

## Two Forensic Cases Solved with Belkasoft Evidence Center

Belkasoft is proud to report that two more forensic cases have been solved with the help of its flagship forensic product, Belkasoft Evidence Center. With two more success stories, published with the permission of all participants, Belkasoft continues to help law enforcement and forensic agencies solve criminal cases and investigate illegal activities.

### *Case 1: Unauthorized Money Transfers*

Group-IB, a leading commercial investigator in Russia, was approached by a major bank. The bank's managers detected unauthorized money transfer activities going on in their system. The activities were the result of someone hijacking the bank's money transfer system. A hard drive image and firewall logs were analyzed in the lab, revealing the computer in question was accessed remotely. In order to discover additional evidence, the lab investigated Web browser logs and user profiles; no suspicious activity was discovered.



At this point, the analysts used Belkasoft Evidence Center, which quickly revealed that the criminals exploited the SYSTEM user profile. The catalog structure of the profile folder was highly untypical for a system profile, being a clear indicator of some sort of malicious activity. From then on, investigators used Belkasoft Evidence Center to retrieve Internet Explorer logs, revealing exact Web addresses used by the criminals, including the exact location on an ftp-server containing malicious code used to access the computer remotely.

The success story ended with the lab being able to reconstruct the chronology of the crime and find out the criminal's IP addresses. Without the help of Belkasoft Evidence Center, investigators could easily miss the fake system profile as such techniques are rarely employed by the criminals.

### *Case 2: Analyzing Seized Laptops under Time Constraint*

In this case, Group-IB was approached by the police to help analyze a number of seized laptops. The police was looking for email and chat communications stored on laptops' hard drives. As none of the other tools used by the police helped retrieve the data in question, Group-IB used the so-called 'carving' feature of Belkasoft Evidence Center to gain full access to current and deleted messages stored in Outlook email databases and instant messenger logs.

A number of deleted Skype and QIP 2010 messages were restored, with IM user profiles discovered in non-standard locations. As a result, all message histories were successfully retrieved and saved in a readable format, producing over 6,000 pages message logs that were made available to the police in easily readable plain-text format.

## *About Belkasoft Evidence Center*

At version 3.0, the company's flagship computer forensic tool helps security and forensic specialists collect and analyze more digital evidence from PC and Mac computers than ever. Belkasoft Evidence Center will automatically locate, process and analyze Internet chat logs, Web browsing history and email communications including all stored passwords, cached forms, information stored in cookies and digital pictures, mailboxes and system files. Low-level access to hard disk and system structures means that even data that's been deleted by a suspect cannot escape from investigators.

The affordable Standard edition is available to private investigators and corporate security departments, while the more comprehensive Enterprise edition allows major security agencies and police departments to have multiple investigators work simultaneously on a case.

## *Pricing and Availability*

Belkasoft Evidence Center 3.0 is available immediately. Pricing for Standard edition starts from \$999.95, while the Enterprise edition is available for \$9999.95.

## *About Belkasoft*

Founded in 2002, Belkasoft is a software vendor specializing in computer forensics and IT security software. Running on the Microsoft Windows platform, Belkasoft products back the company's "Forensics made easier" slogan, offering IT security experts and forensic investigators solutions that work right out of the box, without requiring a steep learning curve or any specific skills to operate.

Along with the flagship Belkasoft Evidence Center, Belkasoft is also marketing Forensic IM Analyzer, Forensic Studio, Forensic Carver, Browser Analyzer and other products used in forensic investigations, law enforcement, intelligence, corporate security and parental control applications.

Belkasoft solutions are used by government and commercial customers worldwide. The company's clients include the FBI, U.S. Army, US Secret Service, multiple police departments in Germany, Norway, Australia, New Zealand and many other countries, PricewaterhouseCoopers, Ernst & Young and other Fortune 100 corporations.

More information about the company and its products is available at <http://belkasoft.com>.

*###*

Belkasoft made the demo version available for free download at [http://belkasoft.com/bec/en/Evidence\\_Center.asp](http://belkasoft.com/bec/en/Evidence_Center.asp)