Belkasoft Evidence Center 5.4 Detects Forged Images, Analyzes Fragmented Memory Dumps and Extracts Destroyed SQLite Records

Belkasoft announces a major update to its flagship forensic product, Belkasoft Evidence Center 2013. Version 5.4 introduces forged image detection, aggregated view of all user activities, native SQLite parsing with freelist analysis, the ability to analyze fragmented memory sets as well as support for forensic artifacts available in Windows Registry.

St. Petersburg, Russia (PRWEB) August 08, 2013 -- Belkasoft announces a major update to its flagship forensic product, Belkasoft Evidence Center 2013. Version 5.4 introduces forged image detection, aggregated view of all user activities, native SQLite parsing with freelist analysis, the ability to analyze fragmented memory sets as well as support for forensic artifacts available in Windows Registry.

Customers having a non-expired Extended Software Maintenance and Support contract are eligible for a free update to version 5.4. Customers without such a contract are welcome to purchase it from their Personal Cabinet.

Belkasoft Evidence Center 5.4

The newly added Forgery Detection plugin enables automatic detection of digital photos that have been altered. The ability to process fragmented memory dumps enhances Live RAM analysis, reassembling scattered memory blocks together to produce solid evidence. The Timeline view displays all discovered events in a single list, allowing investigators to quickly glance over recent events or scrutinize a certain time period. Windows Registry support automatically locates and parses registry hives, extracting many types of valuable evidence. Native SQLite support with freelist analysis enables the recovery of destroyed database records, allowing investigators to recover cleared Skype histories.

Office 2007-2013 carving support and built-in check for updates are two more features to mention.

Forgery Detection

A new Forgery Detection plugin is available in the Ultimate edition of Belkasoft Evidence Center 5.4. This plugin allows investigators automatically detecting digital pictures that have been altered, modified or edited after leaving the camera. The plugin enables law enforcement authorities tell whether submitted pieces of evidence are original or are faked. Over 1,000 camera models are supported.

Improved Live RAM Analysis

The ability to recover evidence from memory dumps with Live RAM analysis is greatly improved in the new version thanks to the ability to defragment memory sets. In real life, Windows rarely stores volatile data in contiguous fashion. Instead, reasonably large images and other types of data are split into chunks that are scattered along the entire memory content. Traditional RAM analysis algorithms have little success analyzing fragmented memory sets. The new BelkaCarving algorithm is based on a scientific research enabling Evidence Center to carefully reconstruct fragmented chunks into contiguous pieces of information, allowing the tool to extract broken pieces such as recently viewed images that no other tool can access. At this time, support is based on memory dumps captured on 32-bit and 64-bit Windows 7 systems. Support for other operating
systems is being actively developed.

Aggregated Timeline View of User Activities

Evidence Center 5.4 introduces a new Timeline view, displaying all detected user activities and system events in a single aggregated list. By using the Timeline, investigators can quickly glance at user activities over a certain time period or scrutinize a particular period of time with ease.

Recovering Destroyed Evidence with Native SQLite Parsing

Version 5.4 implements fully native parsing of SQLite databases, allowing investigators recover database records from badly damaged, fragmented and incomplete databases such as those resulting from a carving attempt.

The newly implemented freelist analysis feature allows analysts extract records that were deleted by the user. This, in particular, allows recovering cleared Skype histories.

In addition, a built-in SQLite viewer is now available.

Windows Registry Support

The newly added support for Windows Registry artifacts automatically locates and parses registry hives, extracting many types of valuable evidence such as MRU of various applications (e.g. MS Office, Acrobat Reader etc.), UserAssists, program startup data, list of connected USB devices, network cards, wireless profiles and many other types of artifacts. This feature is available in Professional and Ultimate editions.

About Belkasoft Evidence Center 2013

Belkasoft Evidence Center is the company’s flagship computer forensic tool enabling security experts and forensic specialists collect and analyze more digital evidence than ever. Belkasoft Evidence Center can automatically locate, process and analyze Internet chat logs, Web browsing history and email communications including information stored in digital pictures and videos, a variety of history and log files. Low-level access to hard disk and system structures means that even data that’s been deleted by the suspect cannot escape from investigators. Supporting Windows, Unix/Linux and Mac OS X file systems and natively mounting images created in EnCase, DD and SMART formats without using these or any third-party tools, Belkasoft Evidence Center can collect more evidence than any single competing tool in its class.

Pricing and Availability

Belkasoft Evidence Center 2013 is available immediately. Pricing for Forensic IM Analyzer edition starts from $499.95, the Professional edition is available from $799.95, while the Ultimate edition sells for $1099.95.

Forgery Detection Plugin is available to users of Forensic Studio Ultimate for $999.95.

About Belkasoft

Founded in 2002, Belkasoft is a computer forensic software vendor. 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.

Belkasoft Evidence Center 2013 is a world renowned tool used by thousands of customers for conducting forensic investigations, as well as for law enforcement, intelligence and corporate security applications. Belkasoft customers include government and private organizations in more than 40 countries, including the FBI, US Army, DHS, police departments in Germany, Norway, Australia and New Zealand, PricewaterhouseCoopers, and Ernst & Young.

More information about the company and its products at http://belkasoft.com

###

Information on Belkasoft Evidence Center as well as the free demo download are available at http://forensic.belkasoft.com/

The complete list of additions and enhancements in version 5.4 is available at http://forensic.belkasoft.com/en/bec/en/Whats_New_In_Version_5.4
Contact Information
Yuri Gubanov
Belkasoft
http://belkasoft.com
+7(812) 9211201

Online Web 2.0 Version
You can read the online version of this press release [here](#).