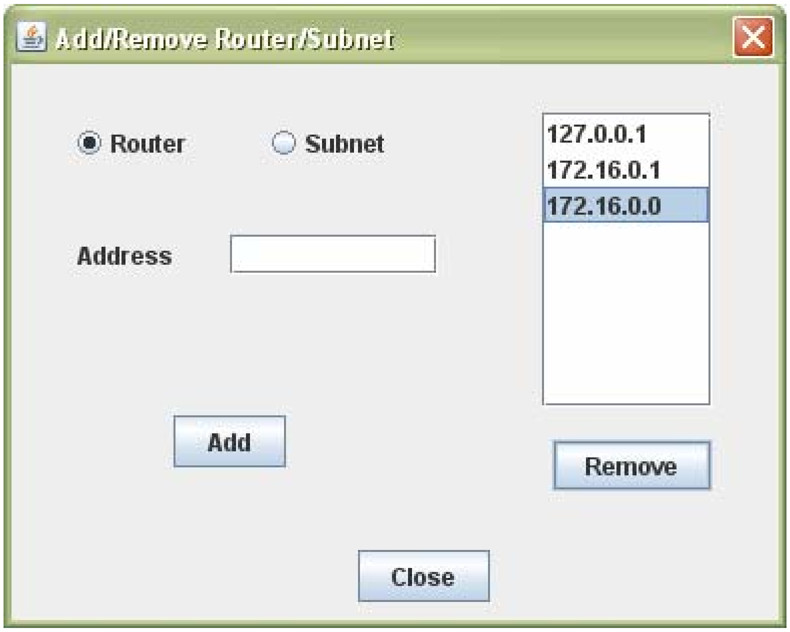
The following dialog will appear



● Router ○ Subnet

127.0.0.1
172.16.0.1
172.16.0.0

You need to select the IP address of the router or the subnet and then click remove. This is shown below.

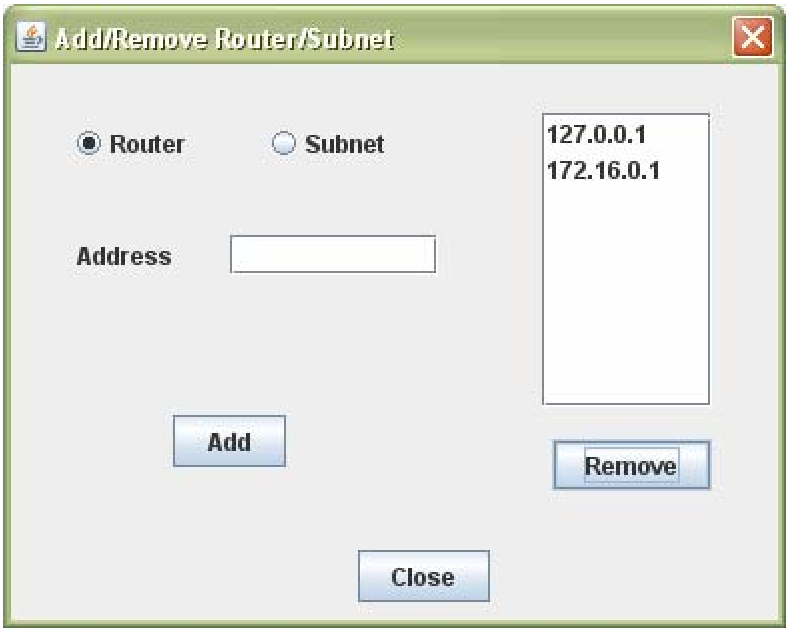


● Router ○ Subnet

Address

127.0.0.1
172.16.0.1
172.16.0.0

And then, after you click remove, the following screen is shown.

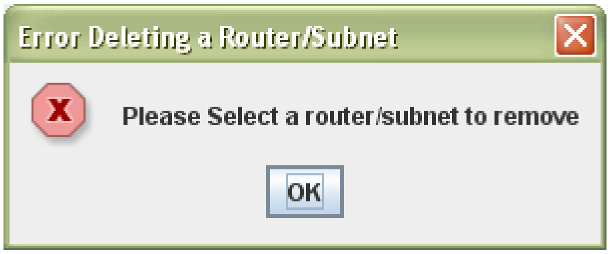


● Router ○ Subnet

Address

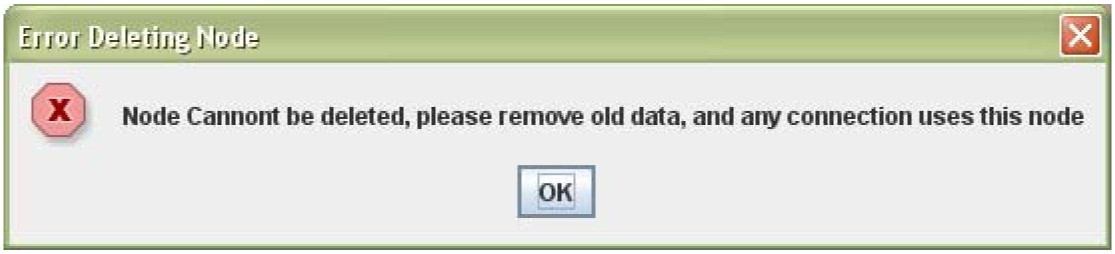
127.0.0.1
172.16.0.1

If you try to remove a node without selecting one the following error appear.



Please Select a router/subnet to remove

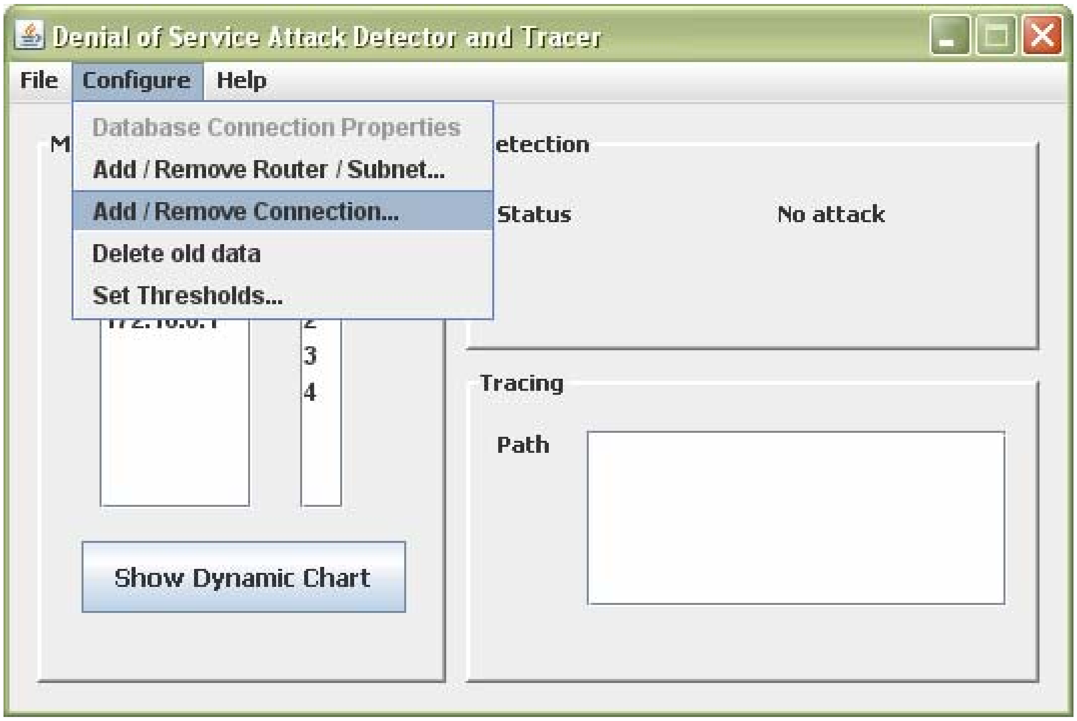
If you try to remove a node that has a connection to other node, or has some traffic data stored about it in the database, then the following error appears.



Node Cannont be deleted, please remove old data, and any connection uses this node

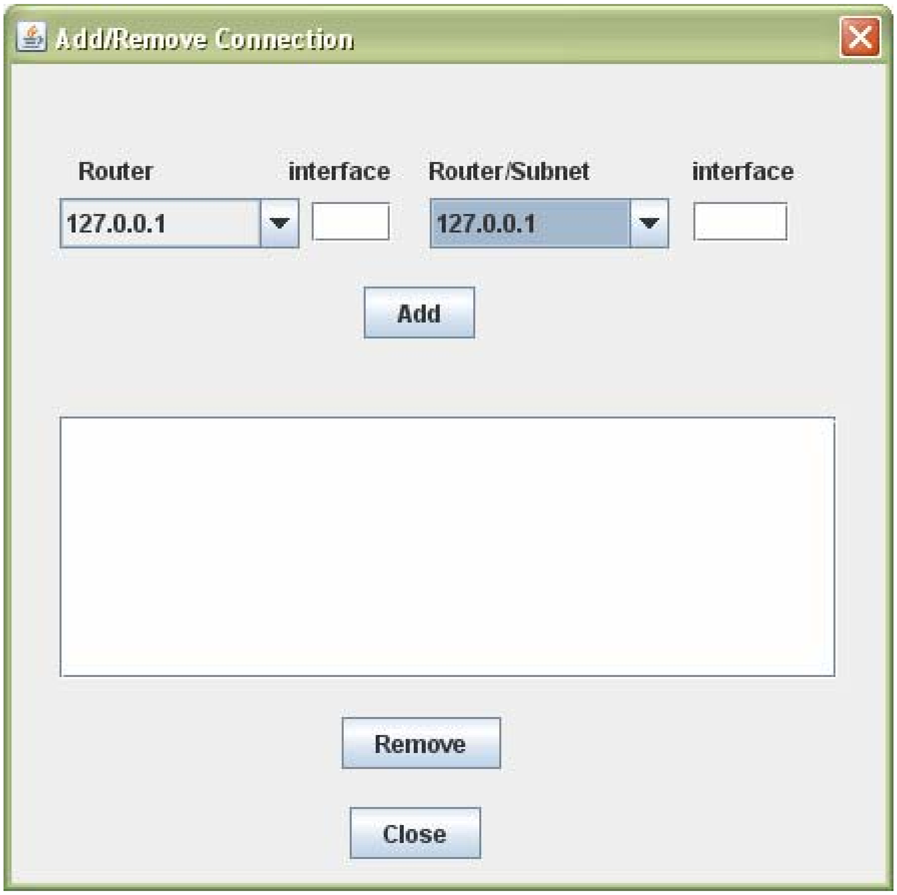
7. How to add a connection?

For each router you have a number of interfaces. For each connected interface in all routers, user has to enter to where this interface is connected. To add a connection, go to “Add/Remove Connection” menu item in the “Configure” menu. This shown below:

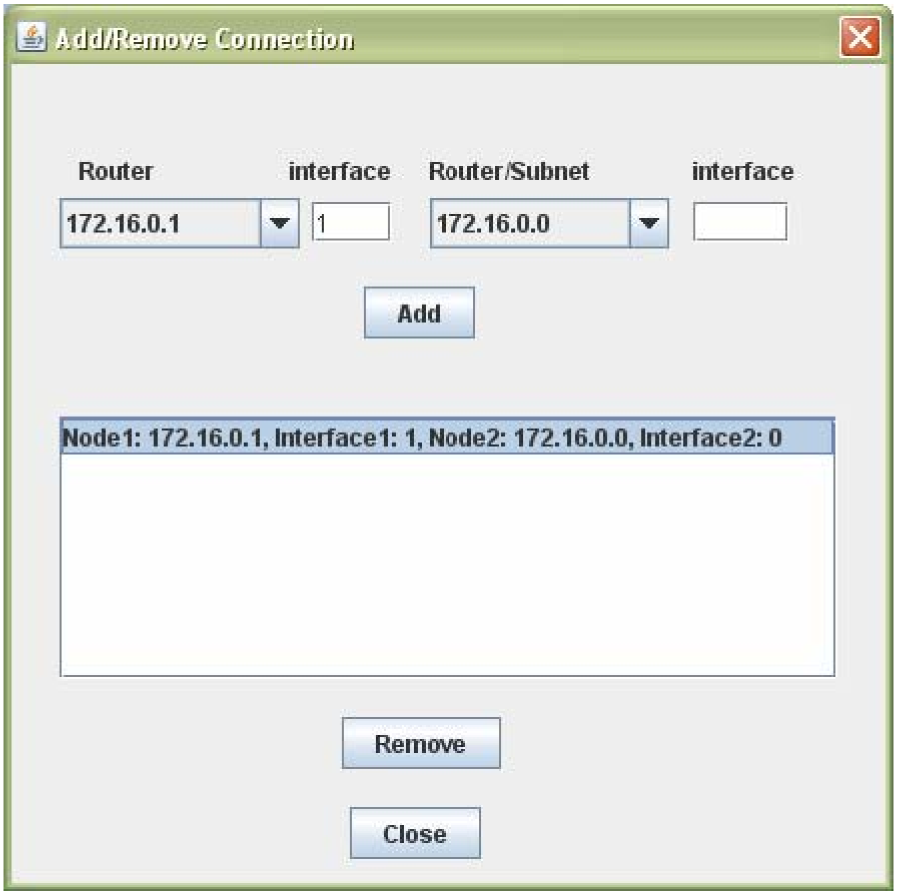

Denial of Service Attack Detector and Tracer
File
Configure
Help
Database Connection Properties
Add / Remove Router / Subnet...
Add / Remove Connection...
Delete old data
Set Thresholds...
M
etection
Tracing
Path
3
4
Show Dynamic Chart

Status No attack

After you click the following dialog appear.



Choose a router in the first compo box, enter which interface and then choose another router (you need to say which interface) or subnet (you do not need to enter any interface) the first router is connected to and then click “Add” button. The connection between routers needs to be represented in both directions. How to add a connection is shown below.

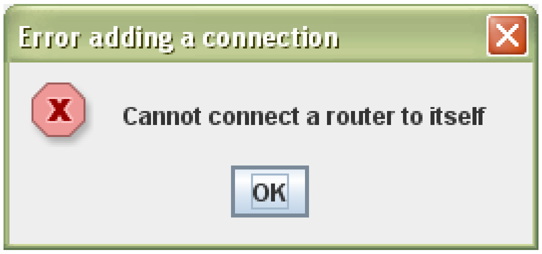


Router interface Router/Subnet interface

172.16.0.1 1 172.16.0.0

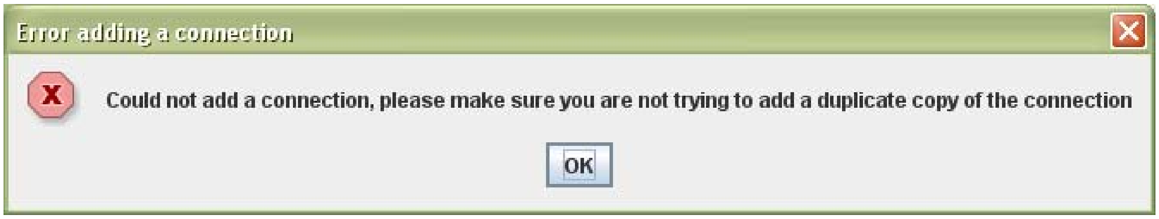
Node1: 172.16.0.1, Interface1: 1, Node2: 172.16.0.0, Interface2: 0

If you try to add a connection that connects a router to itself the following error appears.



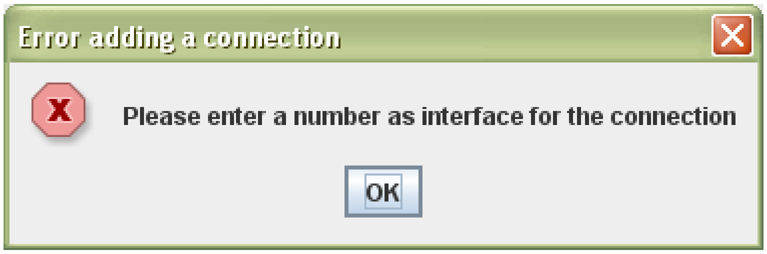
Cannot connect a router to itself

If you try to add a connection that exists already, the following error appears.



Could not add a connection, please make sure you are not trying to add a duplicate copy of the connection

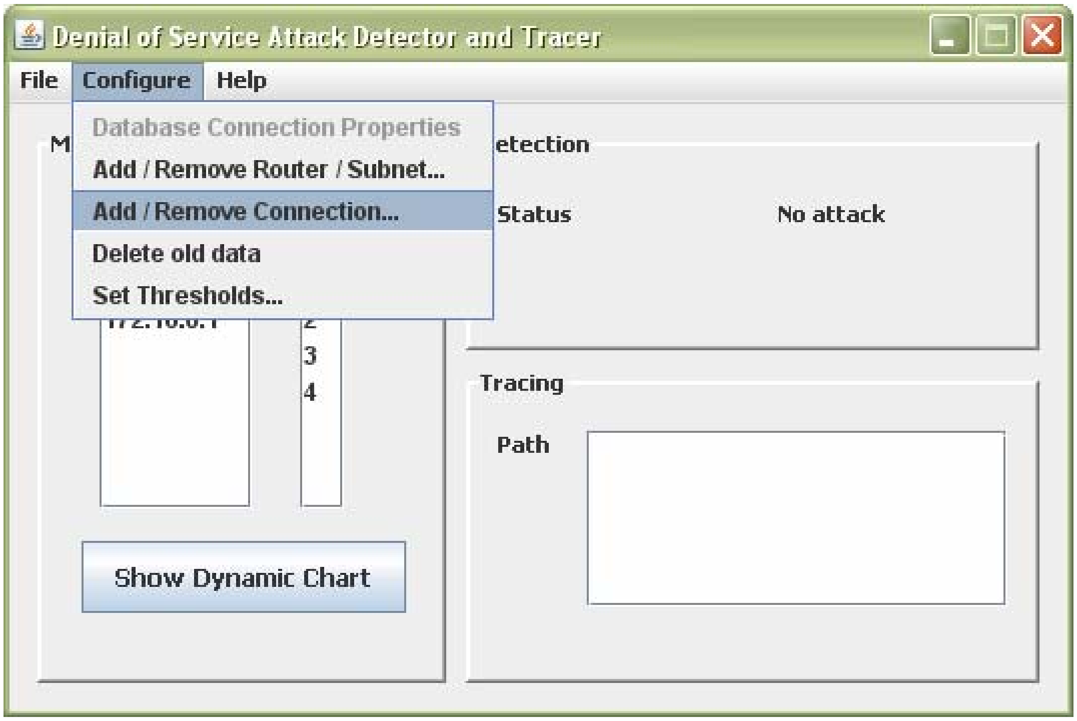
If you try to add a connection to a router without entering the interface number the following error appear.



Please enter a number as interface for the connection

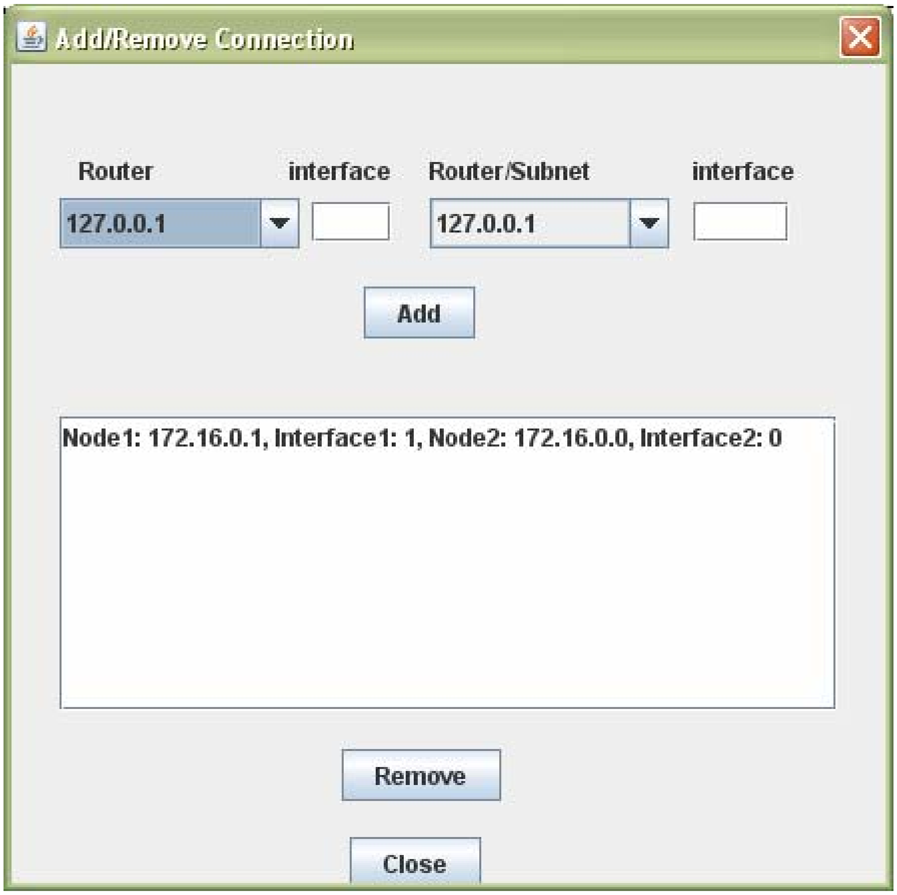
8. How to remove a connection?

To remove a connection, go to “Add/Remove Connection” menu item in the “Configure” menu. This shown below.


Denial of Service Attack Detector and Tracer
File
Configure
Help
Database Connection Properties
Add / Remove Router / Subnet...
Add / Remove Connection...
Delete old data
Set Thresholds...
M
etection
Tracing
Path
3
4
Show Dynamic Chart

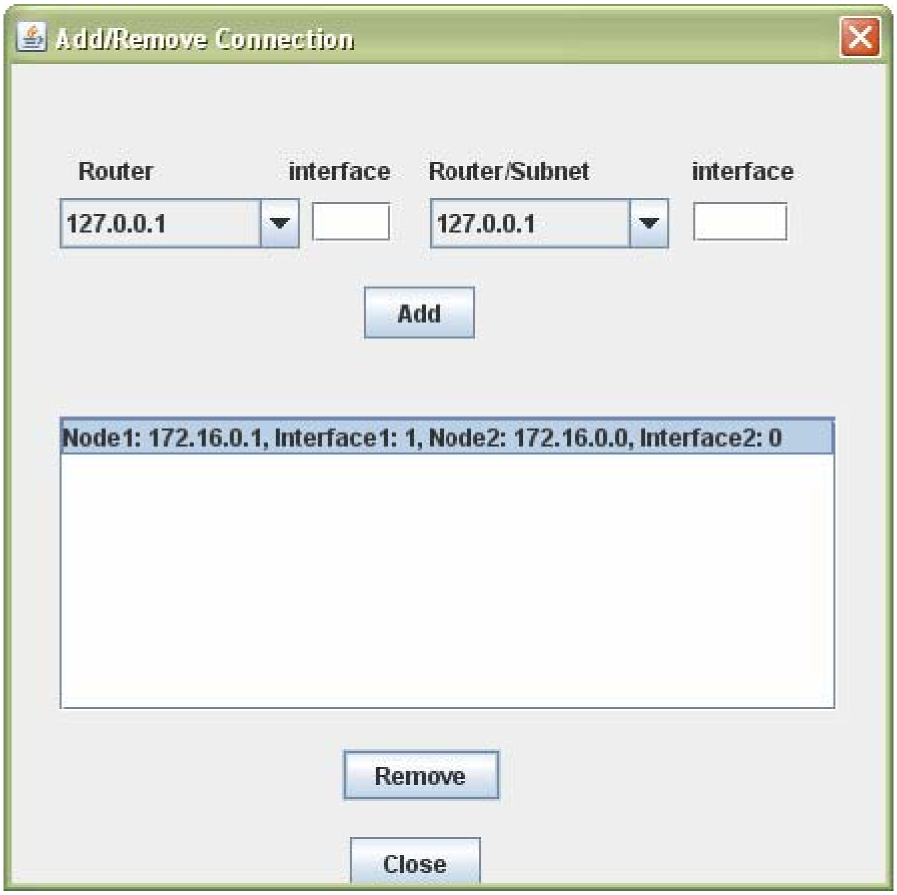
Status No attack

After you click the following dialog appear.



Node1: 172.16.0.1, Interface1: 1, Node2: 172.16.0.0, Interface2: 0

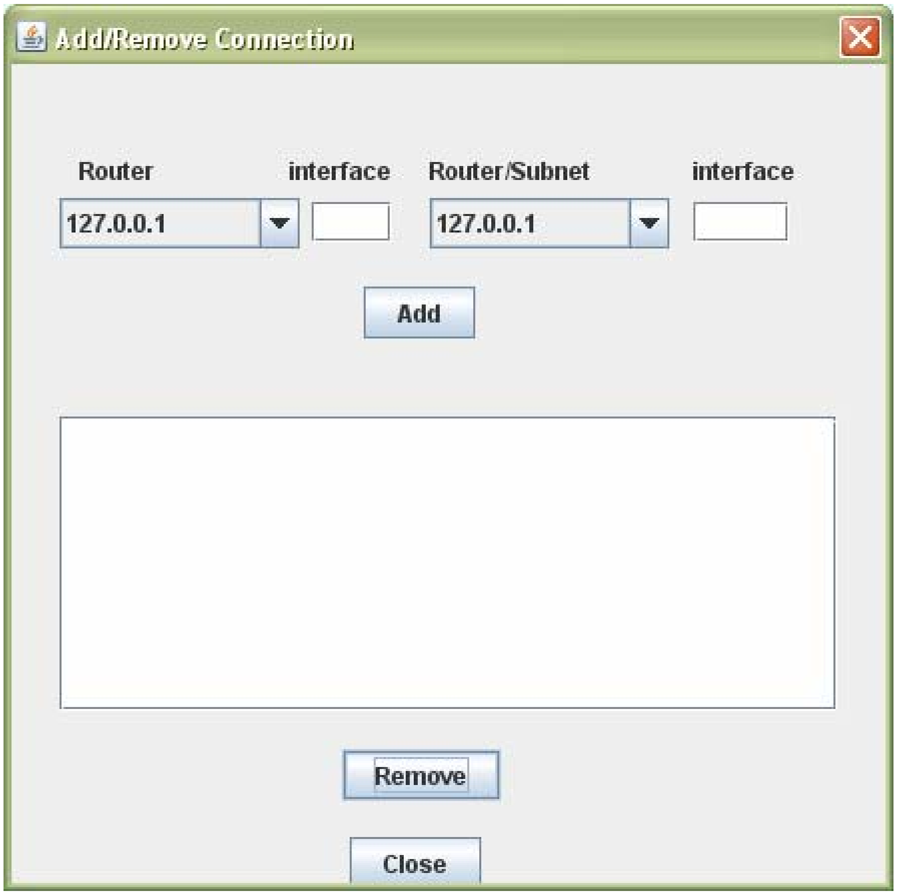
Then you have to choose the connection you want to delete and then click on the "Delete" button, as shown below.



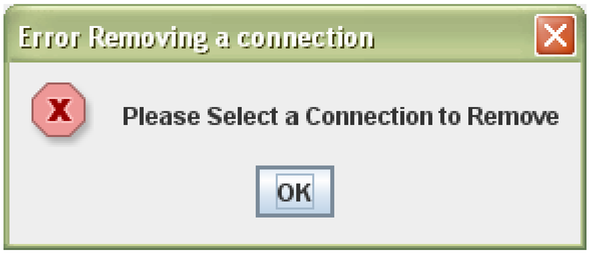
Router: 127.0.0.1

Router/Subnet: 127.0.0.1

Node1: 172.16.0.1, Interface1: 1, Node2: 172.16.0.0, Interface2: 0



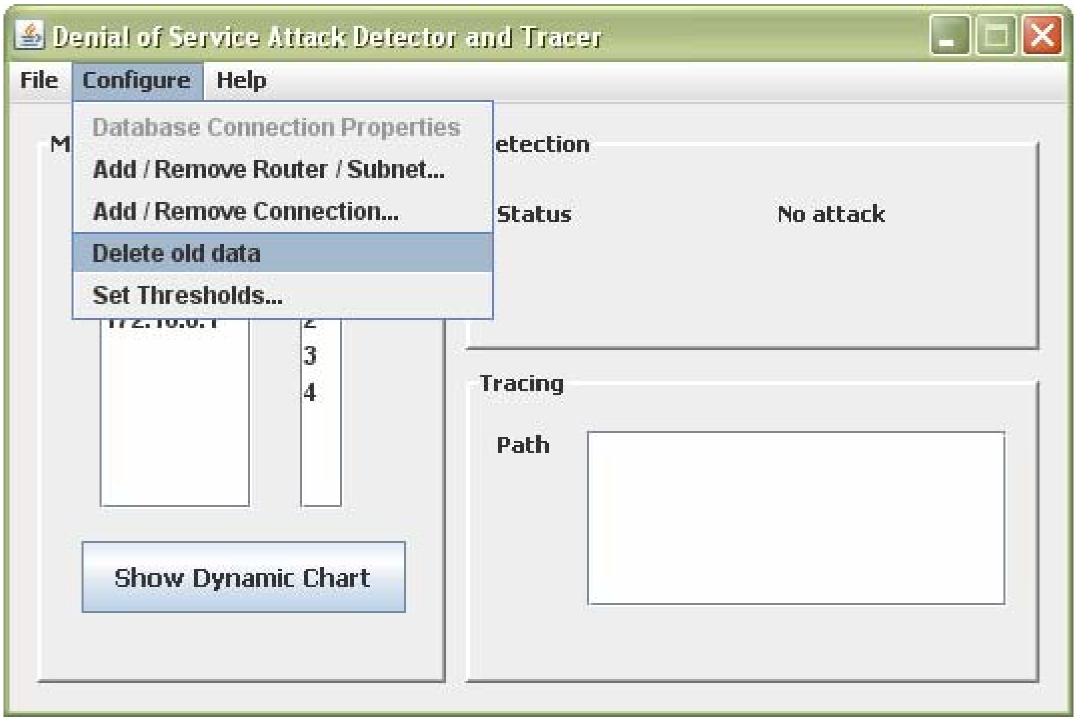
If you try to remove a connection without selecting one, the following error appears.



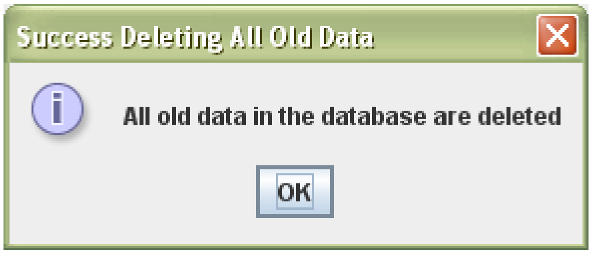
Please Select a Connection to Remove

9. How to delete old data?

When you monitor the routers, all the traffic rate data for all interfaces in all routers per specific amount of time are stored in the database. If you want to delete this data from the database just go to "Delete Old Data" menu item in the "Configure" menu as shown below.


Denial of Service Attack Detector and Tracer
File
Configure
Help
Database Connection Properties
Add / Remove Router / Subnet...
Add / Remove Connection...
Delete old data
Set Thresholds...
M
etection
Status
No attack
172.16.0.1
2
3
4
Tracing
Path
Show Dynamic Chart

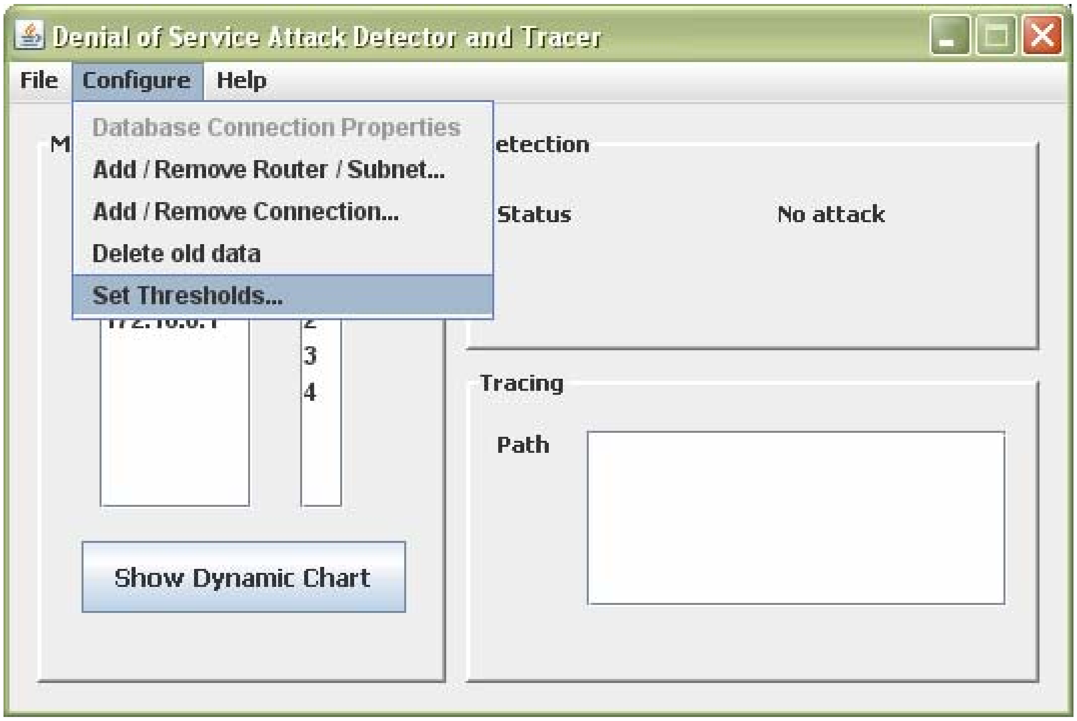
After you click “Delete old data”, all the data will be deleted and you get the following message.



All old data in the database are deleted

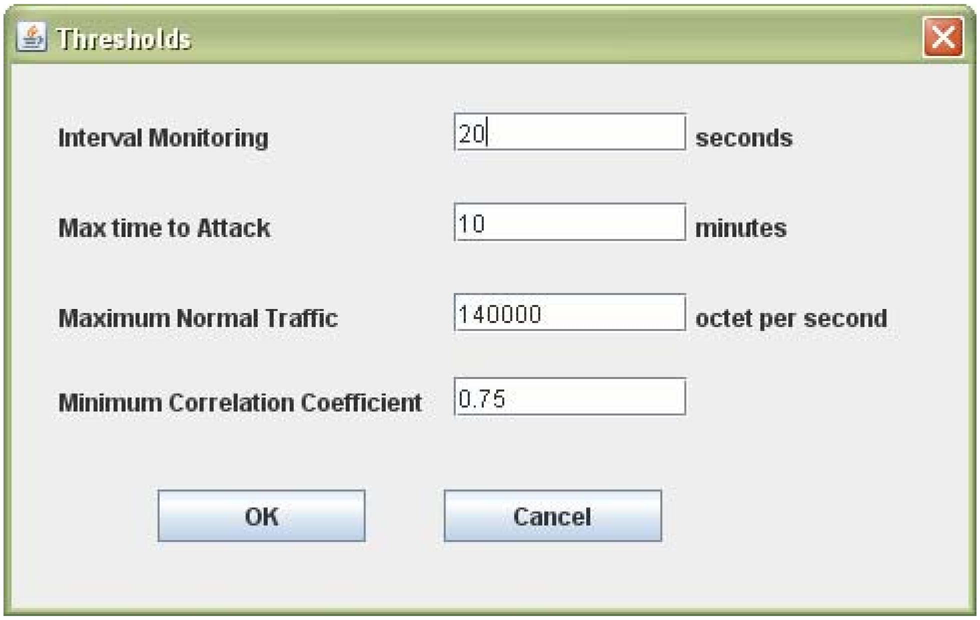
10. How to update threshold values?

The user is allowed to configure how the program works by updating some thresholds values. To display the dialog that enables updating threshold values, from the “Configure” menu, click on “Set Thresholds…” menu item as shown below.


Denial of Service Attack Detector and Tracer
File
Configure
Help
Database Connection Properties
Add / Remove Router / Subnet...
Add / Remove Connection...
Delete old data
Set Thresholds...
etection
Tracing
Path
Show Dynamic Chart

Status No attack

The thresholds dialog appears with some default values.

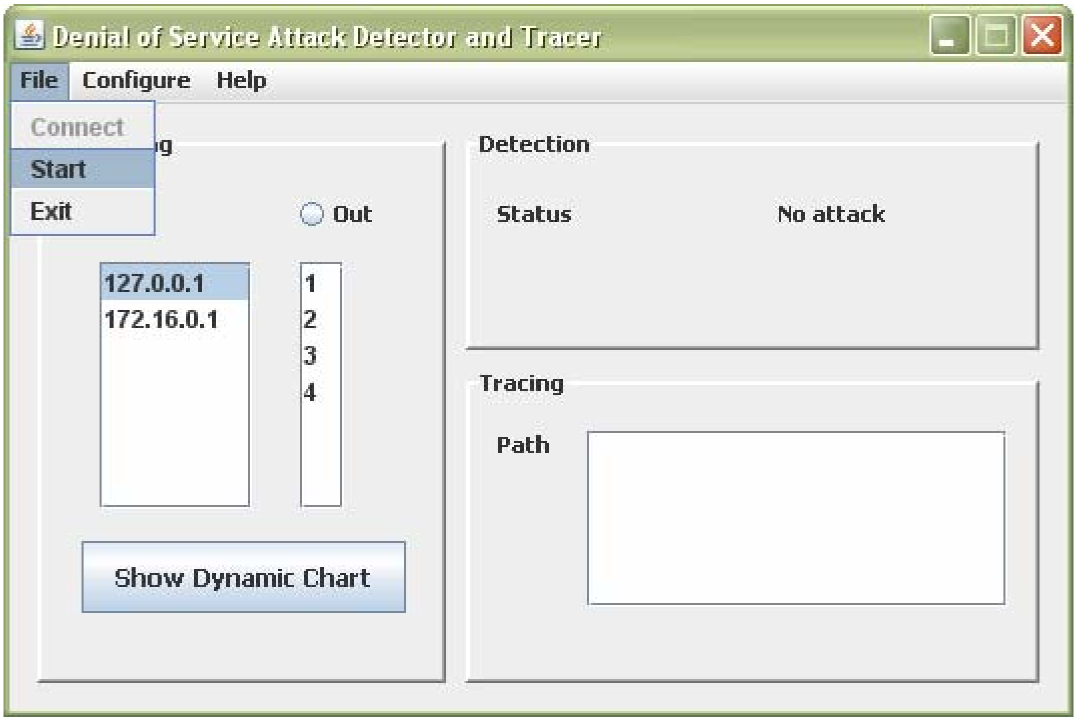


Interval Monitoring	20	seconds
Max time to Attack	10	minutes
Maximum Normal Traffic	140000	octet per second
Minimum Correlation Coefficient	0.75	

As we can see, the user can update the “Interval Monitoring” which is how long in seconds the system should waits between two successive requests to routers. The “Max time to Attack” is how long the attack is allowed to proceed before the tracing is started. The “Maximum Normal Traffic” is the maximum traffic acceptable to consider that there is no attack, if the traffic rate exceeds this threshold then the system consider that there is an attack. The “Minimum Correlation Coefficient” is the minimum correlation value acceptable to consider two traffic patterns as correlated. You can update any value you want and then click “OK” button. You may click “Cancel” button if you do not want to change the previous value.

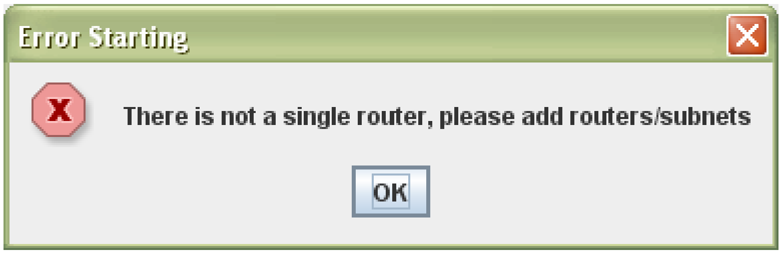
11. How to start monitoring?

After you are connected to the database, and you have supplied the system with all the needed topology and thresholds information, you can start the system by clicking “Start” menu item from the “File” menu. The system after clicking “Start” starts monitoring network by sending requests and receiving responses from routers.



Status No attack

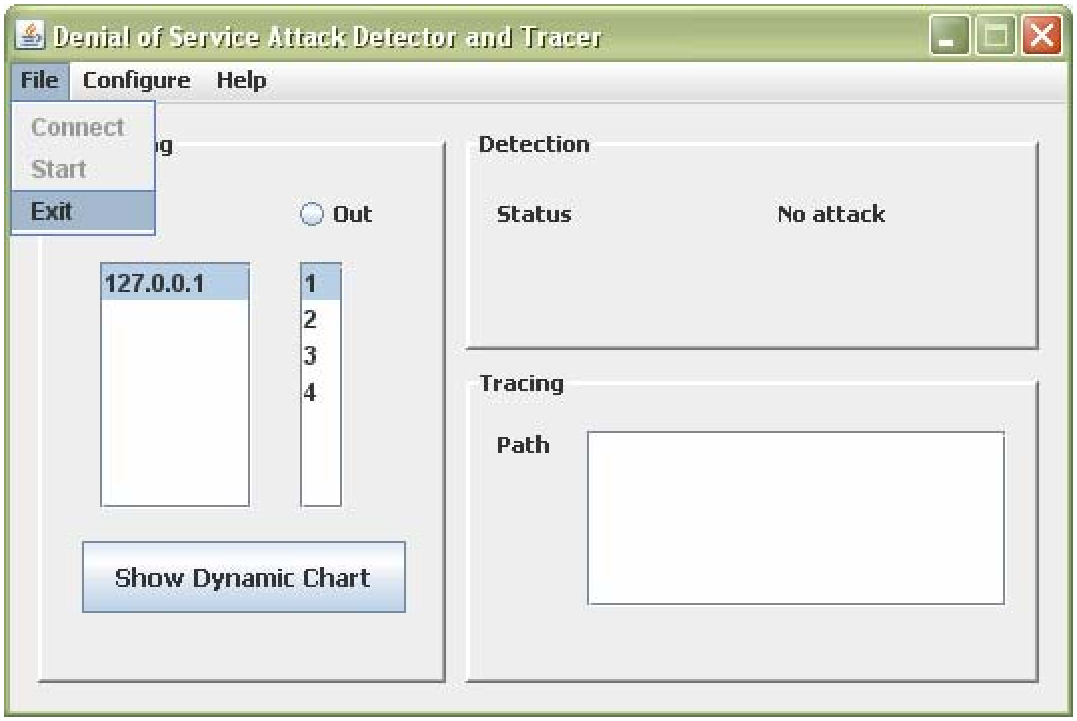
If you try to start the application without having any router, the following error message appears.



There is not a single router, please add routers/subnets

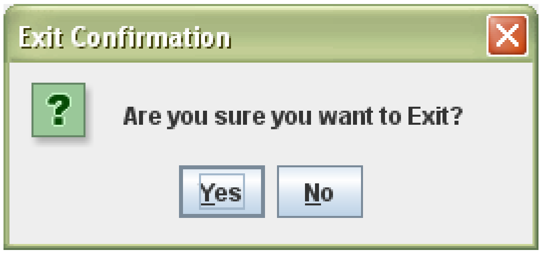
12. How to exit the system?

You can exit the system at any time by choosing "Exit" menu item from the "File" menu, as shown below.



Status No attack

After that a confirmation message is displayed.

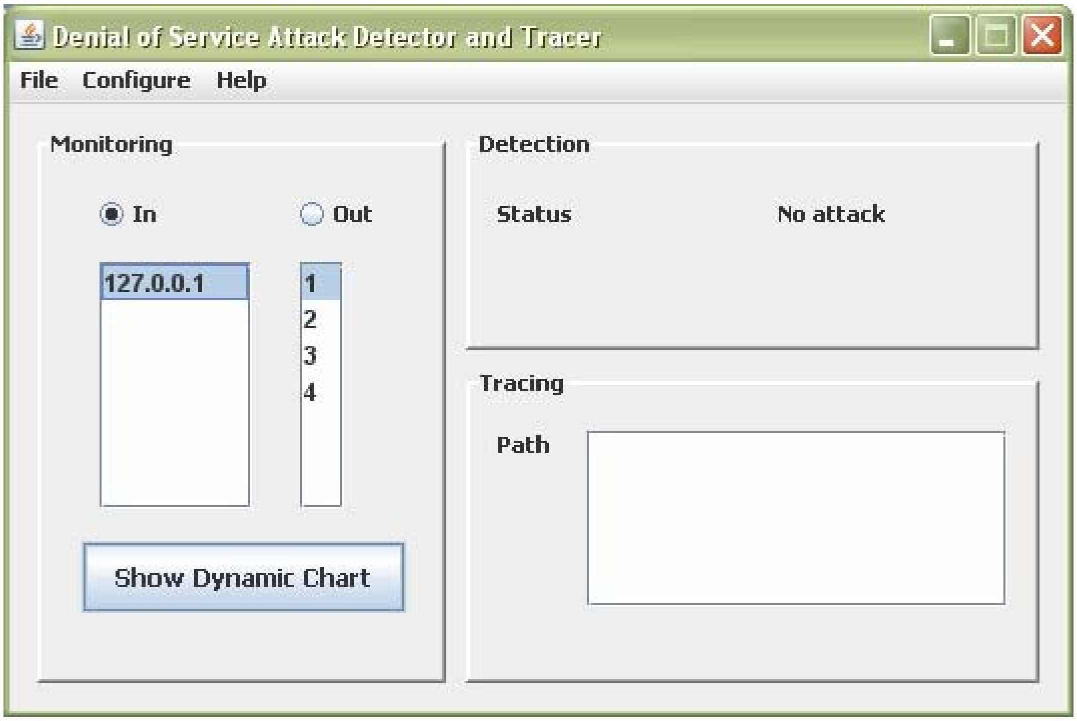


Are you sure you want to Exit?

If you click "Yes", the system will exit, if you click "No" nothing will happen.

13. How to get dynamic chart feedback?

You can get dynamic chart of any of the monitoring interfaces in all routers. Make sure that the monitoring is started and you select router address, interface number, and the type whether it is "in" or "out".



Denial of Service Attack Detector and Tracer

Monitoring

● In ○ Out

127.0.0.1

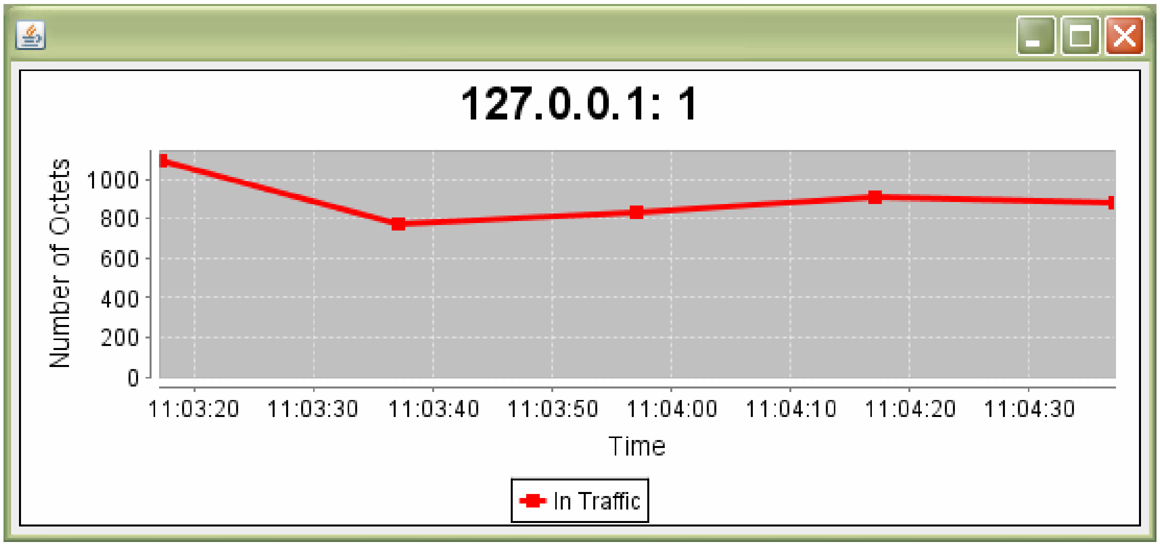
1
2
3
4

Detection

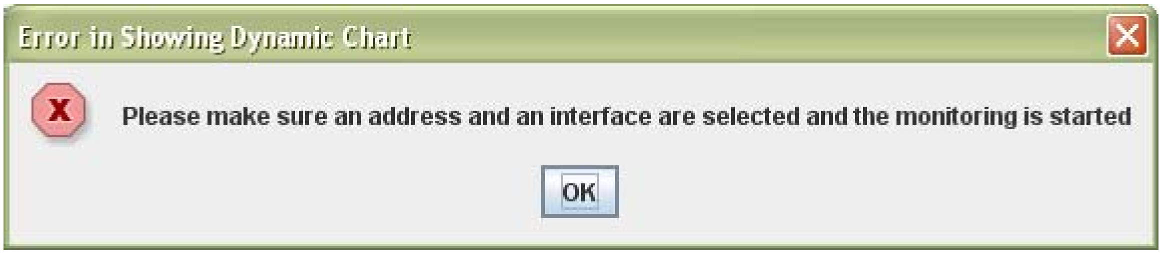
Status No attack

Tracing

Path



If you try to get feedback and the application is not started or not selecting an address or an interface the following error appears.

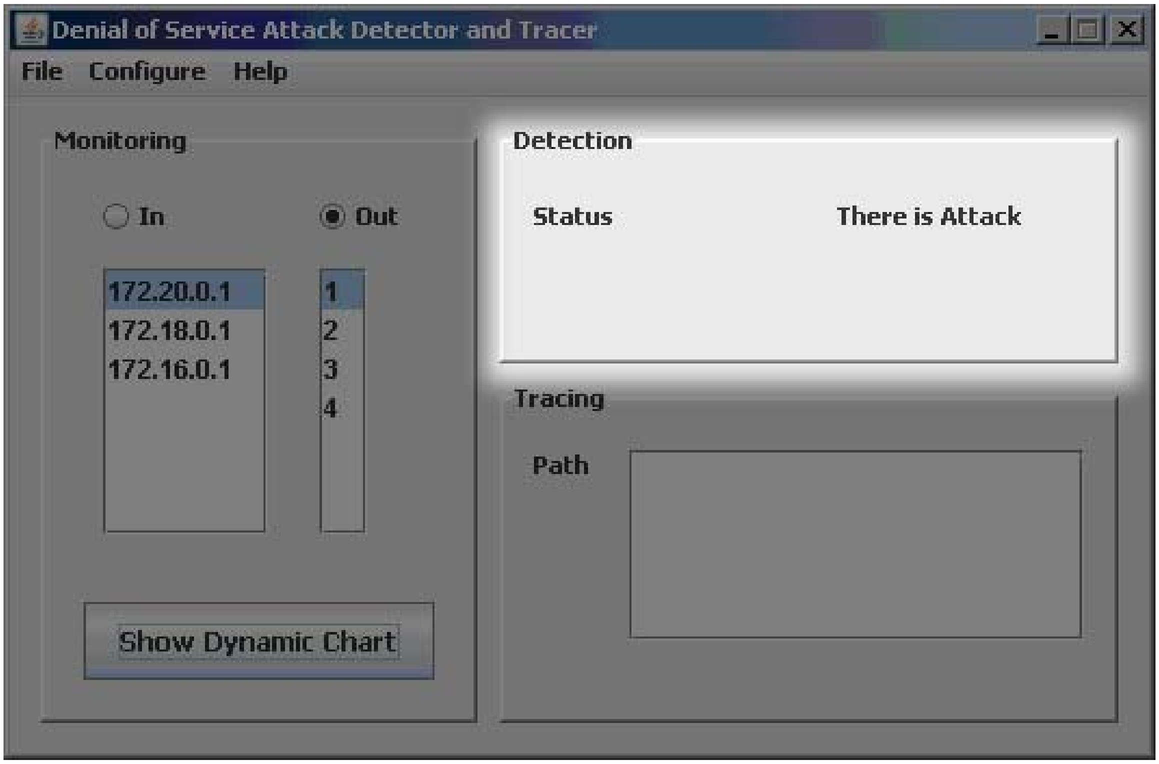


Error in Showing Dynamic Chart

Please make sure an address and an interface are selected and the monitoring is started

14. How to get detection information?

The detection information can be displayed whether there is an attack or there is not in the upper right corner. This is shown in the next diagram.



○ In ● Out

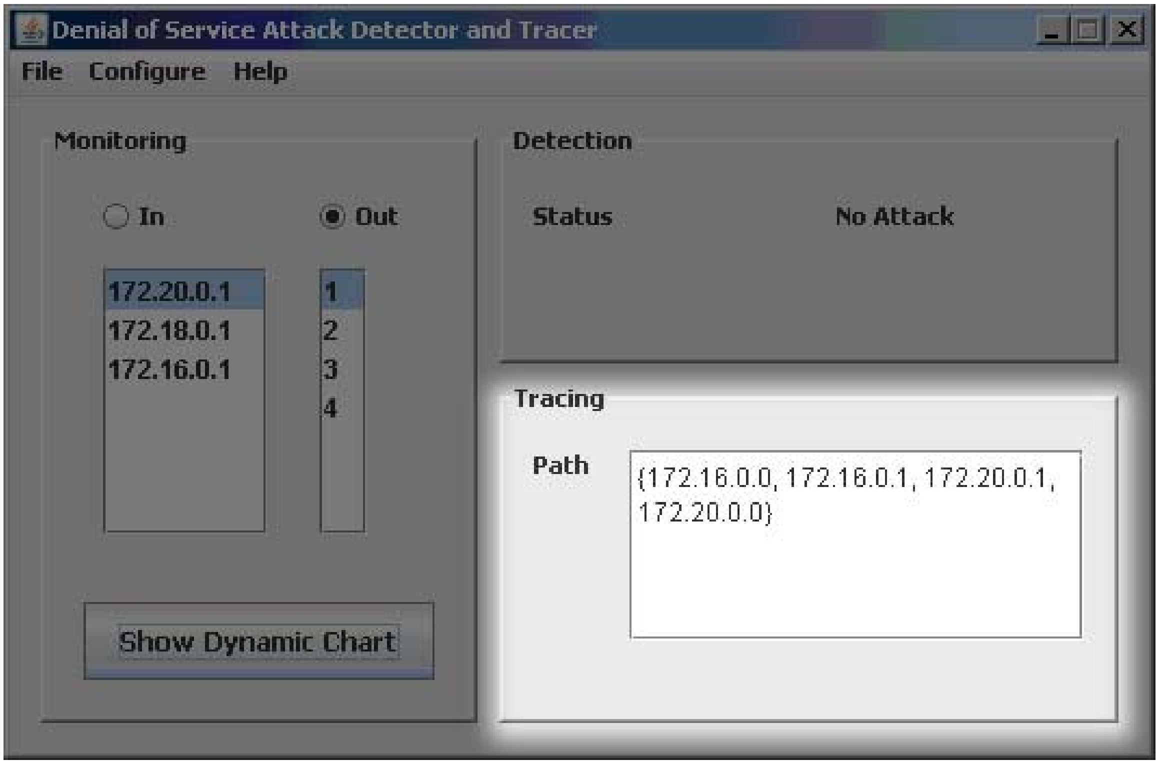
172.20.0.1
172.18.0.1
172.16.0.1

1
2
3
4

Status There is Attack

15. How to get tracing information?

You can get the Traced path from which subnet to any other subnet in the network going through a number of routers from the lower right corner. This is shown in the next figure.



○ In ● Out

172.20.0.1
172.18.0.1
172.16.0.1

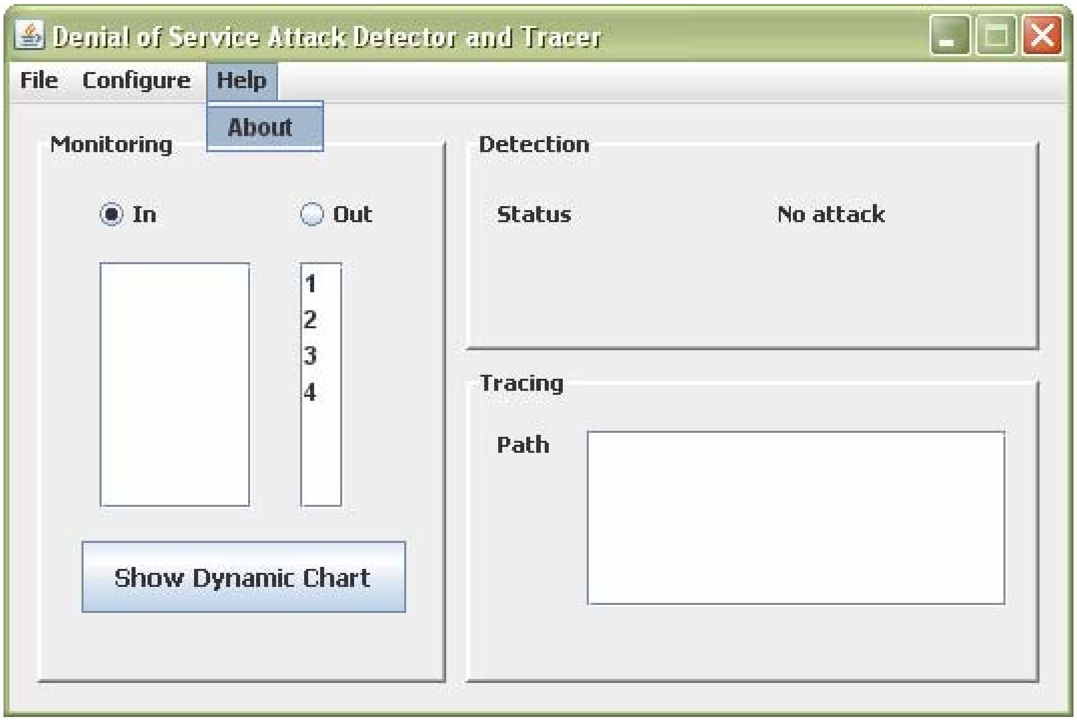
1
2
3
4

Status No Attack

Path {172.16.0.0, 172.16.0.1, 172.20.0.1, 172.20.0.0}

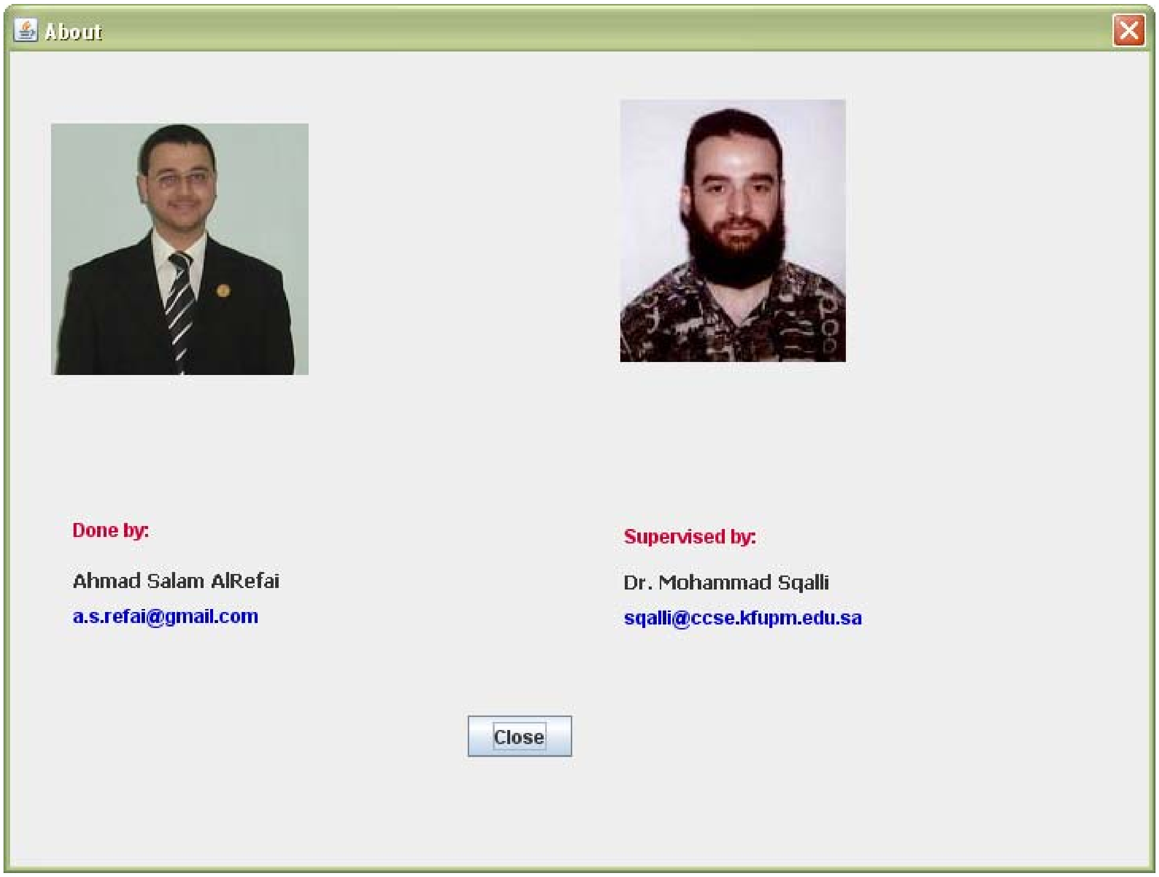
16. How to get Information about the system designer and programmer and his supervisor?

From the “Help” menu go to “About” menu item this is shown below.



Status No attack

After you click the following screen will be displayed.



Done by:

Ahmad Salam AlRefai
a.s.refai@gmail.com

Supervised by:

Dr. Mohammad Sqalli
sqalli@ccse.kfupm.edu.sa