Belkasoft

forensics made easier

Belkasoft

This brochure features the Belkasoft Evidence Center software:

Belkasoft Evidence Center Standard

Belkasoft Evidence Center Enterprise

About

Forensics made easier

Belkasoft is an independent software vendor founded in 2002. We specialize in computer forensics and system software for the Windows platforms. With our slogan "Forensics made easier," we are trying to help IT security experts and forensic investigators by creating the tools with out-of-the-box solutions which do not require deep specific knowledge to operate.

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

Our solutions, chosen by the FBI, the US Secret Service, the police of Germany, Norway, Australia, New Zealand, etc, PricewaterhouseCoopers, Ernst & Young and others, greatly increase the efficiency of collecting digital evidence from a computer.

Belkasoft D-U-N-S number is 683524694.
Belkasoft NATO Commercial and Government Entity (NCAGE) code is SKF09.
Belkasoft is also registered within Central Contractor Registration (CCR).

Contact information

Product support:

support@belkasoft.com

Business-related queries, investor relations, cooperation:

business@belkasoft.com

All other questions:

contact@belkasoft.com

Customer problems solved

Computer forensic investigation

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

— How to find such evidence quickly without doing too many manual searches?

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

Corporate security

— Did a dismissed employee give away any business secrets?

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

Intelligence / Counterintelligence

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

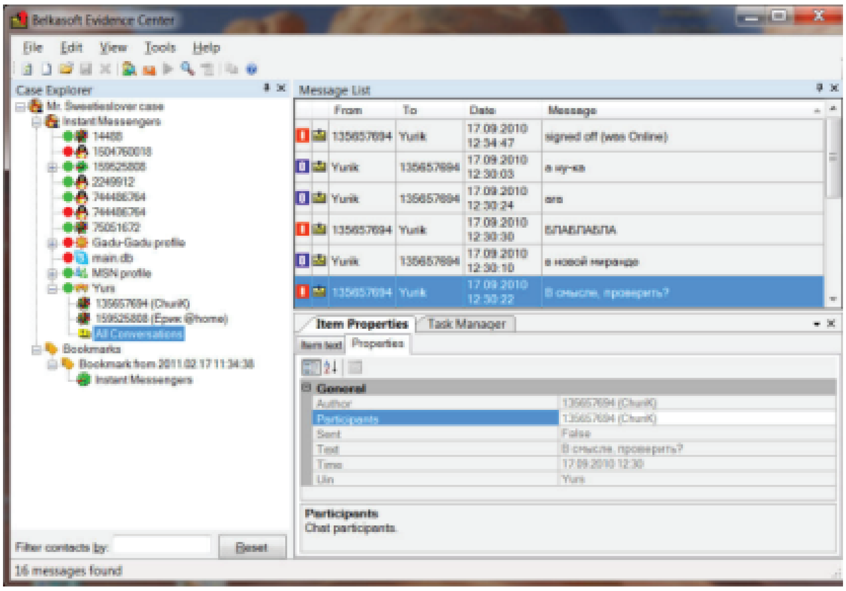
Parental control

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

Belkasoft Evidence Center

Belkasoft Evidence Center is the most recent, patent-pending computer forensics product by Belkasoft. This product makes it easy for an investigator to search, analyze and store digital evidence found in Instant Messenger histories, Internet Browser histories and Email client mailboxes, Social Network remnants, Picture and Video files.

- ☆ All major Messengers and Browsers supported;
- ☆ Outlook, Outlook Express, The Bat, Thundebird email clients supported;
- ☆ Pornography, faces and text detection in pictures and videos available;
- ☆ Stored evidence broken by cases;
- ☆ Hashes calculated for history files;
- ☆ Huge cases (e.g. containing several 10Gb mailboxes) supported;
- ☆ Multiple-monitor enabled;
- ☆ Highly customizable export to text, HTML, XML, CSV and PDF available;
- ☆ Multi-user feature is available;
- ☆ Memory and drive carving supported (Windows and MacOS);
- ☆ Network analysis module available.



From	To	Date	Message
135657694	Yurik	17.09.2010 12:34:47	signed off (was Online)
Yurik	135657694	17.09.2010 12:30:03	а ну-ка
Yurik	135657694	17.09.2010 12:30:24	ага
135657694	Yurik	17.09.2010 12:30:30	БЛАБЛАБЛА
Yurik	135657694	17.09.2010 12:30:10	в новой миранде
135657694	Yurik	17.09.2010 12:30:22	В смысле, проверить?

General

Author	135657694 (ChuriK)
Participants	135657694 (ChuriK)
Sent	False
Text	В смысле, проверить?
Time	17.09.2010 12:30
Uin	Yuri

Participants
Chat participants.

16 messages found

Features

Case management

The product allows you to manage information for different cases. You can add information you are working with to a named case, assign a name and a description to a case, create, edit and delete a case. This is handy when you work with multiple cases at a time.

Information persistence

All found information is now stored in a database. Unlike the older products, this product allows you to safely shut it down because all data is stored right after it is extracted. This enables you to work with multiple cases and handle big cases, for example, those involving multiple huge Outlook mailboxes. The product does not have a limit of 2Gb of Outlook mailbox space which the previous products have.

Integration

Unlike Belkasoft Forensic Studio which is a bundle of 3 products, Belkasoft Evidence Center integrates all the work with Instant Messengers, Browsers, Email, Pictures and Images in one user interface. You can perform all operations with a piece of evidence in a uniform way: It is possible, for example, to search through all found chats, URLs and emails in a single search operation.

Multiple monitor support

The product has a number of windows showing various aspects of a case you are working with. To make it more efficient to work with several windows, the product supports multiple monitors, so you can arrange windows and resize them as you find convenient.

Features

Search a seized drive or image for histories

There is a seized hard drive in you lab, and you want to find all history files the drive contains. You have no idea as to which means of communication the suspect has been using. The product allows you to search the entire hard drive for all supported types of histories: Instant Messenger chats, Browser URLs history, passwords and cookies, various mailboxes, pictures and videos:

- All drives or particular ones can be selected;
- Particular folders can be chosen to search through;
- Histories to be searched for can be limited to a particular type (e.g. Skype files only) ;
- Encase, DD and SMART drive images can be searched;
- Histories to analyze can be selected manually;
- Sophisticated techniques like drive and live RAM carving are supported.

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

Network traffic analysis

The product supports the analysis of PCAP files created by various network traffic interceptors (so called sniffers). Such files can be located by the tool and analyzed for Instant Messenger chats. Most popular protocols, such as Oscar (ICQ, AIM, etc.) and XMPP (Jabber, Facebook, etc), are supported.

Bookmarking

You can mark any extracted information by using named bookmarks. Bookmarks are persistent and stored in the same database as the case is. You can see all pieces of information in a bookmark, go to the original item and, vice versa, from an item to any bookmark which contains that item. Bookmarked items are highlighted with another color, so you will not miss them in an item list.

Picture and video support

The product allows you to search, add and explore pictures and videos. You can inspect EXIF properties and filter pictures by them. For pictures with GPS EXIF properties you can view the places they were taken at, on Google Maps or Google Earth. The product makes it possible to split videos on a series of key frames, thus decreasing time required for video analysis.

Picture analysis

With Evidence Center you can do the following analysis on images (including video key frames): pornography detection, faces detection and text detection. When the product completes analysis task, detected pictures are grouped according to the results for ease of reviewing, e.g. “Images with faces”.

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 or mails in a selected folder;
- Sort by time, message direction, message text;
- Apply filtering;
- Find histories by means of simple searches;
- Conduct advanced searches using a reference 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, PDF as well as to CSV, which makes it possible to work with data in powerful Microsoft Excel;
- Limit exported histories to selected dates;
- Limit exported histories to selected items;
- Divide huge histories into separate files, broken by contact or mail folder;
- Split reports into smaller files by specifying a number of items to be included in the report, for example, 50 messages per report file.

Features

Supported Instant Messengers

Some of supported IMs (not all) are listed below:

- ICQ (all versions from 97a to ICQ 7);
- Microsoft MSN / LiveMessenger;
- Skype versions 2, 3, 4, 5;
- Skype chatsync recovery;
- Yahoo! Messenger;
- MySpace IM;
- &RQ;
- Miranda;
- SIM;
- QIP;
- QIP Infium;
- Google Hello;
- Trillian;
- QQ 2008;
- Digsby;
- Rambler Virtus;
- Mail.Ru Agent;
- Pidgin;
- AIM;
- Gadu-Gadu;
- Qutim and some others

See http://belkasoft.com/bec/en/Instant_Messenger_Support.asp for a complete list.

Features

Deleted history carving support:

- Skype 3, 4, 5;
- Yahoo! Messenger;
- ICQ Lite;
- ICQ 7;
- Miranda IM;
- Windows Live Messenger;
- QIP Infium/2010;
- SIM;
- AIM;
- Virtus;
- Pidgin;
- Trillian;
- Mail.ru Agent 5;
- Gajim;
- Emesene;
- Digsby.

Live memory images carving:

- ICQ 7;
- Yahoo! Messenger;
- Skype;
- Facebook;
- Vkontakte.ru;
- Gmail;
- MSN;
- Meebo;
- Google Talk;
- Paltalk.

The lists are not complete; for complete information refer to
http://belkasoft.net/en/bec/en/Instant_Messenger_Support.asp

Features

Supported Browsers

All major browsers are supported:

- Microsoft Internet Explorer
- Mozilla Firefox
- Opera
- Apple Safari
- Google Chrome

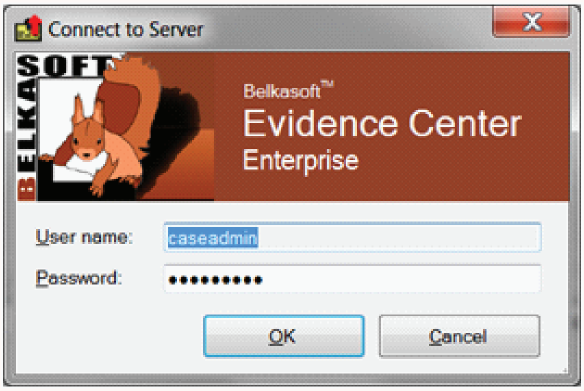
Supported Email Clients

The following email clients are supported:

- Microsoft Outlook (2003, 2007, 2010)
- Microsoft Outlook Express
- Mozilla Thunderbird
- RITLabs The Bat!

Enterprise edition

There is a client-server edition of the product, called "Enterprise", which allows for simultaneous work of several users on the same cases. It stores all case information in a central database available in the local network of your lab.



User name: caseadmin

Password: ••••••••••

Ideal for teamwork

The Enterprise edition is an ideal solution for a big or medium-sized security or forensic department where multiple security specialists or investigators may work on the same or difference cases. The product supports managing users and roles, and assigning rights to them, thus making it possible to grant users or groups of users access to some cases and deny them access to others.

Choose only the features you need!

The basic version of the product includes support for the following:

- Managing cases;
- Searching history files;
- Analyzing Instant Messenger, Browser and Email history files;
- Search for picture and video files; exploring their properties;
- Exporting history;
- Bookmarking;
- Searching within extracted history.

On top of that, you can purchase additional features like these:

- Deleted information retrieval (so-called carving);
- Live RAM dump analysis;
- Mounting drive images in Encase, DD and SMART formats;
- Network traffic analysis for chat artifacts;
- Picture analysis for pornography, faces and text;
- Video analysis;
- Dongle protection (ability to run the software on multiple machines).

The product configuration is remarkably flexible. You can request only those features you need and not pay for those you do not need.

Dongle protection

The product supports usage with USB keys (so called "dongles").
When to choose 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 and onsite trainings if a customer requires it. We offer an eight-hour course to Belkasoft Evidence Center users. The number of attendees should not exceed 7 people at a time.

Online training is delivered via GoToMeeting (analogue of WebEx).

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

Customer testimonials

— It works like a charm! The software is more than straightforward!

Andreas D., a forensic professional, who has helped Belkasoft with the Beta testing of the product, Germany**.**

— Your product is very versatile and is a good additional tool. Other tools are not that good in making a "readable" report for the court!.

Wolfgang L., a forensic investigator from the German police.

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

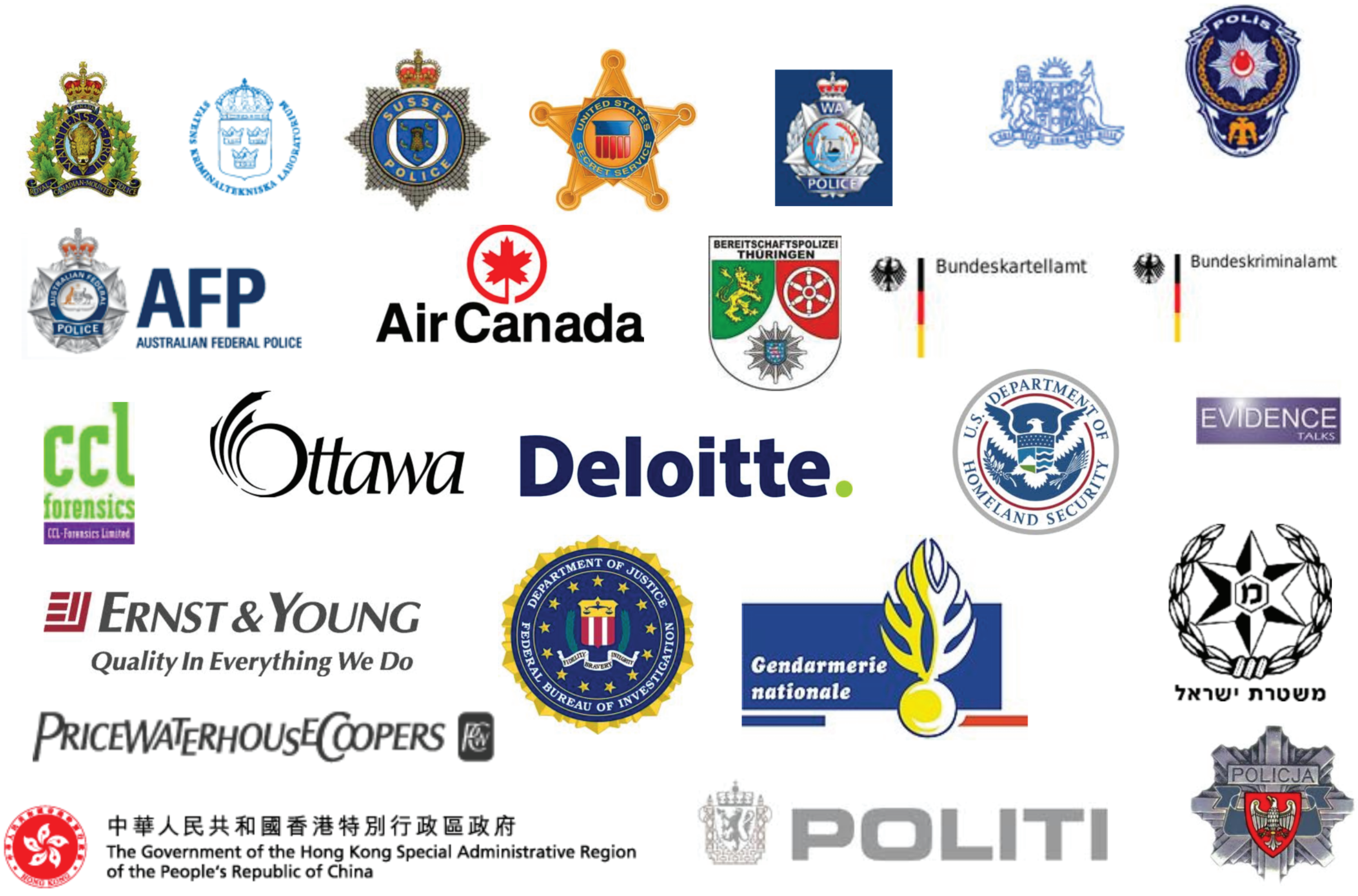
Holger Morgenstern, independent forensic IT expert, Germany.

Our customers

Belkasoft is proud to mention some of our customers.

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

Why Evidence Center?

- Reduced investigation cost;
- Reduced investigation time;
- Less specific knowledge required for investigators;
- Ideal for triage;
- Simultaneous work of several analysts on the same case.

Download now from http://belkasoft.com!