

Quick **Start** Guide



Paraben's[®]
Chat Examiner[®]

Paraben's
Chat Examiner
Getting Started Guide



Contact Information

Mailing Address

P.O. Box 970483
Orem, UT 84097-0483
USA

After Hours Support

1.801.369.8210

Email Support

forensicsupport@paraben.com

Forensic Support

Business Hours:
9:00 AM to 5:30 PM MST

Main Fax

1.801.796.0610

Main E-mail

forensics@paraben.com

Product Information

Main Phone
1.801.796.0944

Table of Contents

Introducing Paraben's Chat Examiner.....	4
Chat Examiner Related Applications.....	5
P2Commander.....	5
Installing and Configuring Chat Examiner.....	6
Computer System Requirements.....	6
Installing Chat Examiner.....	7
Registration.....	8
Working in Chat Examiner.....	10
Exploring the Chat Examiner Interface.....	10
Chat Examiner Data Examination Process.....	12
Creating a Case.....	13
Adding Evidence.....	15
Examining Evidence.....	21
Creating Reports.....	22
Exporting.....	24
Additional Features.....	25

Introducing Chat Examiner

Paraben Chat Examiner is a program designed to read, analyze, and report on supported chat program data. It supports the following types of messenger clients:

- Hello
- ICQ 1999-2003a
- ICQ 2003b
- ICQ6
- ICQ7
- Miranda
- MSN and Windows Live
- Skype
- Trillian
- Yahoo!

Chat Examiner Related Applications

Paraben makes one application related to Chat Examiner.

- Paraben P2 Commander

Paraben P2 Commander

Paraben's P2 Commander is a comprehensive digital forensic tool designed to handle more data, more efficiently while adhering to Paraben's P2 Paradigm of specialized focus on the entire forensic exam process. P2 Commander utilizes Paraben's advanced plug-in architecture to create specialized engines that examine elements like e-mail, network e-mail, chat logs, file sorting, Windows registry analysis and more—all while increasing the volume of data that can be processed and utilizing resources through multi-threading and task scheduling.

Installing and Configuring Chat Examiner

The installation process has two parts:

- Installing
- Licensing

After installing Chat Examiner, you must register the program. Without a registration, Chat Examiner can be used for 30 days or 23 uses. This section outlines the installation process.

Computer System Requirements

The following computer system requirements are needed to use Chat Examiner.

- Operating system: Microsoft Windows 2000 or later 32 bit OS.
- .Net Framework version 3.0 or later.

Installing Chat Examiner

When you place the installation CD in your computer, the auto-run feature launches the installation program that guides you through the installation process. If the auto-run feature needs to be started manually, you can click autorun.exe in the root directory of the installation CD.

To install Chat Examiner

1. On the Welcome screen, click **Install Now**
2. When the install wizard is displayed, click **Next**.
3. Accept the license agreement, and then click **Next**.
4. Do one of the following:
 - Type the location on the folder where you want to install Chat Examiner, and then click **Next**.
 - Click **Browse** and select the location of the folder where you want to install Chat Examiner, and then click **Next**.
 - Click **Next** to keep the default location.
5. Click **Install**.

Registration

Install the software: Install Chat Examiner from the CD or from your registration site account at <http://register.paraben-forensics.com>

If your license came with a dongle:

Install Chat Examiner from your CD and plug in your dongle. As long as the dongle is plugged in, Chat Examiner will work. To ensure you have the latest version, you will want to visit your registration site account frequently. Use the Dongle Manager program to update your dongle to work with new versions.

If you don't have a dongle:

Go to <http://register.paraben-forensics.com>, log into your account, click on your Product ID (PID), and download a key.lic file. Save the license key into the same folder Chat Examiner is installed in and run Chat Examiner.

If you ordered a dongle but want to use Chat Examiner before your dongle arrives:

Go to <http://register.paraben-forensics.com> , log into your account and click your dongle number under “USER DONGLES”. Click “Get temporary key” to access your temporary license key (a self-extracting archive that extracts the key to the Paraben’s Chat Examiner installation folder). This key allows you to use the full version of Chat Examiner for 20 days, giving time for the dongle to arrive. If you’ve installed a newer version of Chat Examiner before your dongle arrives, you will need to update it using the Dongle Manager.

Working in Chat Examiner

When your license key is in place, you can begin using Chat Examiner. If you have not yet obtained a license, Chat Examiner functions for 30 days or 23 uses.

Exploring the Chat Examiner Interface

The Chat Examiner has four main information panes as displayed in the following image.

The panes are:

- Case Explorer pane – Upper left – Displays the structure of the added chat database evidence.
- Data Viewer pane – Upper right – Displays the contents of the selected node in the Case Explorer pane.
- Properties pane – Lower left – Displays properties of the selected item.
- RTF View pane – Lower right – Displays the conversation in a convenient way.

NOTE: You can add, remove, or resize panes as you work to see more or less information. If you want to reset the display to the default settings, in the main menu you can click **View > Restore Layout**.

Paraben's Chat Examiner - test case.chx

File View Tools Help

New Open Add Evidence Back Forward Case History Options

Search Generate Report Add Bookmark

Case Explorer

Items

- test case
 - j88888888831
 - Yahoo Database
 - j88888888831
 - Messages
 - arlytan123
 - 2010.04.06
 - gina_sun2007

Path: 88888831/YahooDatabase/j8888888831/Message/arlytan123/2010.04.06_0 Go

<input type="checkbox"/>	Sender	Time	Message
<input type="checkbox"/>	j88888888831	06.04.2010 5:12:17	Hello, Arly
<input type="checkbox"/>	arlytan123	06.04.2010 15:12:22	Hi! I've found you at last!!!!
<input type="checkbox"/>	j88888888831	06.04.2010 15:12:44	oh, I'm so so happy!!! haven't seen u for
<input type="checkbox"/>	arlytan123	06.04.2010 15:13:02	now I'll always be here.
<input type="checkbox"/>	arlytan123	06.04.2010 15:13:10	and won't go anywhere

Finished Total: 5

RTF View

j88888888831 06.04.2010 5:12:17 : Hello, Arly
 arlytan123 06.04.2010 15:12:22 : Hi! I've found you at last!!!!
 j88888888831 06.04.2010 15:12:44 : oh, I'm so so happy!!! haven't seen u for ages
 arlytan123 06.04.2010 15:13:02 : now I'll always be here.
 arlytan123 06.04.2010 15:13:10 : and won't go anywhere

Change color j88888888831

Common Log Tasks RTF View

Case Explorer Bookmarks

Properties

Common

Messages 5

Chat Examiner Data Examination Process

When you work in Chat Examiner, there are several functions that you need to be familiar with and perform in order to store and examine the evidence. The functions include:

- Create a case
- Add evidence
- Examine evidence
- Create reports
- Export data


Each of these is outlined in this guide, but more comprehensive information is available in the help file that is located in Chat Examiner under the Help menu.

Creating a Case

When you initially start Chat Examiner, you need to create a case. If you attempt to add evidence before creating or opening a new case, the New Case wizard is displayed and asks you to name the case file so that it can store your case data. This ensures that your case data is automatically saved, and reduces the risk of information loss due to equipment failure.

Creating a case consists of naming the file, and providing details related to the case. The New Case wizard provides you with fields that you can use to type your file information.

To create a new case:

1. In the main menu, click **File** > **New Case** or in the tool bar, click **New**. ()
2. On the Welcome page, click **Next**.
3. On the Case Properties page, do the following:
 - In the Case Name field, type a name for your case. The case name is required and serves as the name of the file in which your case is stored. Initially Chat Examiner saves your case in the folder where Chat Examiner is installed. Case names should be descriptive.
 - Type a description of the case. While not required, this data can be very useful if time has passed and you are reexamining the case, or if someone else needs to look at the case.
 - Click **Next**.

4. On the Additional Information tab, optionally type the following information. Each field in this tab uses menus that remember information you have previously typed:

- Investigator name
- Agency/Company
- Phone number
- Fax number
- E-mail
- Address
- Comments

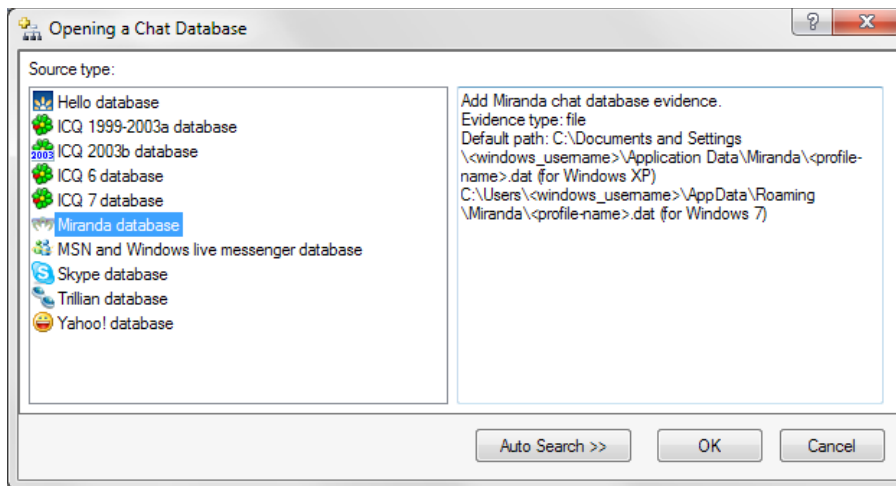
Click **Finish**.

NOTE: This information is displayed in reports that you create.

Adding Evidence

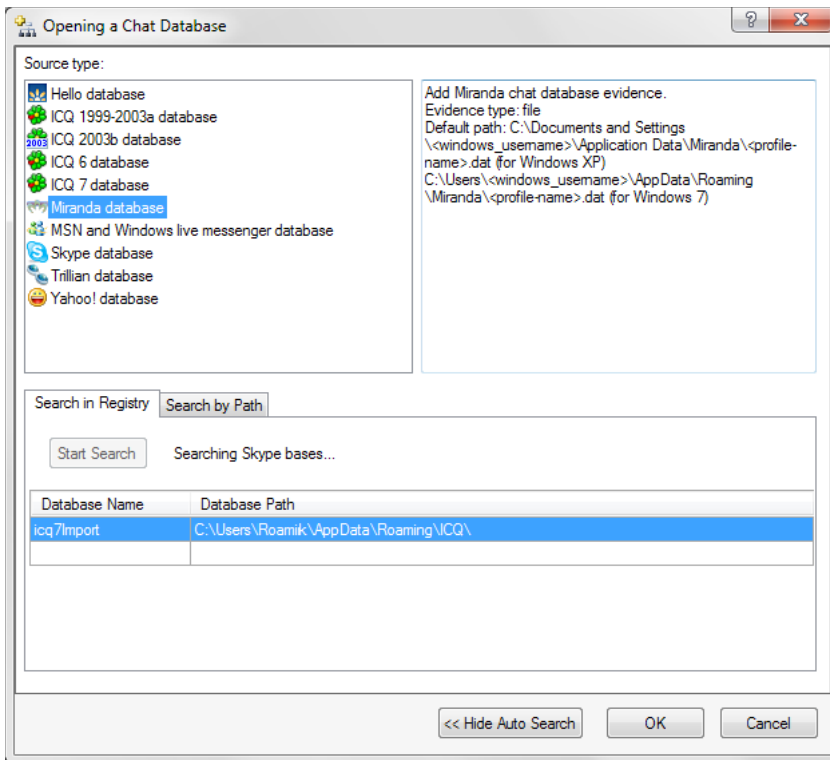
After creating your case, you need to add the evidence. Adding evidence is the process of selecting which information you want to analyze. Chat Examiner allows you to add the chat database evidence in one of two ways:

- Manually selecting the folder with chat database evidence of the known type;
- Automatically detect the chat database in Registry or defined location.



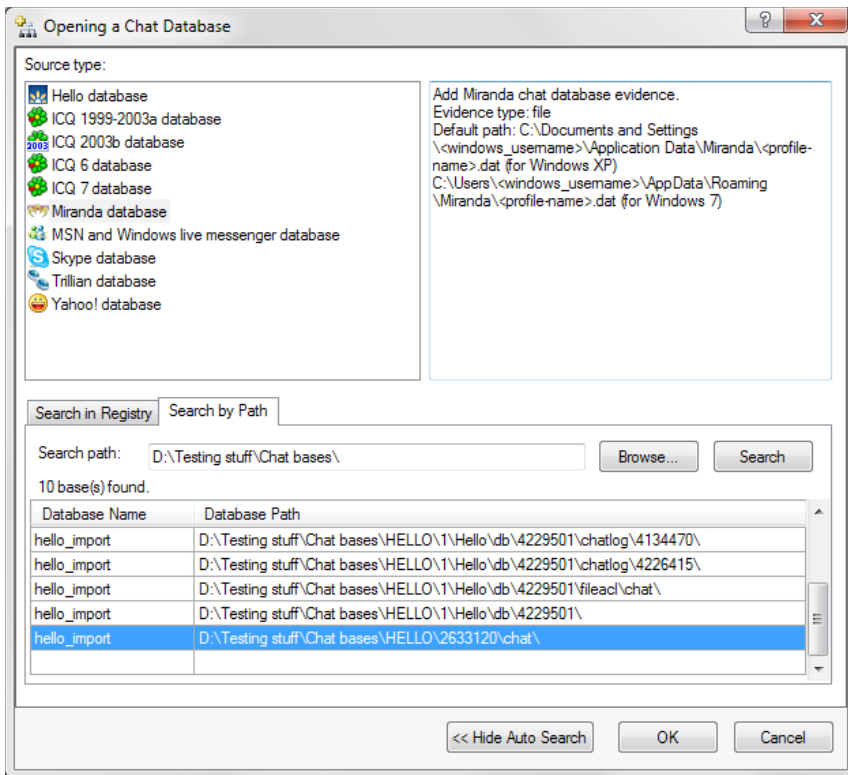
To add evidence manually:

1. Create a case. See [Creating a Case](#) on page [12](#).
2. Click **Add Evidence** or click **File >Add Evidence**.
3. In the Add New Evidence window, select the type of evidence that you want to add, and then click **OK**.
4. Browse to the file or folder you want to select, and then click **OK**.
5. Type the name for the evidence. By default, this is the name of the evidence you select when you browse. It is the name that is displayed in the list of evidence objects. Click **OK**.
6. Select from the options you want to use when adding the evidence, then click **OK**.



To search for installed chat database in Registry:

1. Create a case. See [Creating a Case](#) on page [12](#).
2. Click **Add Evidence** or click **File >Add Evidence**.
3. Click **Auto-search** and select the **Search by Registry** tab.
4. Click **Start Search**.
5. In the list of detected chat databases, select the required database and double click it.
6. Type the name for the evidence. Click **OK**.



To auto-detect chat database in the specified folder:

Create a case. See [Creating a Case](#) on page 12.

Click **Add Evidence** or click **File >Add Evidence**.

Click **Auto-search** and select the **Search by Path** tab.

Do one of the following:

- Click **Browse** and navigate to the folder where the chat database should be auto-detected.
 - Enter the path to the folder where the chat database should be auto-detected manually in the **Search Path** field.
1. Click **Search**.
 2. In the list of detected chat databases, select the required database and double click it.
 3. Type the name for the evidence. Click **OK**.

After you add the evidence, it is displayed in the Case Explorer pane of the application. You can expand and view it.

Examining Evidence

Examining chat database evidence means viewing the chat history, attached files (only in Hello chat database evidence). Chat Examiner allows you to view the chat history in two ways: in the Data Viewer pane and in RTF View pane. It is convenient to view data in RTF View pane as the chat history is displayed in one file where all messages are given one by one in the following format: **<Sender nickname> <Time> <Message text>**. You can also change font and background colors in the viewer.

To view chat database evidence:

1. In the main menu, click **View > Viewers**, and ensure that all viewer options are selected.
2. In the Case Explorer pane, expand the nodes until you reach the node with conversation you want to look at.
3. Conversation is displayed in the Data Viewer pane (upper right) and in the RTF View pane (lower right).
4. Change the color settings in the RTF View pane by clicking **Font color** or **Background color** and selecting the required color.
5. Click the edge of the pane to resize it if necessary.

NOTE: Properties of the selected item are displayed in the Properties pane in the lower left of your screen.


Creating Reports

Chat Examiner lets you export four different standard reports. The following types of reports are available:

- HTML investigative report – This creates a graphical report in HTML format. The report allows you to add all evidence and include thumbnails of files and links to files in the report (if any are available).
- Simple text report – This report is exported to a ***.txt** file. It has options for including or leaving out specific information, but all evidence is listed in the text format.
- CSV text report – Exports information into a spreadsheet. This type of report has options similar to the text report.
- HTML evidence summary report – Provides a brief overview of the evidence for managers and supervisors.

When you create reports, you can select specific information that you want to add to the report. You can select this information by checking the boxes to the left of the nodes in the Case Explorer pane or Data Viewer pane. You can also export all evidence.

To create reports:

1. If you want to create a report that displays specific data, navigate to the data in the Case Explorer pane or the Data Viewer pane and check the box next to the node/row you want to include.
2. Click **Generate Report** () or from the main menu, click **File > Generate Report**.
3. In the initial screen of the report wizard, select the type of report and the location where you want to save the report. By default, the report and all associated files are saved in a new folder named using the file name of the case.
4. Click through the remaining screens in the wizard and select the options you want to display in your reports. These include Investigator Information, Bookmarks, chat database evidence options, and logs and supplementary files. The report options change depending on the type of report you select. For complete information on all report options, see the help file in Chat Examiner.
5. Click **Finish** to begin the process of creating the report. Depending on the size and options you select when creating the report, the creation process might take several minutes.

Exporting

Chat Examiner allows you to export chat history to a ***.csv** file. You can use the check boxes in the Data Viewer pane to select which data you want to export.

To export data to a spreadsheet:

1. In the **Data Viewer pane**, check the boxes next to the messages you want to export.
2. Right click and select **Export Info to Spreadsheet**.
3. Browse to the location where you want to place the file, then click **Save**.
4. Selected data is exported to a ***.csv** file.

Additional Features

This quick start guide has the basic features you need to begin working in Chat Examiner. However, Chat Examiner has a powerful set of additional features that you can use to make your analysis easier and more complete. These are listed in this section with a brief description. Complete documentation for each is available in the Chat Examiner help file:

- **Search** – Allows you look for required data in the evidence.
- **Bookmarks** – Creates links that let you quickly find locations in the evidence.
- **Case History** – Displays a list of tasks and processes performed that relate to the case. It displays dates with the events.
- **Options Wizard** – Lets you change and save the default settings for Chat Examiner.