



# **EYEWITNESS FORENSIC – WHOIS REPORT Manual**

Version 1.0

# EYEWITNESS FORENSIC – WHOIS REPORT Manual

## Table of contents

1	Introducing.....	3
2	Installation.....	4
3	Start Whois Report.....	4
4	Main Window.....	5
4.1	Registration.....	5
4.2	Select Firefox History DB.....	<b>Fehler! Textmarke nicht definiert.</b>
4.3	Report Section.....	5
4.4	Firefox 3 History.....	<b>Fehler! Textmarke nicht definiert.</b>
4.5	Report generation.....	6
4.6	Quit Whois Report.....	6
5	Showing Reports.....	7
5.1	Saving Reports.....	7
5.2	Printing Reports.....	7
5.3	Editing Reports.....	7
5.4	Quit Report Window.....	8
6	Command line mode.....	<b>Fehler! Textmarke nicht definiert.</b>
7	Support.....	10
7.1	Contact Information.....	10

# **EYEWITNESS FORENSIC – WHOIS REPORT Manual**

## **1 Introducing**

In forensic examinations of hard disks, cell phones and any other digital media, the examiner will get more and more problems with the increasing amount of data. IP Adresses and URLs must be examined and printed for court use. For examination of IPs and URLs this software will be the one, who is able to scan Whois Databases and make a pdf file from it.

# EYEWITNESS FORENSIC – WHOIS REPORT Manual

## 2 Installation

Start WHRSetup.exe for Installation.

The Setup will guide you through the setup routine. While Installation you can see Update Changes in Info Window.

After Installation you can run the program.



Please note that an actual .NET Framework Package (Version 3.5) from Microsoft is necessary to run Whois Report!

## 3 Start Whois Report

By clicking the Whois Report Icon on desktop you can start the application.

# EYEWITNESS FORENSIC – WHOIS REPORT Manual

## 4 Main Window

Registration Information (Mouse Double Click for Registration):  
Whois Report is registered for free use!

Report Information:  
Case Description i.e. Number: 12345/00971223456789  
Evidence Description i.e. Number: IP der Webseite www.tatortgruppe.de  
Case Examiner: Ronny Bodach

IP-Adress Check:  
IP-Adress/URL: www.tatortgruppe.de [Check Up!] [Geo-Location!]

⚠ All the domain data that is visible in the whois search is protected  
⚠ by law. It is not permitted to use it for any purpose other than  
⚠ technical or administrative requirements associated with the  
⚠ operation of the Internet or in order to contact the domain holder  
⚠ over legal problems. You are not permitted to save it electronically  
⚠ or in any other way without DENIC's express written permission. It  
⚠ is prohibited, in particular, to use it for advertising or any similar  
⚠ purpose.  
⚠  
⚠ By maintaining the connection you assure that you have a legitimate  
⚠ interest in the data and that you will only use it for the stated  
⚠ purposes. You are aware that DENIC maintains the right to initiate  
⚠ legal proceedings against you in the event of any breach of this  
⚠ assurance and to bar you from using its whois query.

Domain: tatortgruppe.de  
Domain-Ace: tatortgruppe.de  
Nserver: ns01.1blu.de  
Nserver: ns02.1blu.de  
Status: connect  
Changed: 2008-05-07T12:43:46+02:00

[Holder]  
Type: PERSON  
Name: Ronny Bodach

[Generate Report!] [Show Report!] [Save Report!] [Copy WhoIs Text] [Help!] [About!] [Quit!]

©2009 Eyewitness Forensic - Whois Report | Registered Version 21.06.2009 13:54:19

### 4.1 Registration

Registration:  
Owner 1: Whois Report is registered for free use! [Set Registration]  
Owner 2: Ronny Bodach  
Key: Freeware [Close]

©2009 Eyewitness Forensic - Whois Report | Registered Version

With double click on it, you can set your name in owner2 field, which is loaded into examiner field at startup of application.

### 4.2 Report Section

Case / Evidence Description i.e. Number are two text fields for Report Information which will be listed in the report header with the report date and examiner. Here you can put your case file number and the evidence number too. It is necessary to write in these fields, because report generation does only start with entries in these fields!

## **EYEWITNESS FORENSIC – WHOIS REPORT Manual**

### **4.3 IP Adress Check**

Please put here the IP address or URL.

[Check UP!] – checkst he IP or URL in whois databases and shows result into window.

[Geo-Location!] – if you installed GeoLiteCity.dat database, you can open the geo loaction window.

### **4.4 Report generation**

Press [Generate Report!] and the whole report generation will be started. A progress window shows the current progress of scanning.

After scanning the show report window will open and show up the report. To show the report there are some time to and the application does not response. Be patience and wait this moment.

The Show report window can be shown by pressing the button [Show Report Window!].

With the button [Copy Whois Text!] you can copy the whois response text into clipboard.

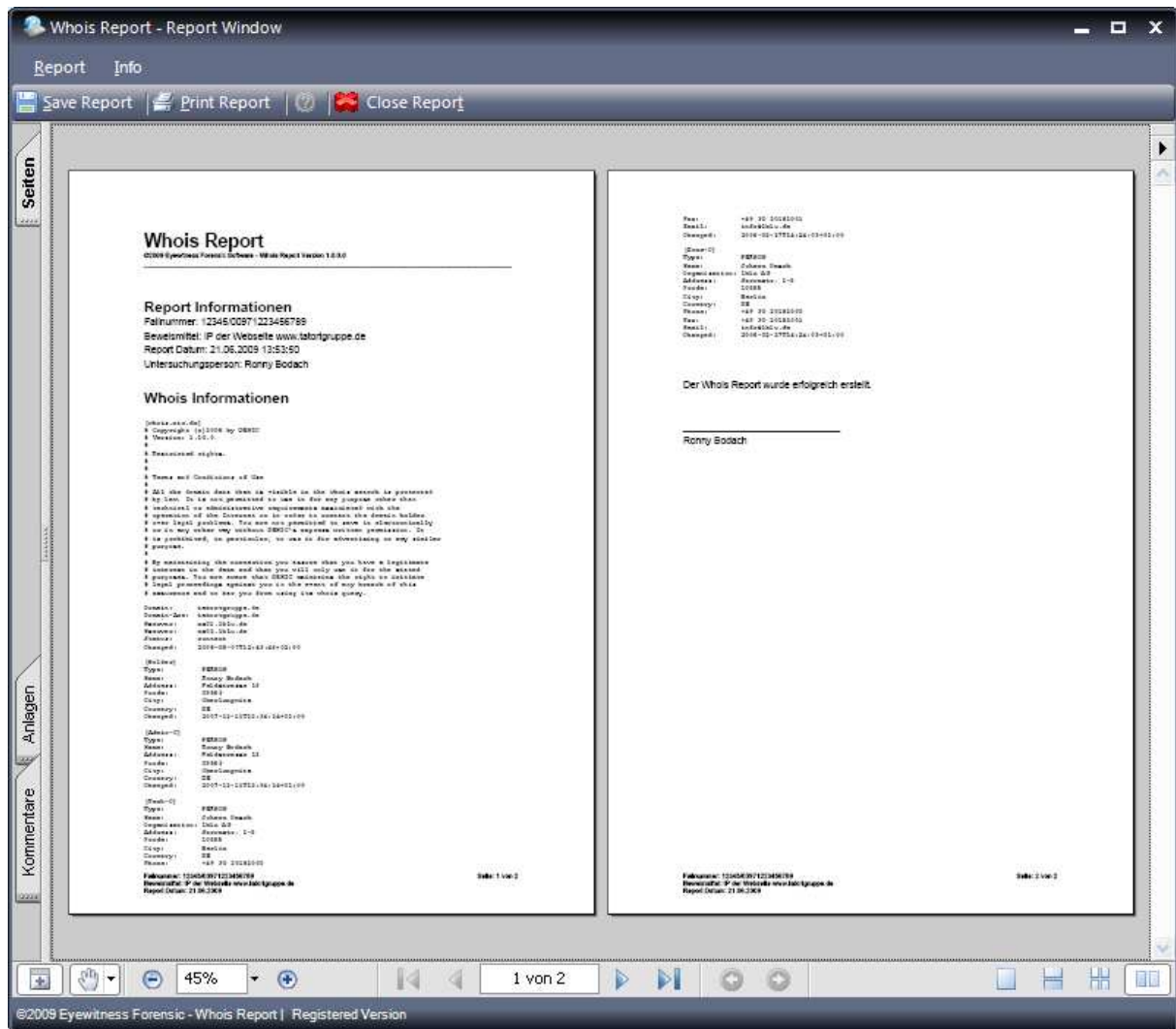
### **4.5 Quit Whois Report**

[Quit] closes the application.

# EYEWITNESS FORENSIC – WHOIS REPORT Manual

## 5 Showing Reports

Here you will be able to see, print or save the report, which is done by scanning.



### 5.1 Saving Reports

With [Save Report] or menu Report [Save Report] you can save the report as standard PDF file (\*.pdf). So you can show it in Acrobat™ Reader once again.

### 5.2 Printing Reports

With the button [Print Report] or menu Report [Print Report] the report can be printed. Into the printer dialog you will be able to set the printer, like any others in Microsoft Windows.

### 5.3 Editing Reports

It is not possible to edit Reports.

## **EYEWITNESS FORENSIC – WHOIS REPORT Manual**

### **5.4 Quit Report Window**

[Close Report] or Menu Report [Close Report] closes the report window.

# EYEWITNESS FORENSIC – WHOIS REPORT Manual

## 6 Geo Location checkup

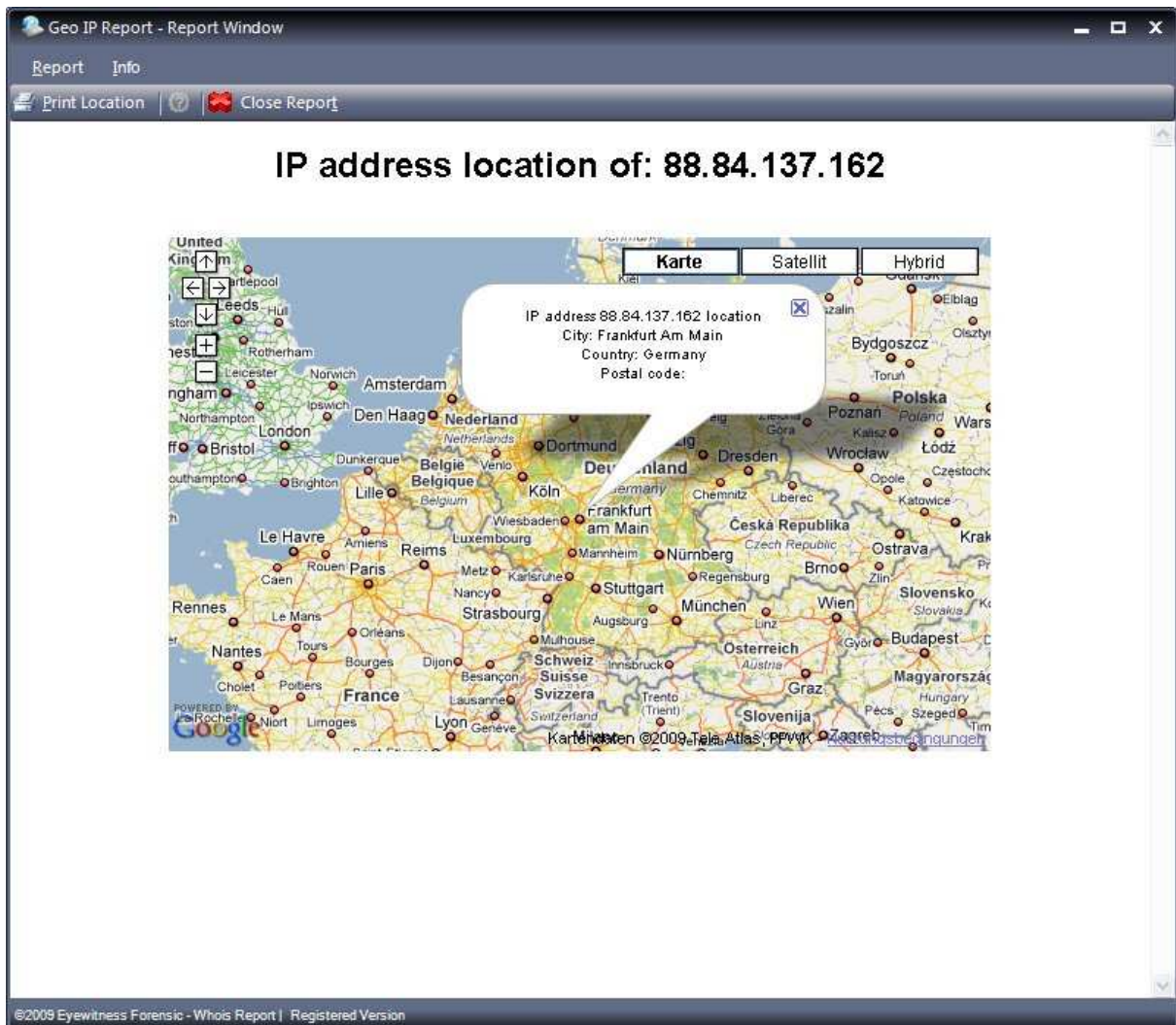
By using the GeoLiteCity database from Geo Tagging specialist maxmind.com you will be able to show and print geo location of IP addresses.

You only have to download *GeoLiteCity.dat* database on following website. Just unzip it to Whois Report application directory.

<http://geolite.maxmind.com/download/geoip/database/GeoLiteCity.dat.gz>

The database will be updated monthly, at the beginning of each month.

The result will be shown in geo location window:



# **EYEWITNESS FORENSIC – WHOIS REPORT Manual**

## **7 Support**

### **7.1 Contact Information**

If you encounter any errors or problems write to support email:

**Ronny.Bodach@tatortgruppe.de**

or look at the FAQ's a tour website:

**[www.tatortgruppe.de](http://www.tatortgruppe.de)**

We will help as soon as possible.

If you will report an error, please send the error.log file within the email to us. This file you will find in user application directory.

Best success at your evidential work!

Yours

Ronny Bodach

# **EYEWITNESS FORENSIC – WHOIS REPORT Manual**

©2009 Eyewitness Forensic – Dipl.-Ing. (BA) Ronny Bodach – All Rights reserved

Whois support done by T. Bhimani

This product includes GeoLite data created by MaxMind, available from  
<http://maxmind.com/>

Report Generation is well done by report.NET, which is licensed under GNU LGPL.  
Report.NET copyright 2002-2004 root-software ag, Bürglen Switzerland  
by O. Mayer, S. Spirig, R. Gartenmann.