Spamtracker Dokumentation

Installation Instructions for spamtracker components:

This document describes how you can get and install spam-tracker. Further information about spam-tracker can befound at our project page at http://sourceforge.net/projects/spam-tracker/ .

Requirements, or what you should have at your disposal

a.) PHP – enabled webspace for the honeypot website

b.) A webserver accessible from the internet with a servlet engine installed, we recommend to use Jakarta Tomcat version 5.5.9 (http://jakarta.apache.org/tomcat/)

c.) On this webserver, you also need a user account with the rights to run traceroute commands, to access crontab or scheduler functions. These functions should be allowed to manage the server and to deploy a webapplication on it.

d.) A database running on the same server as your webserver. We recommend to use MySQL . Database

e.) An email domain with a catch-all account

f.) JDK 1.5 (http://java.sun.com/j2se/)

g.) For getting the sources you should have installed cvs, on windows be sure that the PATH is set to it! (on windows tortoise doesn't set it automatically)

h.) To compile the sources and to build the jar's you should have installed Apache ANT buildtool (http://ant.apache.org)

i.) Because several jars have to be transferred to the server, you also need a file transfer client that supports ssh

Installation procedure

Download the initial build script

In the download section of our project Page at sourceforge you find the initial ant file, it's called build.xml. With this file you can get and build the rest of spamtracker very comfortable. Download it and place it in the directory where you want to have spam-tracker installed in. Further we will call this the **$InstallDir**.

Get the sources with the build script

Be sure that ANT and CVS are installed correctly, you can test it best at commandline by typing *ant -version* respectively *cvs -version*. Now you can get all sources and compile them with the ant command:

```
yourPrompt>ant getAll
```

After this procedure check whether there exist the following directories

```
$InstallDIR/spamtracker_honeypot
$InstallDir/spamtracker_library
$InstallDir/spamtracker_link
$InstallDir/spamtracker_localizer
$InstallDir/spamtracker_server
$InstallDir/spamtracker_sql
$InstallDir/spamtracker-visualisation
```

Install spamtracker database

We assume, that you have an account to a MySQL database server. First you have to create an empty database. The simplest way to do so is to use the command line like shown below.

```
yourPrompt>mysql -u username -p

mysql>create database yourDatabaseName;
    Query OK, one row affected (0,02 sec)

mysql>\q
```

In the *$InstallDir/spamtracker_sql* directory there is a file called dump.sql. It contains the raw database with the minimum needed structure and dataset for the application. Install them with the following command.

```
yourPrompt> mysql -u username -p yourDatabaseName < dump.sql
```

(There are two other sql files, the one called test_data.sql contains a small dataset for those who want to test the application without waiting for gathered data. The other one is called dump_with_test_data.sql and contains the minimum structure including some test data.)

Modify the configuration files

Set the database properties to your local facts:
After you have downloaded the sources with ant the configuration file for the database connection can be found at

$InstallDir/src/spamtracker_library/src/de/fhkl/zw/medkon/spamtracker/library/db/db.properties

Open this file with an editor and enter your own parameters accordingly for your database connection. The parameters in this file are selfdescribing.

Mailclient configuration:

The configuration file for the getting the spammail from the catch all account can be found at:

```
$InstallDir/src/spamtracker_link/src/de/fhkl/medkon/spamtracker/link/SpamToDB/EmailAccount.properties
```

The parameters in this file are also self-descripting, these are similar parameters as you have to enter when you configure a pop3 mail client.

Honeypot configuration:

The honeypot configuration file can be found at

```
$InstallDir/src/spamtracker_honeypot/database_config.inc
```

In this file you have to define the variables host and port, they must point to the tomcat server where you will install the spamtracker_server.war. Further you have to fill in your email domain with the catch-all account.

Build all stuff

After having modified the property files you can build spam-tracker using the build.xml script with the following ant command:

```
yourPrompt>ant buildAll
```

When this procedure has done all components of spam-tracker are qualified to get installed.

Installing the components

The Linker:

```
$InstallDir/src/spamtracker_link/build/bin/spamtracker_link.jar
```

The Localizer:

```
$InstallDir/src/spamtracker_localizer/build/bin/spamtracker_localizer.jar
```

The linker and the localizer are jobs which should run regularly. They get the mails, and link them with the tracked harvesters and they do the localisation.

To execute them periodical tell on linux the cron-daemon or define a job in the taskplaner on windows a to execute the following commands maybe every 12 hours:

For the linker:

```
cd $InstallDir/src/spamtracker_link/build/bin/ && java
-jar spamtracker_link.jar
```

For the localizer:

```
cd $InstallDir/src/spamtracker_localizer/build/bin/ &&
java -jar spamtracker_localizer.jar
```

The Server:

```
$InstallDir/src/spamtracker_server/spamtracker_server.war
```

The comfortablest way to install your server is to use the tomcat manager application and to deploy the spamtracker_server.war package.

The honeypot:

To install the honeypot you just have to copy the directory $InstallDIR/spamtracker_honeypot to your php enabled webspace. Usually this is done by using an ssh client. For details how this can be done ask your provider.

The Client:

```
$InstallDir/src/spamtracker-visualisation/spamtracker-
client.jar
```

To use the client just execute the spamtracker_client with the command

```
yourPrompt> java -jar spamtracker-client.jar
```

or alternatively just double click the spamtracker-client.jar file within the file system.

How does spamtracker work?

In order to visualise information about spam senders and email harvesters, Spamtracker is split up into three different modules:

- the honeypot
- the tomcat webserver
- the visualisation client

The honeypot:

the honeypot is a website, that generates email addresses each time somebody enters the website. To run the honeypot, you only need a php enabled webspace and a domain with a „catch all“ email account.

Once a harvester or somebody else enters the website, the honeypot determines the current time and the ip-address of the harvester and generates a standard emailaddress using caesar encryption.

Because spamtracker also wants to show that different kinds of harvesters have different levels of harvesting intelligence, the email addresses are prepared in different ways. One emailaddress is presented in the standard way (see below), the others are cloaked, using ASCII and HEX encrypting technology to show how many harvesters are able to recognise spam counter measures.

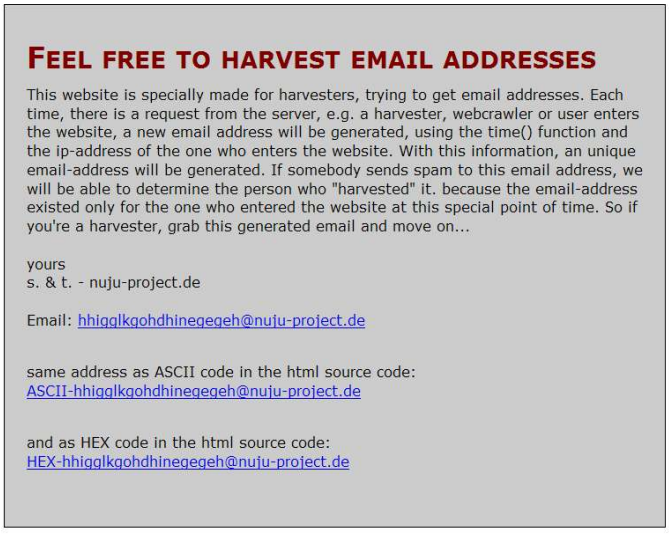


Fig. 1 - screenshot of the website with the generated email addresses

Harvesters will only see this:

Normal:
emailaddress@domain.ending

ASCII:
<a href='mailto:ASCII-
hhigglkgohdhi
negegeh@nuju-&#
112;roject.de'>ASCII-
hhigglkgohdhi

negegeh@nuju-project.de

HEX:
HEX-hhigglkgohdhinegegeh@nuju-project.de

After generating the email addresses, the honeypot sends all collected data about the harvester with a XML-RPC call to the tomcat webserver, where the data will be stored into a database.

The tomcat webserver
The tomcat webserver is the most sophisticated part within spamtracker and fulfilles serveral tasks. First, there is a module to receive data from the honeypot with details of the harvester access. This data will be stored in the database. Second module is the spam mail fetcher. This module is responsible for fetching all mails from a given domain. It is important that the domain is set up to have a „catch all“ function, enabling the spam mail fetcher to receive all messages that are sent to the domain.

Each received mail will be processed, analysed and compared with the harvester database. If a mail was sent to an email address that's not in the harvester database, it's useless. If a mail doesn't contain an advertising link in the mail body such as „buy cheep pills http://www.spampills.com“ it's also useless, because you never will find out who's behind the spam mail. However, there will be enough spam mails to process. After fetching all mails, an object showing the connection between email harvester and spam sender will be created, storing information about the responsible harvester for the received spam mail.

Third, the localising process will be invoked. This process takes the ip-address of the harvester as well as the URL of the extracted advertising link of the spam mail. The localising process will try to determine the geo location of the two addresses. Once the addresses are localised, the data will be build in a ready prepared dataset that's ready for visualising.

The visualisation Client

Connection Manager:

Here you can set up, delete or modify connection details for your tomcat webserver(s). If you have several tomcat webservers, this can be quite convenient.

Connect:

To establish a connection, choose an existing connection in the frame on the left side and click with the left mouse button (lmb) to select it. Once it is colored, click with the lmb on the connect button on the lower right.

New connection:

To set up a new connection, use the four textfields on the right side. Enter a name for the new connection as well as the hostname or server ip of the tomcat server you want to connect with. You also have to enter the path of the servlet. If your servlet runs at http://localhost:8080/spamtracker/servlet, all you have to enter is /spamtracker/servlet . Because tomcat webservers normally use port 8080, it's the default value. If your tomcat webserver runs on another port, alter that value accordingly.

Modify connection:

In case, some connection details have changed, just select the connection you want to modify. The values of the choosen connection will be displayed in the textfields. Just click into the the textfields and enter your new values. Save your changes by clicking the modify button. This will save your changes.

Delete connection:

In case you want to delete a connection, simply select the connection in the left frame and click the delete button below with the lmb. This will delete the selected connection.

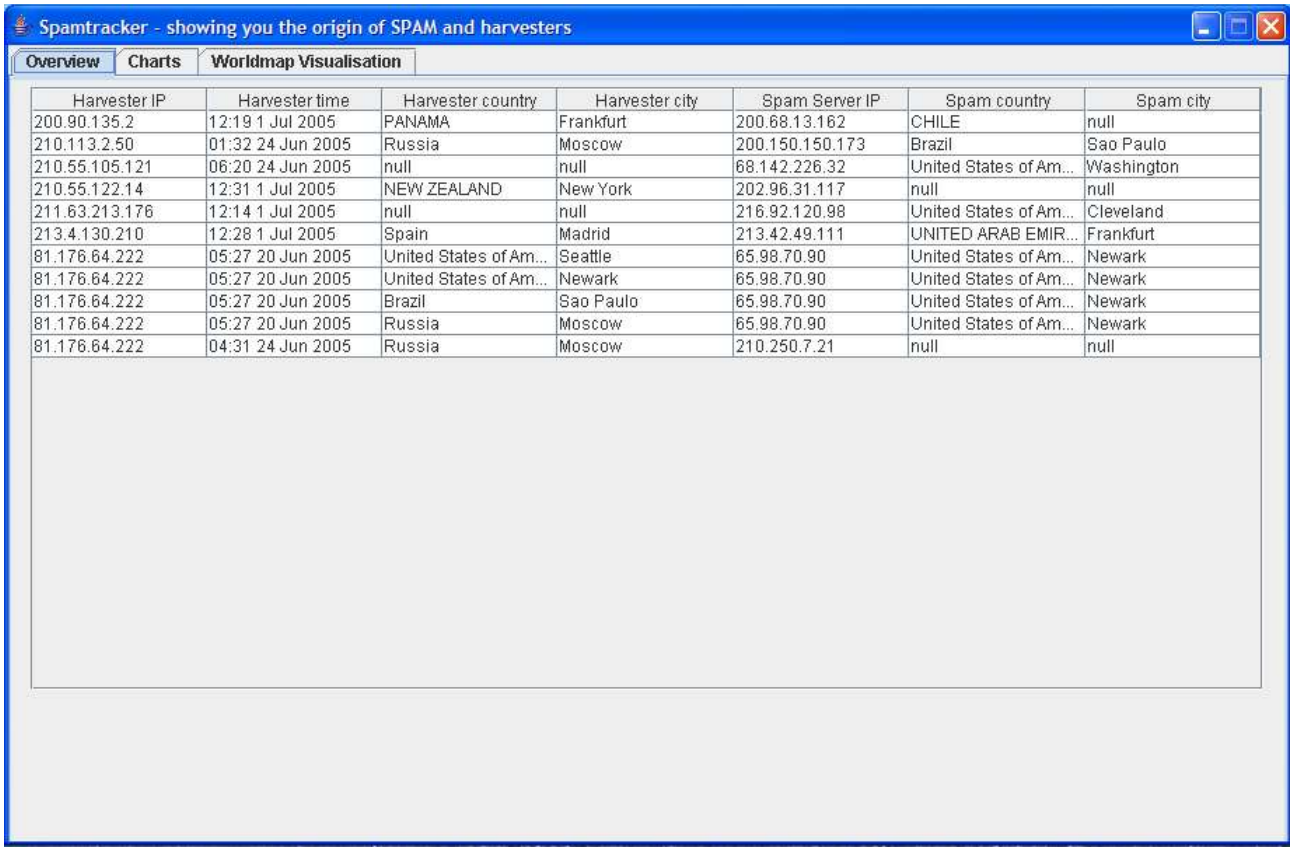
Fig. 2 - Connection Window: Here you can connect, modify, delete or create a new connection to a tomcat webserver

Visualisation:

After having selected a connection, the client will display a window with serveral tabs. Each tab offers you the opportunity to watch different kinds of visualisations showing you the relationsships of harvesters and spammers.

Overview:

Here you will see a table, showing you several rows. Each row is representing a match between the harvester that has harvested your email and the spammer, who has sent you the spam email. You also will learn from which country and city the harvesters were coming from, as well as the geo locations of the advertising URL in the body of the spam emails.



Harvester IP	Harvester time	Harvester country	Harvester city	Spam Server IP	Spam country	Spam city
200.90.135.2	12:19 1 Jul 2005	PANAMA	Frankfurt	200.68.13.162	CHILE	null
210.113.2.50	01:32 24 Jun 2005	Russia	Moscow	200.150.150.173	Brazil	Sao Paulo
210.55.105.121	06:20 24 Jun 2005	null	null	68.142.226.32	United States of Am...	Washington
210.55.122.14	12:31 1 Jul 2005	NEW ZEALAND	New York	202.96.31.117	null	null
211.63.213.176	12:14 1 Jul 2005	null	null	216.92.120.98	United States of Am...	Cleveland
213.4.130.210	12:28 1 Jul 2005	Spain	Madrid	213.42.49.111	UNITED ARAB EMIR...	Frankfurt
81.176.64.222	05:27 20 Jun 2005	United States of Am...	Seattle	65.98.70.90	United States of Am...	Newark
81.176.64.222	05:27 20 Jun 2005	United States of Am...	Newark	65.98.70.90	United States of Am...	Newark
81.176.64.222	05:27 20 Jun 2005	Brazil	Sao Paulo	65.98.70.90	United States of Am...	Newark
81.176.64.222	05:27 20 Jun 2005	Russia	Moscow	65.98.70.90	United States of Am...	Newark
81.176.64.222	04:31 24 Jun 2005	Russia	Moscow	210.250.7.21	null	null

Abbildung 3 - Overview table: Each row represents a match of a harvester and a received spam email.

Charts:

Here you will see the data put into graphs. With the buttons on the right side, you can display pie charts showing you the geo origin of the harvesters, the geo origin of the advertising URL in the spam mail body and the harvester intelligence.

In the harvester intelligence pie chart, you will see how many harvesters are able to harvest normal, ASCII and HEX – coded email addresses.

Below the buttons, there is a textfield showing you the average time from harvest to spam as well as the fastest and the slowest time from harvest to spam.

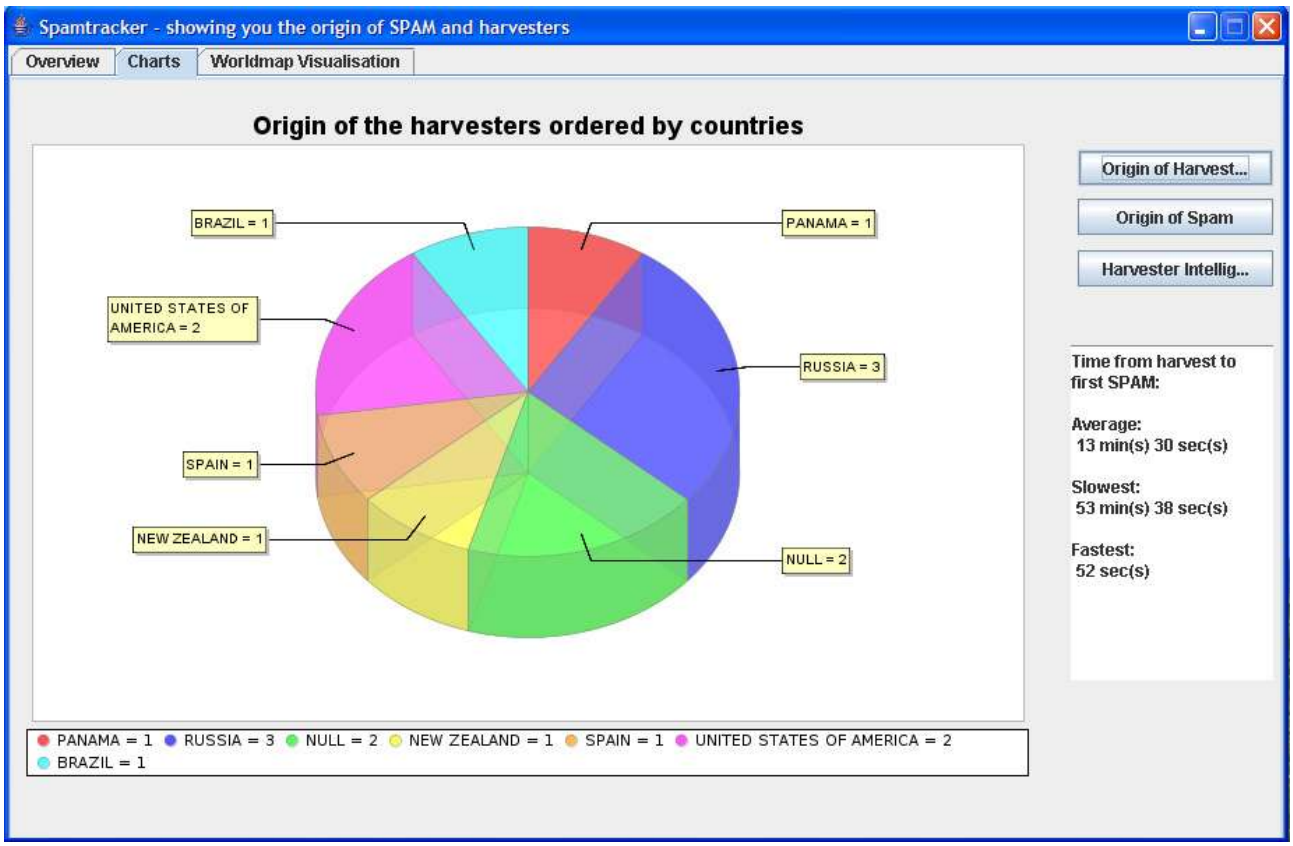


Fig 4 - pie charts: Here you will be informed about the countries the harvesters and spam emails are coming from. There are also statistics about the harvester intelligence and the duration of harvesting and spamming.

Worldmap visualisation:

on this screen, you should first determine the geo location of the domain the spam was sent to. (i.e. If your server, the spam is sent to is located in Germany, just select Germany). The default location is Zweibrücken, Germany. To change that geo position, just click on the select box on the upper right corner to choose the accordant country.

Below the worldmap, you can press three different buttons. The „show spammers“ - button will draw a curve from each geo location that has sent a spam mail(s) to the geo location of your domain. In case there are more than two spam mails from one geo location (e.g. there are 14 spam mails coming from New York, USA) the curves will be drawn randomly, so you can determine that a lot of spam is coming from one special geo location.

The „show harvesters“- button, will also draw curves. This time, the curves will be drawn from the geo locations of the harvesters to the geo location of your domain.

The „show harvesters & spammers“ button draws curves from the geo locations of the harvesters to the geo locations of the spam senders. In this view, you will see which harvester is providing the spammers with harvested email addresses.

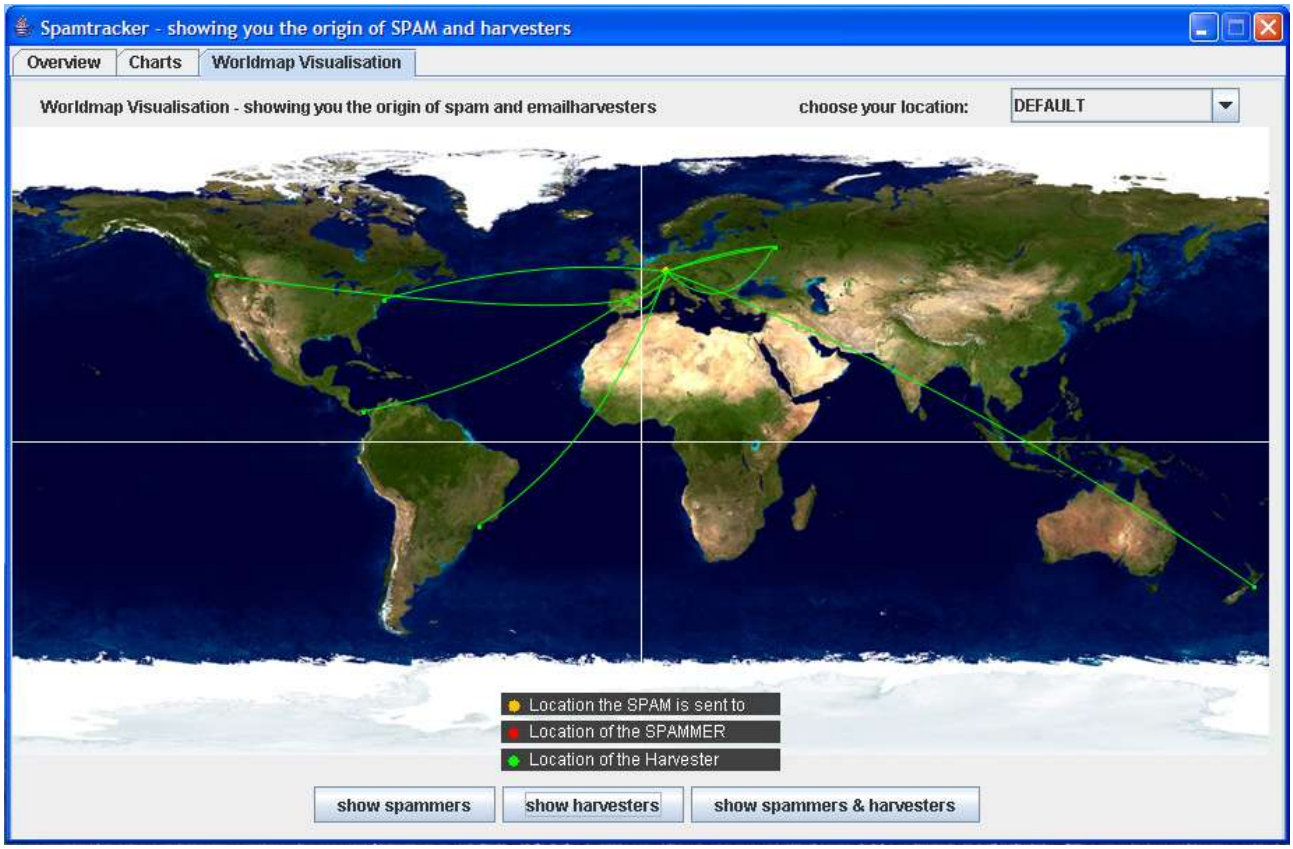


Fig 5 - worldmap : Here you can see how many spam emails or harvesters are coming from wich country. You can also see which harvester is delivering email adresses to which spammer.