Belkasoft

In this brochure you will find information about the following products:

Belkasoft Forensic IM Analyzer

(Home, Standard, Professional, Ultimate and Intelligence editions)

Belkasoft Forensic Studio

(Home, Standard, Professional and Ultimate editions)

About

Forensics made easier

Belkasoft is an independent software vendor. We specialize in computer forensics and system software for the Windows platforms. With our slogan "Forensics made easier", we are trying to make IT forensic investigators' hard work easier by creating tools with out-of-the-box solutions which do not require deep specialized knowledge to operate.

Along with the flagship *Belkasoft Forensic IM Analyzer*, we are also known for our *Belkasoft Forensic Studio*, *Belkasoft Forensic Carver*, *Belkasoft Browser Analyzer*, and some other software used in forensic investigations, law enforcement, intelligence, corporate security and parental control.

Contact information

Product support:

support@belkasoft.com

Business-related queries, investor relations, cooperation:

business@belkasoft.com

All other questions:

contact@belkasoft.com

If you are interested in our products, please contact us.

Customer problems solved

Computer forensic investigation

— Is there any evidence on a suspect's computer?

Out-of-the box solution for a number of evidence types

Parental control

— Is a child safe while surfing the web and chatting?

Corporate security

— Did a fired employee give away any business secrets?

— Are the current employees use their computers only for business needs?

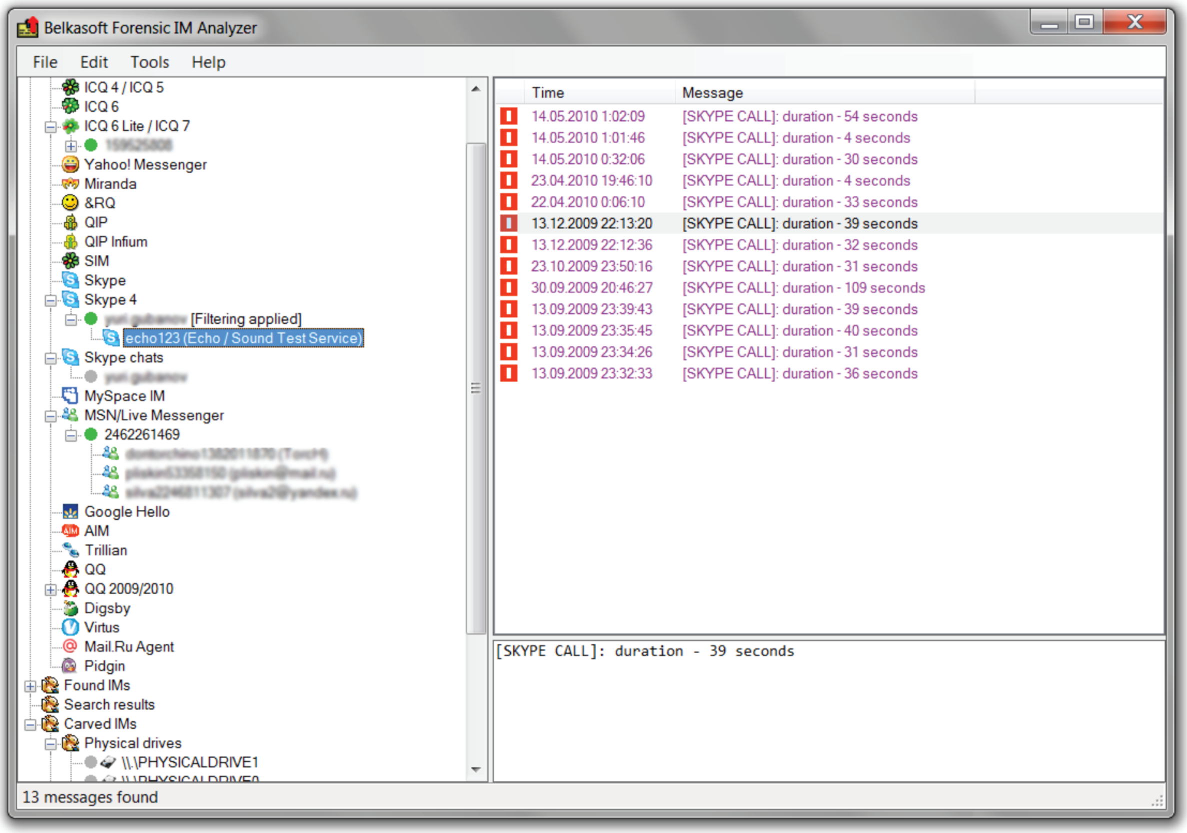
Intelligence

— Are there any suspicious chats made in an Internet café?

Forensic IM Analyzer

Belkasoft Forensic IM Analyzer is the most popular, patent-pending forensic product by Belkasoft. The product facilitates searching and analyzing numerous Instant Messenger histories.

- All popular Instant Messengers supported;
- No password required;
- Works with write-blocking devices;
- Allows for mounting Encase and DD drive images;
- Export to text, HTML, CSV and XML formats available;
- "Intelligence" edition available;
- Translated into German, Spanish and Chinese.



Time	Message
14.05.2010 1:02:09	[SKYPE CALL]: duration - 54 seconds
14.05.2010 1:01:46	[SKYPE CALL]: duration - 4 seconds
14.05.2010 0:32:06	[SKYPE CALL]: duration - 30 seconds
23.04.2010 19:46:10	[SKYPE CALL]: duration - 4 seconds
22.04.2010 0:06:10	[SKYPE CALL]: duration - 33 seconds
13.12.2009 22:13:20	[SKYPE CALL]: duration - 39 seconds
13.12.2009 22:12:36	[SKYPE CALL]: duration - 32 seconds
23.10.2009 23:50:16	[SKYPE CALL]: duration - 31 seconds
30.09.2009 20:46:27	[SKYPE CALL]: duration - 109 seconds
13.09.2009 23:39:43	[SKYPE CALL]: duration - 39 seconds
13.09.2009 23:35:45	[SKYPE CALL]: duration - 40 seconds
13.09.2009 23:34:26	[SKYPE CALL]: duration - 31 seconds
13.09.2009 23:32:33	[SKYPE CALL]: duration - 36 seconds

```
[SKYPE CALL]: duration - 39 seconds
```

13 messages found

Features

Search seized drive for histories

There is a seized hard drive in you lab, and you want to find all history files it may contain. You do not know which means of communication the suspect in question has been using. The product allows you to search the entire hard drive for all supported types of Instant Messengers:

- All drives or particular ones can be selected;
- Particular folders can be chosen for search;
- Histories to be looked for can be limited to particular types (e.g. Skype files only);
- Encase drives can be searched;
- Histories to analyze can be selected manually.

Analyze found histories

- The product does all the analysis with two mouse clicks;
- No password is required;
- Investigator does not have to be logged under a history owner;
- No write access is required; therefore, the product works with write-blocking devices.

Features

Explore extracted histories

The product shows extracted messages in a user-friendly form. The user interface enables you to:

- See all available histories and their extraction status;
- See all contacts belonging to a profile;
- See all conversations with a selected contact;
- Sort by time, message direction, message text;
- Apply filtering;
- Find histories by means of simple searches;
- Conduct advanced searches using a file with a selected set of words.

Experienced users can benefit from searching by regular expressions, which proves useful while searching for templates or phrases with fuzzy structure.

Export history

After completing your investigation, you need to export history of interest in a readable form. The product allows you to:

- Export found histories to plain text, HTML, XML, as well as to CSV format which makes it possible to work with data in powerful Microsoft Excel;
- Limit exported histories to selected dates and contacts;
- Limit exported histories to selected chat messages;
- Divide huge histories into separate files, broken by contact.

Features

Instant Messengers support

The following IMs are supported:

- ICQ (all versions from 97a to ICQ 7);
- Microsoft MSN / LiveMessenger;
- Skype versions 2, 3, 4;
- Skype chatsync recovery (Professional,Ultimate and Intelligence editions);
- Yahoo! Messenger;
- MySpace IM;
- &RQ;
- Miranda;
- SIM;
- QIP;
- QIP Infium;
- Google Hello;
- Trillian;
- QQ (2008 and earlier);
- QQ 2009/2010 (Professional, Ultimate and Intelligence editions);
- Digsby;
- Rambler Virtus;
- Mail.Ru Agent;
- Pidgin;
- AIM.

Features

Deleted history carving support (Ultimate edition):

- Skype;
- Digsby;
- ICQ Lite;
- ICQ 7;
- Miranda IM;
- Windows Live Messenger;
- QIP Infium/2010;
- SIM;
- AIM;
- Virtus;
- Pidgin;
- Trillian;
- Mail.ru Agent 5;
- Gajim;
- Emesene;
- Yahoo! Messenger.

Live memory images carving (Ultimate edition):

- ICQ 7;
- Yahoo! Messenger;
- Skype;
- Facebook (personal messages);
- Vkontakte.ru (personal messages);
- Gmail;
- MSN;
- Meebo;
- Google Talk.

Product editions

Home

This edition is intended for home (individual) users. Organizations are not allowed to purchase this edition. This is the most basic version of the product.

Standard

This edition is the basic version for organizational users.

Professional

This edition includes support for mounting drive images, extraction of Skype chatsync and QQ 2009/2010.

Ultimate

This edition includes support for carving (retrieving) data of deleted Instant Messengers and data in live RAM.

Intelligence

This edition is distributed as an executable file on a flash-drive which does not require installation on the target computer. This is useful for gathering information outside the forensic lab in uncontrolled environment like an Internet cafe. The edition is only available for the police and law enforcement organizations.

Intelligence edition

This edition matches the Ultimate edition of the tool in terms of functionality; however, it can be used without installation, e.g. in the field.
The benefit of this are:

- The software can be run from a flash drive (you do not have to install it on a target machine);
- You can use it even if you are not the administrator on a target machine;
- You do not have to install Microsoft.NET or other third-party products;
- You can use the software even if Microsoft.NET is not installed on a target computer;
- You can use the software for intelligence purposes (e.g. for investigations in an Internet café, etc);
- The information the software retrieves may be stored on the same flash drive.

The flip side of these advantages are the following disadvantages:

- The software is only available for the police or law enforcement bodies;
- If you run the software under a non-privileged user, some information may not be recovered depending on a computer security configuration.

  For example: you may not be allowed to search through Documents and Settings folder, belonging to other users of the computer; you may not be able to use the carving features, etc.

Forensic Studio

Belkasoft Forensic Studio is the most recent and powerful forensic product by Belkasoft. The product makes it easy for an investigator to search and analyze Instant Messenger histories, Internet Browser histories and various mailboxes.

Forensic Studio is a bundle of the following products:

- Belkasoft Forensic IM Analyzer (described above);
- Belkasoft Browser Analyzer;
- Belkasoft Mail Analyzer.

The products share the same user interface and functionality and thus are very easy to learn. You can read about such features as profiles search, history analysis and export above.

Browsers support

- Microsoft Internet Explorer (including IE version 8);
- Mozilla Firefox versions 2, 3;
- Opera;
- Google Chrome.

Mailboxes support

- Microsoft Outlook 2003, 2007;
- Microsoft Outlook Express;
- RITLabs The Bat! (beta version).

Product editions

Home

This edition is intended for home (individual) users. Organizations are not allowed to purchase this edition. This is the most basic version of the product.

Standard

This edition is the basic version for organizational users, it contains Standard versions of Belkasoft Forensic IM Analyzer and Belkasoft Browser Analyzer.

Professional

This edition contains Professional versions of Belkasoft Forensic IM Analyzer and Belkasoft Browser Analyzer. Professional edition of Forensic IM Analyzer is described above. What Professional edition of Browser Analyzer adds to the Standard edition is an ability to extract passwords entered by a user to view various sites.

Ultimate

This edition contains Ultimate versions of Belkasoft Forensic IM Analyzer and Belkasoft Browser Analyzer. Ultimate edition of Forensic IM Analyzer is described above. Ultimate edition of Browser Analyzer supports cache visualization and cached images export on top of other Professional edition features.

Mail Analyzer is the same in all Forensic Studio editions.

Dongle protection

Both products support usage with USB keys (so called "dongles"). When to choose the version with USB keys?

If you need more flexibility (e.g. you are going to use the software on different computers, you can choose version with USB keys.

For example: if you have 6 investigators and each investigator has 2 workstations and a laptop, instead of purchasing 18 regular licenses you can purchase 6 licenses with dongle support and save money. Please, remember that, unlike the regular version which is available to you almost immediately after the purchase, the version with a USB key may take one week to one month to arrive.

Training

Belkasoft can conduct online or onsite trainings per a customer request. We deliver 2 courses each focusing on one of the products described in this brochure — Forensic IM Analyzer and Forensic Studio. Both courses take 1 day. The number of attendees should not exceed 7 people at a time.

Online training is delivered via Skype.

Onsite training requires travel, accommodation and meal expenses to be covered by a customer.

Customer testimonials

— Nowadays, the evaluation of various messenger programs is immensely important for computer forensic examinations. Connections from the suspect can be better reconstructed and in some cases it can help to enlighten crimes. I am using Belkasoft Forensic IM Analyzer for this kind of tasks.

Dipl. Inform. Yesil, Hessen, Law Enforcement, Germany

— Your program will be a great asset to our forensic inventory.

Vern, Ontario Provincial Police, Electronic Crime Section

— It is a pleasure to work with your IM investigation product. Great tool for getting an overview of important conversations really fast!

Holger Morgenstern, independent forensic IT expert, Germany

Our customers

Among our customers are the Federal Bureau of Investigations (USA), The Department of Homeland Security (USA), Deloitte and Touche, Ernst & Young, PricewaterhouseCoopers, U.S. Secret Service and others.

See also: *http://www.belkasoft.com/home/en/Customers.asp*

STATENS KRIMINALTEKNISKA LABORATORIUM
SUSSEX POLICE
UNITED STATES SECRET SERVICE
WA POLICE
POLIS
AFP
AUSTRALIAN FEDERAL POLICE
Air Canada
BEREITSCHAFTSPOLIZEI THÜRINGEN
Bundeskartellamt
Bundeskriminalamt
ccl forensics
CCL-Forensics Limited
Ottawa
Deloitte.
U.S. DEPARTMENT OF HOMELAND SECURITY
EVIDENCE TALKS
ERNST & YOUNG
Quality In Everything We Do
DEPARTMENT OF JUSTICE FEDERAL BUREAU OF INVESTIGATION
Gendarmerie nationale
משטרת ישראל
PRICEWATERHOUSECOOPERS
中華人民共和國香港特別行政區政府
The Government of the Hong Kong Special Administrative Region of the People's Republic of China
POLITI
POLICJA