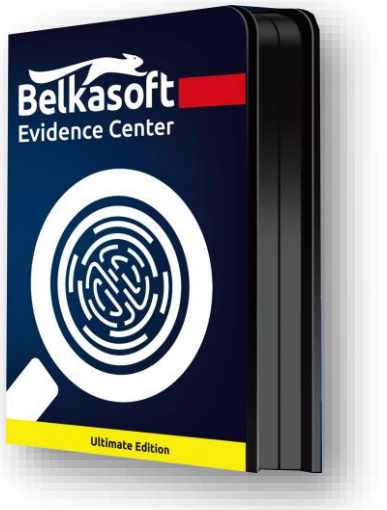
科技創造可能

Evidence Center

Evidence Center 令罪案調查員輕鬆獲取、搜索、分析、存儲及分享取自電腦和手機中的電子證據.



產品特點

- 全自動提取及分析超過 700 種類型的電子證據
- 通過資料挖掘（Data Carving）恢復損壞及隱藏的證據
- 即時 RAM 分析

支持證據類型

- Office 檔案、電子郵件、圖片、視頻
- 數百個當前手機應用程式數據
- 流覽器歷史記錄、cookies、cache、密碼等
- 對話記錄與即時通訊記錄
- 社交網路通訊記錄
- 系統檔案，包括跳轉列表（jump lists）、縮略圖及系統日誌
- 加密檔案
- 註冊表檔案
- SQLite 資料庫
- Plist 文件

資料分析類型

- 現存檔案搜索與分析；通過 Hex 檢視器進行初級調查
- 數據挖掘（Data Carving）及恢復刪除資料
- RAM 即時分析，包括過程提取及資料視覺化
- 休眠檔案及頁面檔案
- 通過空閒列表（free lists）、日誌和 WAL 進行本地 SQLite 分析；支持分析未分配的 SQLite；尋回已刪除的 SQLite 記錄，例如 Skype 對話或 WhatsApp 即時通訊。
- 包括 EXIF 和 GPS 在內的圖片分析，以及面部、文字、皮膚、偽造品偵測
- 提取視頻關鍵幀
- 針對 220 餘種文件的加密偵測
- 特殊檔及資料夾分析，例如磁片區陰影繪製（Volume Shadow Copy）、孤兒檔案（Orphan Files）、MFT 等

順安達科技有限公司
香港新界葵涌貨櫃碼頭路 88 號永得利廣場一期 8 樓 803 & 805 室
網址: www.dataexpert.com.hk 電子郵箱: info@dataexpert.com.hk 服務熱線: +852 3590 2115

資料來源及檔案系統

- 儲存設備：硬碟及可移動儲存設備
- 磁片鏡像：E01/Ex01, L01/Lx01, FTK, DD, SMART, X-Ways, DMG, Atola
- 移動設備：手機備份, UFED dumps, JTAG 和 chip-off dumps
- 虛擬計算機：VMWare, Virtual PC, XenServer, Virtual Box
- 易失性存儲器：即時 RAM dumps
  通過 BelkaCarving™ 進行記憶體片段分析
- 記憶體檔案：休眠文件及分頁檔
- 未配置空間：數據挖掘（Data Carving）獲取損毀證據
- 剩餘空間：為節約時間，可挖掘未佔用空間
- 檔案系統：FAT, exFAT, NTFS, HFS, HFS+, ext2/3/4, YAFFS, YAFFS2

操作系統

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