

Evidence Center

Evidence Center makes it easy for an investigator to acquire, search, analyze, store and share digital evidence found inside computer and mobile devices.

Features

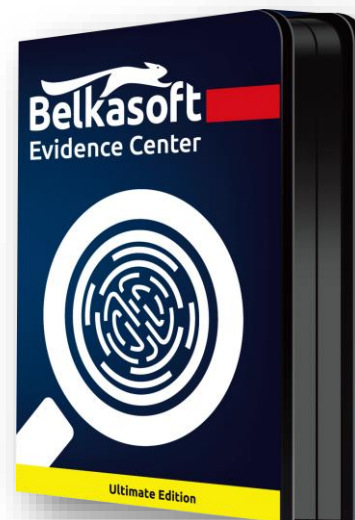
- Fully automated extraction and analysis of 700+ types of evidence
- Destroyed and hidden evidence recovery via data carving
- Live RAM analysis

Types of evidence supported

- Office documents
- Emails
- Pictures
- Videos
- Mobile application data for hundreds of modern apps
- Web browser histories, cookies, cache passwords etc.
- Chats and instant messenger histories
- Social network communications
- System files including jump lists, thumbnails and event logs
- Encrypted files
- Registry files
- SQLite databases
- Plist files

Types of Analysis

- 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 free list, journals and WAL support, SQLite unallocated analysis;
- Discovers deleted SQLite records, e.g. Skype conversations or WhatsApp messages
- Picture analysis including EXIF and GPS analysis, face/text/skin/forgery detection
- Video key frame extraction
- Encryption detection for 220+ types of files
- Special files and folders analysis (e.g. Volume Shadow Copy, Orphan Files, MFT etc.)



Data Sources and File Systems

- **Storage devices** - Hard drives and removable media
- **Disk images** - E01/Ex01, L01/Lx01, FTK, DD, SMART, X-Ways, DMG, Atola
- **Mobile devices** - Mobile backups, UFED dumps, JTAG and chip-off dumps
- **Virtual machines** - VMWare, Virtual PC, XenServer, Virtual Box
- **Volatile memory** - Live RAM dumps
 - Fragmented memory set analysis with BelkaCarving™
- **Memory Files** - Hibernation files and Page files
- **Unallocated space** - Data carving discovers destroyed evidence
 - Free Space: possible to carve non-occupied space only to save time
- **File system** - FAT, exFAT, NTFS, HFS, HFS+, ext2/3/4, YAFFS, YAFFS2

Systems Supported

- Windows (including Windows 10 and Windows Phone 8.1)
- Mac OS X
- Unix-based systems (Linux, Free BDS etc.)
- iOS: iPhone, iPad
- Android
- BlackBerry