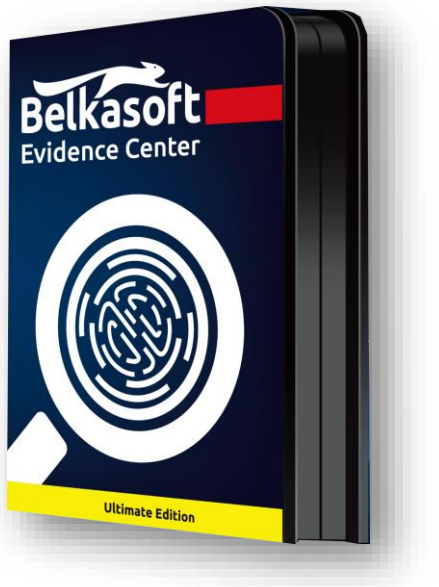
科技创造可能

Evidence Center

Evidence Center 令罪案调查员轻松获取、搜索、分析、存储及分享取自电脑和手机中的电子证据



产品特点

- 全自动提取及分析超过 700 种类型的电子证据
- 通过数据挖掘（Data Carving）恢复损坏及隐藏的证据
- 即时 RAM 分析

支持证据类型

- Office 文件、电子邮件、图片、视频
- 数百个当前手机应用程序数据
- 浏览器历史记录、cookies、cache、密码等
- 对话记录与即时通讯记录
- 社交网络通讯记录
- 系统文件，包括跳转列表（jump lists）、缩略图及系统日志
- 加密文件
- 注册表文件
- SQLite 数据库
- Plist 文件

数据分析类型

- 现存文件搜索与分析；通过 Hex 检视器进行初级调查
- 数据挖掘（Data Carving）及恢复删除数据
- RAM 即时分析，包括过程提取及数据可视化
- 休眠文件及页面文件
- 通过空闲列表（free lists）、日志和 WAL 进行本地 SQLite 分析；支持分析未分配的 SQLite；寻回已删除的 SQLite 记录，例如 Skype 对话或 Whatsapp 即时通讯。
- 包括 EXIF 和 GPS 在内的图片分析，以及面部、文字、皮肤、伪造品侦测
- 提取视频关键帧
- 针对 220 余种文件的加密侦测
- 特殊文件及文件夹分析，例如磁盘区阴影绘制（Volume Shadow Copy）、孤儿档案（Orphan Files）、MFT 等

深圳市顺安特科技有限公司
中国广东省深圳市罗湖区人民南路 2008 号嘉里中心 13 楼 1308 室　　邮编 518001
网址: www.dataexpert.com.hk　　电子邮箱: info@dataexpert.com.hk　　服务热线: +86 755 22905810

数据来源及文件系统

- **储存设备**：硬盘及可移动储存设备
- **磁盘镜像**：E01/Ex01, L01/Lx01, FTK, DD, SMART, X-Ways, DMG, Atola
- **移动设备**：手机备份, UFED dumps, JTAG 和 chip-off dumps
- **虚拟计算机**：VMWare, Virtual PC, XenServer, Virtual Box
- **易失性存储器**：即时 RAM dumps
  通过 BelkaCarving™ 进行记忆体片段分析
- **内存文件**：休眠文件及页面文件
- **未分配空间**：数据挖掘（Data Carving）获取损毁证据
  剩余空间：为节约时间，可挖掘未占用空间
- **文件系统**：FAT, exFAT, NTFS, HFS, HFS+, ext2/3/4, YAFFS, YAFFS2

操作系统

- Windows (包括 Windows 10 和 Windows Phone 8.1)
- Mac OS X
- 基于 Unix 的系统 (Linux, FreeBDS 等)
- iOS: iPhone, iPad
- 安卓
- 黑莓