ADF

ADF4N6.COM

PROVE IT

CONTROLLED DEPLOYMENT TO PRIORITIZE ELECTRONIC EVIDENCE STARTING ON-SCENE

Triage-Investigator® PRO

Empower field investigators with the fastest on-scene digital evidence collection and analysis tool. Triage-Investigator automates investigations with pre-configured scans.

Control What Your Field Investigators Collect with DEI and Triage-Investigator

+ CUSTOM PROFILES **+ INTELLIGENT ANALYSIS** **+ CONTROLLED DEPLOYMENT**

- Leverages AI and Machine Learning to process and speed analysis of relevant data
- Easy-to-learn with built in digital forensic Search Profiles so you can quickly collect digital evidence based on the type of case you are working
- Rapid analysis lets you make decisions in the field or back in the lab
- Create comprehensive reports to share with other investigator or prosecutors for free
- Import Custom Search Profiles from Digital Evidence Investigator PRO

ADD-ON Options:

- Rosoka Entity Extraction and 230+ language gisting
- Learn at your own pace with training and ADF Certification (12 hours Online)

COLLECT: Rapid automated evidence collection

- Advanced logical acquisition of iOS/Android data up to 4GB per minute
- Live Preview Mode - View phone content immediately without waiting for a backup or imaging to finish
- Image live macOS computers via our remote agent and create an AFF4 logical image
- Capture and organize screenshots of connected mobile devices while navigating with automatic processing to extract and index text for search, annotation and reporting
- Recover call records, messages, saved contacts and calendar data
- Recover WiFi connections, installed applications and Android user accounts
- Recover pictures, videos, audio files, documents and user-defined file types
- Recover database files and Property Lists for later review
- Recover browsers, browsing history, download history, search terms, form data, bookmarks, more
- Capture Revolut mobile app data and organize it in a financial transactions table (iOS)
- Search for specific information using keywords, regular expressions, hash values and PhotoDNA
- Identify files or artifacts containing terms related to child exploitation
- iOS devices: Automatically encrypt backup to obtain more data
- Capture RAM and volatile memory
- Collect password protected and corrupted files for later review
- Collect iOS backups on target computers
- Recover deleted records from apps using the SQLite database
- Supports collection of artifacts from Windows and macOS (including T2 and M1 chips)
- Image drives out-of-the-box with image verification and imaging log file
- Recover images from unallocated drive space
- 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.
- Rapidly search suspect media using large hash sets (>100 million), including VICS 2.0 and CAID
- Find relevant files and artifacts using powerful keyword and regular expression search capability
- 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
- Investigate attached devices, live powered on computers, boot scans from powered off computers, forensic images, contents of folders and network shares (including NAS devices)
- Process APFS partitions, NTFS, FAT, HFS+, EXT, ExFAT, and YAFFS2 file systems, compute MD5 and SHA1 on collected files for integrity validation
- Leverage the powerful boot capability (including UEFI secure boot and Macs) to access internal storage that cannot easily be removed from computers

ANALYZE: Timeline view ties suspects to their actions

- View results while a scan is running, and filter search results with sorting and search capabilities (dates, hash values, tags, text filters
- View chat conversations with bubbles to easily identify senders / receivers with message threads
- 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 ADF's comprehensive video preview and frame extraction
- Automatically tag hash and keyword matches
- Leverage Suspect Technologies age detection to identify images of infants, toddlers, children, adults
- Define new file types and select individual ones to be processed
- Display provenance, including comprehensive metadata, of all relevant files and artifacts
- Reorder or disable post-scan tasks (classification of pictures, videos, or entity extraction)

REPORT: Report on-scene and share with prosecutors

- Create a standalone portable viewer for further analysis and reporting to share with prosecutors and other investigators
- Powerful reporting capabilities (HTML, PDF, CSV)
- Scan GrayKey images and present a comprehensive list of files and artifacts
- Export to the Orchesight platform
- Export to Truxton
- Export in VICS format (to Griffeye Analyze Platform or other JSON compatible tool)

IMPORTANT: Triage-Investigator is not sold separately. Triage-Investigator must be purchased with Digital Evidence Investigator PRO or deployed in an environment where it can be used with DEI PRO.

+ Rosoka ADD-ON **230+ Languages**
Natural Language Processing (NLP)
Entity Extraction & English Gisting