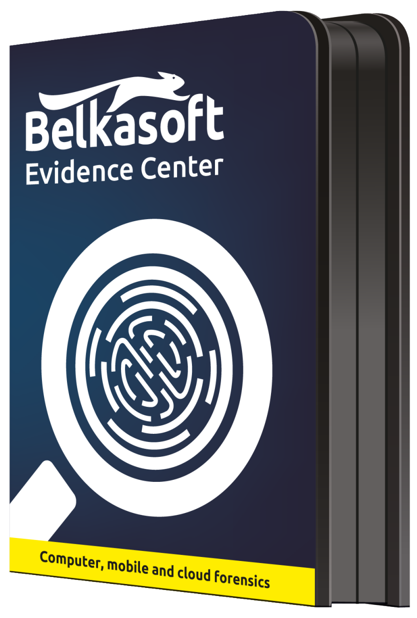
Belkasoft
forensics made easier

3724 Heron Way, Palo Alto, CA 94303, USA
+1 (650) 272-03-84 (USA and Canada)
+7 (812) 926-64-74 (Europe and other regions)

BELKASOFT EVIDENCE CENTER

All-in-one forensic solution for locating, extracting, and analyzing digital evidence stored inside computers and mobile devices and mobile devices, RAM and cloud.

Belkasoft Evidence Center is designed with forensic experts and investigators in mind: it automatically performs multiple tasks without requiring your presence, allowing you to speed up the investigation; at the same time, the product has convenient interface, making it a powerful, yet easy-to-use tool for data extraction, search, and analysis.



INCLUDES

- Fully automated extraction and analysis of 1000+ types of evidence
- Destroyed and hidden evidence recovery via data carving
- Live RAM analysis
- Advanced low-level expertise
- Concise and adjustable reports, accepted by courts
- Case Management and a possibility to create a portable case to share with a colleague at no cost

TYPES OF EVIDENCE SUPPORTED BY EVIDENCE CENTER

- Office documents
- Email clients
- Pictures and videos
- Mobile application data
- Web browser histories, cookies, cache, passwords, etc.
- Chats and instant messenger histories
- Social networks and cloud services
- Encrypted files and volumes
- System files, including Windows 10 timeline and TOAST, macOS plists, smartphone Wi-Fi and Bluetooth configurations etc.
- Cryptocurrencies
- Registry files
- SQLite databases
- Peer-to-peer software
- Plist files

TYPES OF ANALYSIS PERFORMED BY EVIDENCE CENTER

- Existing files search and analysis. Low-level investigation using Hex Viewer
- Timeline analysis - ability to display and filter all user activities and system events in a single aggregated view
- Full-text search through all types of collected evidence. Automatic indexing of various important text templates such as emails, phone numbers, MAC and IP addresses etc
- Data carving and destroyed evidence recovery. Custom carving, including support for Scalpel and FTK sets
- Live RAM analysis including process extraction and data visualization. Malware detection
- Hibernation file (hiberfil.sys) and page file (pagefile.sys) analysis
- Native SQLite analysis with freelist and WAL support
- Discovers deleted SQLite records, e.g. Skype conversations or WhatsApp messages
- Picture analysis including EXIF and GPS analysis, face/test/skin tone/forgery detection, pornography detection using neural networks
- Video key frame extraction
- Analysis of links between persons using Connection Graph features such as communication visualization and communities detection
- Encryption detection and decryption of found encrypted files
- Special files and folders analysis (e.g. Volume Shadow Copy, $OrphanFiles, $MFT etc.)
- Hashset analysis
- Flexible analysis with BelkaScript, scripting module
- Deduplication by using PhotoDNA hashing as well as not carving existing files

EVIDENCE CENTER WORKS WITH THE FOLLOWING DATA SOURCES AND FILE SYSTEMS

- Storage devices - Hard drives and removable media
- Disk images - EnCase (including Ex01), L01/Lx01, FTK, DD, Smart, X-Ways, Atola, DMG, tar and zip files
- Mobile devices - Mobile backups, UFED and OFB dumps, chip-off and JTAG dumps
- Virtual machines - VMWare, Virtual PC, VirtualBox, XenServer
- Volatile memory - Life RAM dumps; fragmented memory set analysis with BelkaCarving™
- Memory files - Hibernation and page files
- Unallocated space - Data carving discovers destroyed evidence

File systems – APFS, FAT, exFAT, NTFS, HFS, HFS+, ext2, ext3, ext4, YAFFS, YAFFS2

EVIDENCE CENTER SUPPORTS THE FOLLOWING ACQUISITION TYPES

- **Mobile devices:** iTunes backup (iOS), ADB backup or agent-based backup (Android), physical backup or EDL (rooted Android)
- **Hard drives:** logical and physical drives, available to DD or E01 images with optional hash calculation and verification
- **Clouds:** Google Clouds (Google Drive, Google Plus, Google Keep, GMail, Google Timeline), iCloud, EMail (Yahoo, Hotmail, Opera, Yandex, Mac.com and 25 more webmail clouds), Instagram, WhatsApp

EVIDENCE CENTER HELPS INVESTIGATE THE FOLLOWING SYSTEMS

- Windows (all versions, including Windows 10)
- macOS
- Unix-based systems (Linux, FreeBSD, etc.)
- iOS: iPhone, iPad
- Android
- Windows Phone 8/8.1
- Blackberry