TRUSTED BY THE POLICE

AROUND THE GLOBE

Used by thousands of forensic experts and police departments worldwide from more than 130 countries

Designed by jcomp / Freepik

Belkasoft
forensics made easier

Try free at https://belkasoft.com/trial
30 days trial

BELKASOFT EVIDENCE CENTER

Forensics Made Easier

Evidence Center features

- Local and remote acquisition of hard drives, mobile devices, cloud data, RAM
- Fully automated extraction and analysis of 1000+ types of evidence
- Destroyed and hidden evidence recovery via data carving
- Live RAM analysis
- Automatic indexing of various important text templates such as emails, phone and SSN numbers, MAC and IP addresses etc.
- Fully customizable reports in a dozen of different formats
- Multi-user Team Edition module

Types of evidence supported by Evidence Center

- Office documents
- Emails
- Pictures & Videos
- Mobile application data for hundreds of modern apps, such as WhatsApp, Telegram X, SnapChat etc.
- Web browser histories, cookies, cache, passwords etc.
- Social network communications
- System files including jumplists, thumbnails, Windows 10 Timeline and event logs
- Encrypted files and volumes (Bitlocker, FileVault, McAfee and 300 more)
- Registry files
- SQLite databases
- Plist files
- Cryptocurrencies
- Geolocation data

Types of analysis performed by Evidence Center

- Existing files search and analysis. Low-level investigation using Hex Viewer
- Data carving and deleted information recovery
- Live RAM analysis including process extraction and data visualization
- Hibernation file and page file analysis
- Native SQLite analysis with freelist, journals and WAL support, SQLite unallocated analysis
- Picture analysis including neural network-based recognition of porn/guns/drug-related signs
- Malware detection
- Video key frame extraction
- Special files and folders analysis (e.g. Volume Shadow Copy, $OrphanFiles, $MFT etc.)
- Communication visualization and communities detection in Connection Graph
- Incident Investigations (Amcache, ShimCache, Syscache, BAM/DAM, AppInit DLLs, Change of default file association, scheduled tasks, remote connections (RDP, TeamViewer), startup tasks, browser extensions)

Evidence Center works with the following data sources and file systems

• Storage devices	Hard drives and removable media
• Disk images	E01/Ex01, L01/Lx01, FTK, AD1, DD, SMART, X-Ways, DMG, Atola
• Mobile devices	Mobile backups, TWRP images, UFED and OFB dumps, GrayKey and Elcomsoft iOS images, JTAG and chip-off dumps
• Virtual machines	VMWare, Virtual PC, XenServer, Virtual Box
• Volatile memory	Live RAM dumps
• Memory files	Fragmented memory set analysis with BelkaCarving™ Hibernation files and Page files
• Unallocated space	Data carving discovers destroyed evidence Ability to carve solely in a non-occupied space to save time
• File systems	APFS, FAT, exFAT, NTFS, HFS, HFS+, ext2, ext3, ext4, YAFFS, YAFFS2

Evidence Center helps investigate the following systems

- Windows (including Windows 10 and Windows Phone 8.1)
- macOS X
- Unix-based systems (Linux, FreeBSD etc.)
- iOS: iPhone, iPad
- Android
- BlackBerry

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)