



EYEWITNESS FORENSIC – ICQ CHAT MESSAGES REPORT
Deutsches Handbuch

Version 2.0

EYEWITNESS FORENSIC – ICQ CHAT MESSAGES REPORT
Programm Handbuch

Inhaltsverzeichnis

1	Einführung.....	3
2	Installation.....	4
3	ICQ Chat Messages Report Starten.....	4
4	Das Hauptanwendungsfenster.....	5
4.1	Registration.....	5
4.2	ICQ Database File.....	6
4.3	Report Informationen.....	6
4.4	Select ICQ Chat User.....	6
4.5	Einen Einzelreport generieren.....	7
4.6	Für alle Chatpartner Reports generieren.....	7
4.7	Beenden von ICQ Chat Messages Report.....	7
5	Reports anschauen.....	8
5.1	Reports Speichern.....	8
5.2	Reports Drucken.....	8
5.3	Reports Editieren.....	9
5.4	Verlassen des Report Fensters.....	9
6	Hex Viewer.....	10
7	Kommandozeilen Modus.....	11
8	Support.....	12
8.1	Kontakt Informationen.....	12

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 Chat Protokollen ist eines der vielen möglichen Aufgabengebiete. Für die schnelle Auswertung von ICQ Chat Verläufen wurde ICQ Chat Messages Report entwickelt. Mit dieser Software lassen sich schnell und bequem ganze ICQ Chat Verläufe in eine oder alle Chatverläufe in mehrere PDF oder CSV Dateien schreiben.

EYEWITNESS FORENSIC – ICQ CHAT MESSAGES REPORT

Programm Handbuch

2 Installation

Zur Installation führen Sie die entsprechende Setup Datei 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 ICQ Chat Messages Report einsatzbereit.



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

3 ICQ Chat Messages Report Starten

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

Beim ersten Starten wird das Programm im unregistered Modus gestartet. Speichern und Kopieren ist in diesem Modus gesperrt.

EYEWITNESS FORENSIC – ICQ CHAT MESSAGES REPORT

Programm Handbuch

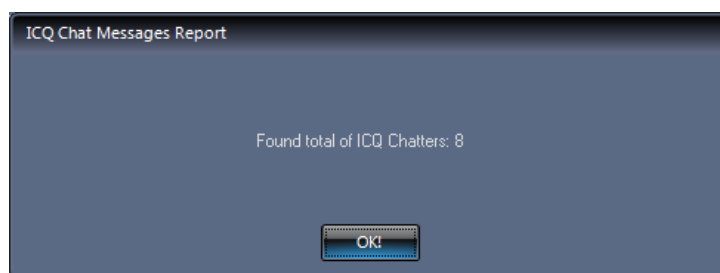
4.2 ICQ Database File

Wählen Sie über den Button [Select ICQ messages database file] die ICQ Chat Verlauf Datenbank aus.

Für ICQ 6.x ist dies die „messages.mdb“ Datei, für ICQ 6.5 Lite und ICQ 7.x ist dies die „messages.qdb“ Datei im ICQ Anwendungsdatenverzeichnis.

Achten Sie darauf, dass die Datenbank nicht geöffnet ist, sonst kann das Programm den Verlauf nicht auslesen.

Nach Auswahl der Datenbank zeigt der nächste Info Dialog die aufgefundenen Chat User mit denen eine Unterhaltung geführt wurde an.



4.3 Report Informationen

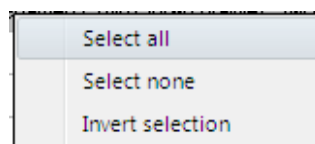
Geben sie in die Textfelder eine Fallnummer und eine Beweismittelbeschreibung ein. Diese Felder sind MUSS Felder, die ausgefüllt werden müssen, sonst kann kein Report erstellt werden.

4.4 Select ICQ Chat User

In der Drop Down Liste kann der zu untersuchende User ausgewählt werden, danach wird im unteren Teil der Anwendung der Chatverlauf angezeigt. Wählen sie hier, durch Anklicken mit der Maus, die Zeilen aus, die in den Report aufgenommen werden sollen.

Die Spalte Data enthält ein @ Zeichen, sofern ein Filetransfer stattgefunden hat. Dies dient für eine schnelle Erkennung bei der Durchsicht des Chats oder aber des Berichtes.

Über die rechte Maustaste ist ein Kontextmenü verfügbar, indem der komplette Chatverlauf ausgewählt, abgewählt oder die Selektierung invertiert werden kann:



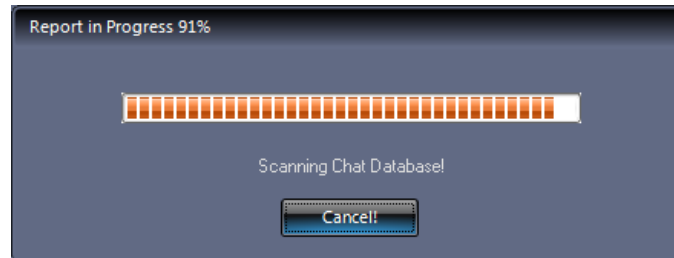
Über den Button [Show Online User Info!] wird ein Browser Fenster mit den bei ICQ hinterlegten Online Informationen des betreffenden Users angezeigt.

EYEWITNESS FORENSIC – ICQ CHAT MESSAGES REPORT

Programm Handbuch

4.5 Einen Einzelreport generieren

Über den Button [Generate PDF Report!] wird der selektierte Teil des Chatverlaufes als Report Datei erstellt und angezeigt.



Über den Button [Export CSV Report!] können die ausgewählten Zeilen des Chatverlaufes als Report im CSV Format gespeichert werden. Sie können damit z.B. im Excel nachbearbeitet werden.

Die CSV Datei wird im Excel eventuell nur beim Öffnen durch das Menü richtig geöffnet, nicht beim direkten öffnen mit einem Doppelklick auf die Datei. Beim Öffnen aus Excel wird nach Einstellungen gefragt, wie getrennte Breite, Semikolon als Trennzeichen und " als Texterkennungszeichen. Damit kann der Text richtig importiert werden.

4.6 Für alle Chatpartner Reports generieren

Über den Button [Export all contacts to PDF!] ist es möglich automatisch von allen Chatpartnern separate PDF Reports in ein wählbares Ausgabeverzeichnis zu erstellen.

Über den Button [Export all contacts to CSV!] ist es möglich automatisch von allen Chatpartnern separate CSV Dateien in ein wählbares Ausgabeverzeichnis zu erstellen.

Es werden dabei immer alle Nachrichten in die jeweiligen Report Dateien übernommen und pro Chatkontakt eine Datei erstellt. Damit ist es bei einer hohen Anzahl von Chatpartnern möglich alle Chats in einem bearbeitbarem Format (PDF, CSV) zu extrahieren und diese einzeln zu sichten.

Diese Funktion ist vor allem bei der Bewältigung von Massendaten hilfreich.

4.7 Beenden von ICQ Chat Messages Report

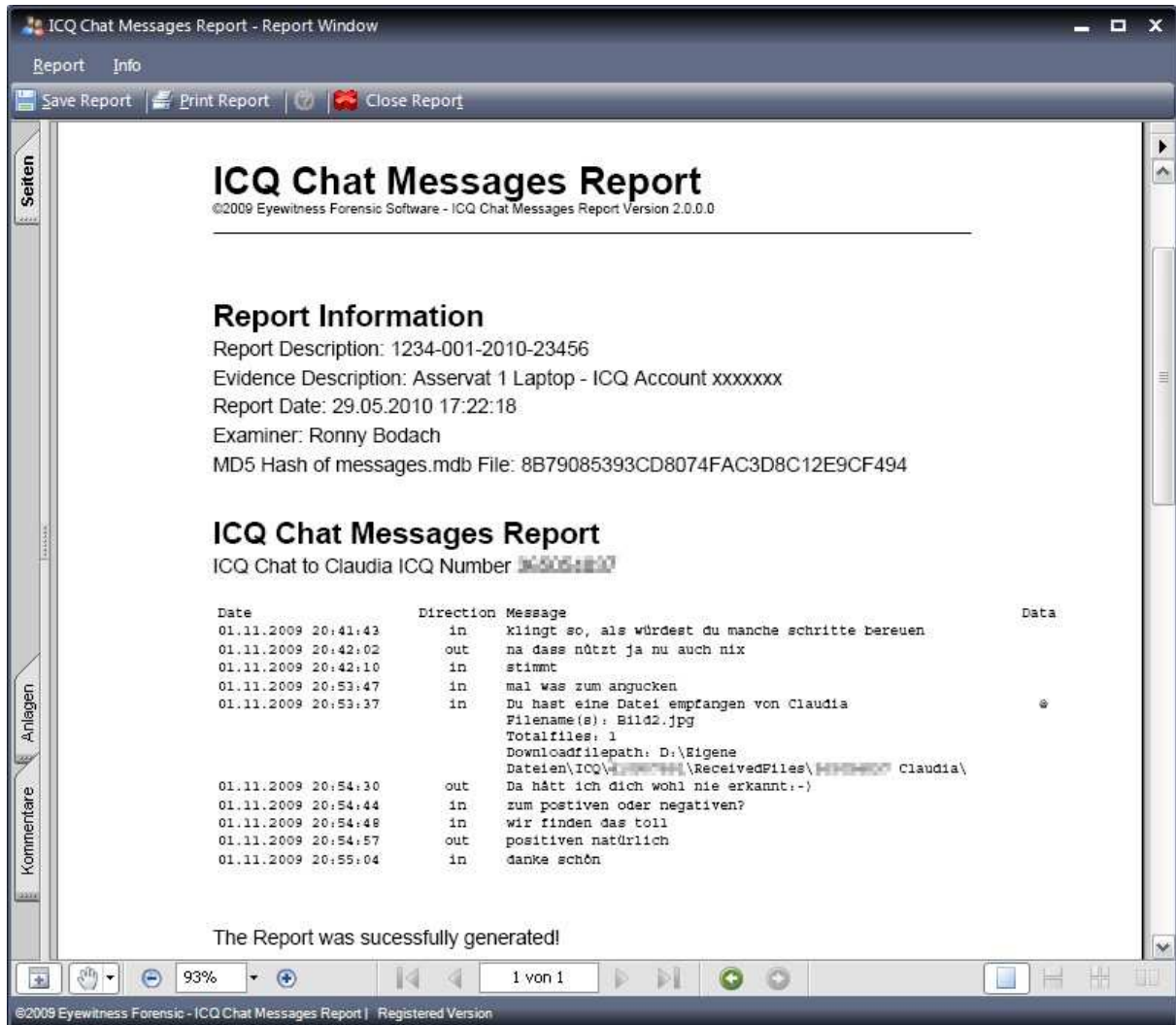
Über den Schließen Button des Fensters oder über den Button [Quit] kann das Programm beendet werden.

EYEWITNESS FORENSIC – ICQ CHAT MESSAGES 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 und abzuspeichern.



5.1 Reports Speichern

Über den Button [Save PDF 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

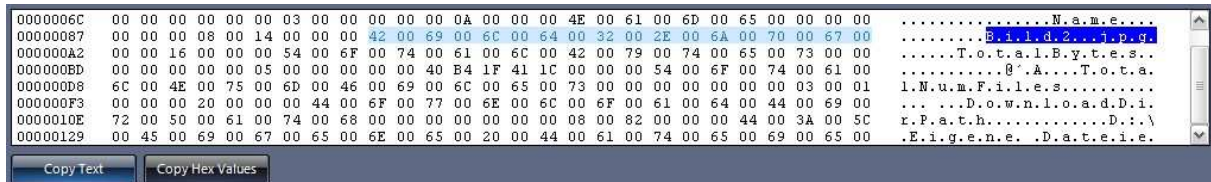
Über den Button [Close Report] oder im Menü Report unter [Close Report] wird das Report Fenster geschlossen und man gelangt zum Hauptanwendungsfenster zurück. Der generierte Report bleibt dabei erhalten.

EYEWITNESS FORENSIC – ICQ CHAT MESSAGES REPORT

Programm Handbuch

6 Hex Viewer

ICQ speichert alle eingehenden wie ausgehenden Nachrichten als Binäres Feld mit diversen Zusatzinformationen in der Datenbank. Dieses Feld kann mit Hilfe des Hex Viewers sichtbar gemacht und ausgelesen werden.



Im Hex Viewer ist es möglich den Inhalt der Binärdaten als Hex sowie als Text Werte (Unicode) zu selektieren und zu kopieren.

Es ist möglich dass die in den Binärdaten hinterlegten Nachrichten auf weitere unsichtbare Zeichen, Http Images oder HTML/PHP Code verweisen, welche im reinen Messages Text nicht angezeigt werden. (Beispiel: IM Phishing)



ICQ Messages mit HTML/PHP werden ICQ intern wie HTML Seiten angezeigt. Es ist damit möglich Fremdcode, wie auch Schadcode per ICQ Nachricht einzuschleusen. Diese Möglichkeit ist auch schon bei einer Kontakteinladung gegeben!

EYEWITNESS FORENSIC – ICQ CHAT MESSAGES REPORT

Programm Handbuch

7 Kommandozeilen Modus

ICQ Chat Messages Report lässt sich auch über die MS-Dos Kommandozeile aufrufen. So könnte ein Aufruf des Programms per Kommandozeile aussehen:

```
C:\>"ICQ Chat Messages Report.exe" "Laufwerk\Pfad\messages.mdb" oder „messages.qdb“
```



Es ist möglich ICQ Chat Messages Report somit in andere Forensic Programme einzubinden. Im ILook oder aber auch X-Ways Forensics lässt sich ICQ Chat Messages Report z. B. somit als ICQ Chat Viewer einbinden.

EYEWITNESS FORENSIC – ICQ CHAT MESSAGES REPORT
Programm Handbuch

8 Support

8.1 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 ICQ Chat Messages Report und hoffe es erleichtert Ihre Arbeit bei der forensischen Auswertung der Digitalen Beweisstücke!

Ihr

Ronny Bodach

EYEWITNESS FORENSIC – ICQ CHAT MESSAGES REPORT

Programm Handbuch

©2008-2010 Eyewitness Forensic – Dipl.-Ing. (BA) Ronny Bodach – All Rights reserved

ICQ and their logos are trademarks of ICQ LCC.

ICQ Chat Messages Report uses Krypton Toolkit® for Skinning Application.

ICQ Chat Messages Report uses MS ADODB Jet database support for ICQ 6.x and ADO.NET 2.0/3.5 SQLite Data Provider using SQLite 3.x written by Robert Simpson for ICQ 7.x support.

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.

This Software uses Be Hex Editor, copyright 2007-2009 by Bernhard Elbl.