



# SOLVE

# INVESTIGATIONS

AUTOMATED SOFTWARE FOR FIELD OR LAB

## Digital Evidence Investigator®

Digital Evidence Investigator® (DEI) enables investigators and lab examiners to leverage ADF's fully automated, forensically sound, intelligent and highly configurable artifact and file collection software.

### 10,000+ Global Users Rely on ADF to Speed Investigations

+ RAPID CAPTURE

+ INTELLIGENT ANALYSIS

+ SHARED REPORTING

## COLLECT

Prioritize speed in evidence collection and use in the field or in the lab investigations with minimal training.

- Highly configurable artifact and file collection including web browser cached files, social media, P2P, Cryptocurrency, cloud storage, user login events, anti-forensic traces, saved credentials, files shared via Skype, USB history, user connection log, etc.
- Supports collection of artifacts from Windows and macOS (including High Sierra and Mojave)
- Search and collect emails including MS Outlook, Windows Mail, Windows Live Mail 10, Apple Mail
- Investigate attached devices, live powered on computers, boot scans from powered off computers, forensic images, the contents of folders and network shares (including shares made available by NAS devices)



- Rapidly search suspect media using large hash sets (>100 million), including Project VIC and CAID
- Find relevant files and artifacts using DEI's powerful keyword and regular expression search capability
- Image drives Out-of-the-box with image verification and imaging log file
- Recover images from unallocated drive space
- Use password and recovery key to decrypt and scan or image BitLocker volumes including those using the new AES-XTS encryption algorithm introduced in Windows 10
- Process APFS partitions, NTFS, FAT, HFS+, EXT, ExFAT, and YAFFS2 file systems, compute MD5 and SHA1 on collected files for integrity validation
- Capture RAM and volatile memory
- Collect password protected and corrupted files for later review
- Collect iOS backups on target computers
- Detect and warn of BitLocker and FileVault2 protected drives
- Leverage DEI's powerful boot capability (including UEFI secure boot and Macs) to access internal storage that cannot easily be removed from computers

## ANALYZE

Use the single timeline view that combines files and artifact records with a user's actions.

- View results while a scan is running
- Filter search results with sorting and search capabilities (dates, hash values, tags, text filters, more)
- View pictures and videos organized by visual classes such as people, faces, currency, weapons, vehicles, indecent pictures of children
- View links between files of interest and user's activities such as recently access files, downloaded files, attachments, and more
- Inspect video using DEI's comprehensive video preview and frame extraction
- Automatically tag hash and keyword matches
- Define new file types and select individual ones to be processed
- Display provenance, including comprehensive metadata, of all relevant files and artifacts

## REPORT

Digital Evidence Investigator® lets you create a standalone portable viewer for further analysis and reporting for prosecutors and other investigators.

- Powerful reporting capabilities (HTML, PDF, CSV)
- Export in VICS format

