



EYEWITNESS FORENSIC – WHOIS REPORT
Deutsches Handbuch

Version 1.0

EYEWITNESS FORENSIC – WHOIS REPORT
Programm Handbuch

Inhaltsverzeichnis

| | | |
|-----|------------------------------------|----|
| 1 | Einführung..... | 3 |
| 2 | Installation..... | 4 |
| 3 | Whois Report Starten | 4 |
| | Das Hauptanwendungsfenster | 5 |
| 3.1 | Registration..... | 5 |
| 3.2 | Report Informationen | 5 |
| 3.3 | IP Adress Check | 6 |
| 3.4 | Report generieren | 6 |
| 3.5 | Beenden von Whois Report | 6 |
| 4 | Reports anschauen | 7 |
| 4.1 | Reports Speichern | 7 |
| 4.2 | Reports Drucken | 7 |
| 4.3 | Reports Editieren..... | 7 |
| 4.4 | Verlassen des Report Fensters..... | 8 |
| 5 | Support..... | 10 |
| 5.1 | Kontakt Informationen | 10 |

1 Einführung

Die digital forensische Auswertung von Computer, Mobiltelefonen, PDA und anderen Datenträgern ist mittlerweile ein sehr breit gefächertes Aufgabengebiet. Die sich ständig vervielfachende Datenmenge und die unterschiedlichen Untersuchungsaufgaben bei der forensischen Auswertung stellt die Auswerter regelmäßig vor das Problem diese enorme Datenmenge zu handeln. Vor allem aber ist die Notwendigkeit der Erstellung eines forensischen Berichts oder Gutachtens stets ein sehr arbeits- und zeitintensives Vorhaben. Die Auswertung von IP Adressen ist eines der vielen möglichen Aufgabengebiete. Für die schnelle Auswertung von IP Adressen und Webseiten ist Whois Report entwickelt. Mit dieser Software lassen sich schnell und bequem Whois Einträge in eine PDF Datei schreiben.

2 Installation

Zur Installation führen Sie die WHRSetup.exe aus.

Das Setup Programm leitet Sie durch den gesamten Installationsprozess. Während der Installation können Sie auch noch einmal die Update Changes im Info Fenster einsehen.

Nach der Installation ist Whois Report einsatzbereit.



Beachten Sie aber bitte, dass ein aktuelles .NET Framework Paket (ab Version 3.5) von Microsoft eine Grundvoraussetzung zum Betrieb von Whois Report darstellt und das Programm ohne diese nicht startet!

3 Whois Report Starten

Starten Sie das Programm über das Symbol auf dem Desktop oder im Programmordner und das Programm Hauptanwendungsfenster erscheint.

EYEWITNESS FORENSIC – WHOIS REPORT

Programm Handbuch

4.3 IP Adress Check

Tragen sie hier die zu prüfende IP Adresse oder URL ein.

[Check UP!] – überprüft die Eintragungen zur eingetragenen IP Adresse oder URL und zeigt diese im unteren Teil der Anwendung an.

[Geo-Location!] – zeigt bei installierter GeoLiteCity.dat Datenbank die ermittelte Geo Location in einem neuen Report Fenster an.

4.4 Report generieren

Über den Button [Generate Report!] wird der Report zur angezeigten IP oder URL als PDF Datei erstellt.

Über den Button [Copy Whois Text!] kann der Whois Abfrage Text in die Zwischenablage kopiert werden.

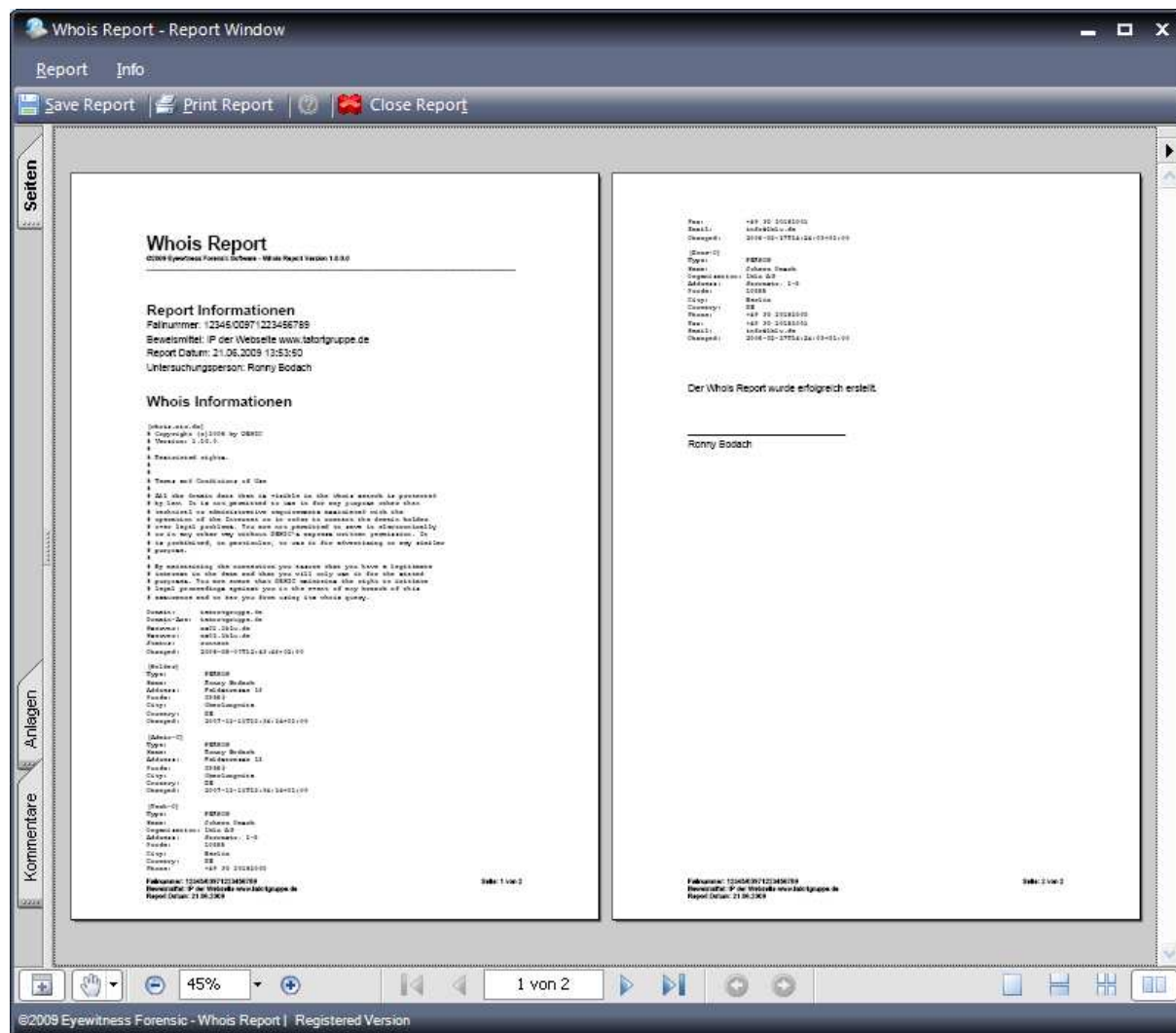
4.5 Beenden von Whois Report

Über den Schließen Button des Fensters oder über den Button [Quit] kann das Programm beendet werden.

EYEWITNESS FORENSIC – WHOIS REPORT Programm Handbuch

5 Reports anschauen

Über den Button [Show Report!] des Hauptanwendungsfensters öffnet sich das Report Fenster. Im Report Fenster ist es möglich den generierten Report einzusehen, diesen zu drucken, zu kopieren und abzuspeichern.



5.1 Reports Speichern

Über den Button [Save Report] oder im Menü Report unter [Save Report] kann der generierte und sichtbare Report als PDF Datei (*.pdf) abgespeichert werden. Er lässt sich somit im Acrobat™ Reader anzeigen.

5.2 Reports Drucken

Die im Report Fenster angezeigten Reports können über den Button [Print Report] oder im Menü Report unter [Print Report] ausgedruckt werden.

Im Printer Dialog können Sie den Drucker zum Ausdrucken auswählen und alle anderen Windows üblichen Druckereinstellungen sind verfügbar.

5.3 Reports Editieren

Reports lassen sich generell nicht Editieren, da diese den nur Lesen Status haben.

5.4 Verlassen des Report Fensters

Über den Button [Close Report] oder im Menü Report unter [Close Report] wird das Report Fenster geschlossen und man gelangt zum Hauptanwendungsfenster zurück. Der generierte Report bleibt dabei erhalten.

EYEWITNESS FORENSIC – WHOIS REPORT Programm Handbuch

6 Geo Location abrufen

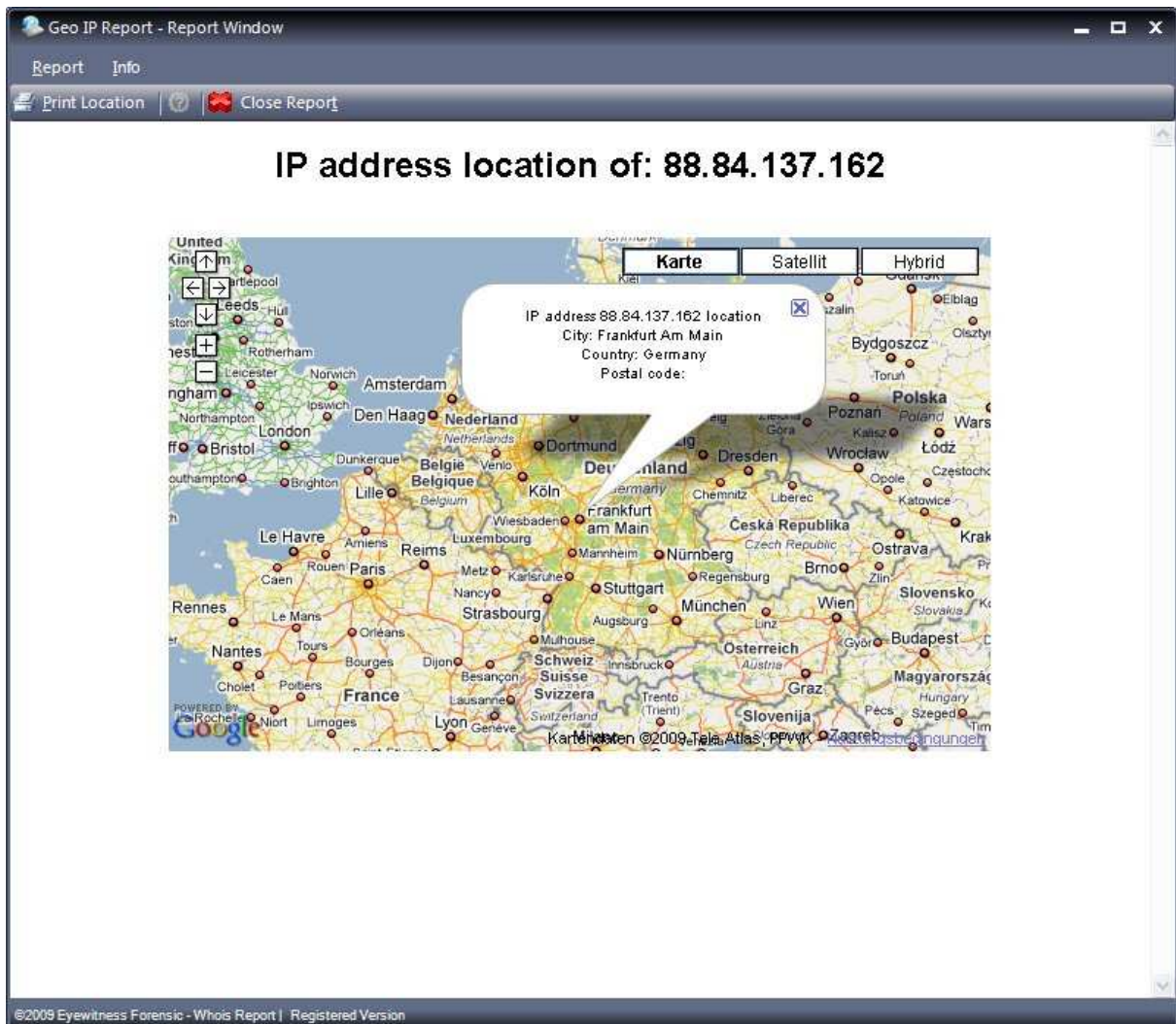
Die Anwendung ist in der Lage mit der GeoLiteCity Datenbank des Geo Tagging Anbieters maxmind.com Geo-Informationen von IP Adressen zu verarbeiten und anzuzeigen.

Dazu ist es notwendig die *GeoLiteCity.dat* Datenbank auf folgender Seite kostenfrei herunterzuladen und in das Whois Programm Verzeichnis abzuspeichern. Die Datenbank muss zur Nutzung jedoch zuvor mit einem EntPacker, wie etwa Winzip entpackt werden.

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

Die Datenbank wird zum Monatsanfang regelmäßig aktualisiert und muss entsprechend oft geupdatet werden um korrekte Ergebnisse zu erzielen.

Das Ergebnis wird im Geo-Location Fenster wie folgt angezeigt werden:



7 Support

7.1 Kontakt Informationen

Bei Fehlern oder Problemen wenden Sie sich bitte an folgende Support Email:

Ronny.Bodach@tatortgruppe.de

oder Besuchen Sie unsere Internet Seite um unsere FAQ's einzusehen:

www.tatortgruppe.de

Wir setzen uns umgehend mit Ihnen in Verbindung.

Ich wünsche Ihnen viel Erfolg bei der Anwendung von Whois Report und hoffe es erleichtert Ihre Arbeit bei der forensischen Auswertung der Digitalen Beweisstücke!

Ihr

Ronny Bodach

EYEWITNESS FORENSIC – WHOIS REPORT
Programm Handbuch

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

Whois Report uses Krypton Toolkit® for Skinning Application.

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.