ADF

ADF4N6.COM

FIELD Investigator for Teams

CONTROL YOUR INVESTIGATIONS

Empower non-technical field investigators with the fastest on-scene digital evidence collection and analysis tools and maintain control to focus and speed their investigations.

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

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

- Automated and easy-to-learn with built in digital forensic Search Profiles so non-technical field investigators can quickly collect digital evidence based on the type of case they are working
- Rapid analysis lets field investigators make decisions on-scene
- Create comprehensive reports to share with other investigators or prosecutors for free
- Control and create Custom Search Profiles in Digital Evidence Investigator to export and share with Triage-Investigator licenses across teams or agencies

ADD-ON Options:

- Rosoka Entity Extraction and 230+ language gisting
- Learn at your own pace with self-paced training and ADF Certification in 8-16 hours

OS X Windows 7 Windows 10

COLLECT: Rapid automated evidence collection

- 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.
- Recover deleted records from apps using the SQLite database
- Supports collection of artifacts from Windows and macOS (including T2 and M1 chips)
- Search and collect emails: 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, contents of folders and network shares (including made available by NAS devices)
- 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
- 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 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, more)
- 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
- Leverage Suspect Technologies age detection to identify images of infants, toddlers, children, adults
- 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
- 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) or export to Truxton
- Export in VICS format (to Griffeye Analyze Platform or other JSON compatible tool)

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

Add Mobile Capabilities
UPGRADE TO PRO
FIELD Investigator for Teams PRO