MOBILE & COMPUTER FORENSICS

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

All ADF software shares the same intelligent search engine and rapid scan capabilities. The key differences are in the features focused on deployment and usage scenarios: Ideal for front-line and lab investigators who seek to solve investigations of iOS and Android smartphones and tablets, as well as Mac, Windows and Linux computers, external drives, drive images, and other media storage (USB flash drives, memory cards, etc.).

DEI

Digital Evidence Investigator® is the easy-to-learn, automated digital forensic software for early case assessment in the lab or on-scene. Advanced capabilities and separate authentication and collection keys allow users to scan multiple computers simultaneously. Examiners and investigators can customize search profiles to share with Triage-Investigator® users. DEI empowers investigators, reduces forensic backlogs and helps you solve your case fast.

TINV

Triage-Investigator® is the world's leading intelligent triage tool used by investigators on the front line for on-scene investigations. Triage-Investigator® is fast, easy-to-use, and supports a wide array of computer hardware with powerful boot capabilities. The forensically sound tool is deployed widely to non-technical field investigators who need to collect and analyze evidence. Investigators can import custom search profiles from DEI and benefit from a variety of court ready report options.

TG2

Triage-G2® is the ruggedized media exploitation tool deployed by special forces, military and intelligence agencies as part of their identity operation kits for sensitive site exploitation (DOMEX, MEDEX, Tactical Media Exploitation). Designed to be used in stealth mode, non-technical operators can rapidly scan, extract, and analyze critical intelligence from computers and digital devices in the field.

+

MDI

Mobile Device Investigator™ is designed to be operated by front line police, sheriffs, field agents, and digital forensic investigators to quickly and easily collect digital evidence from iOS and Android phones and tablets by connecting a suspect device via USB port to quickly collect evidence and perform an advanced logical acquisition.

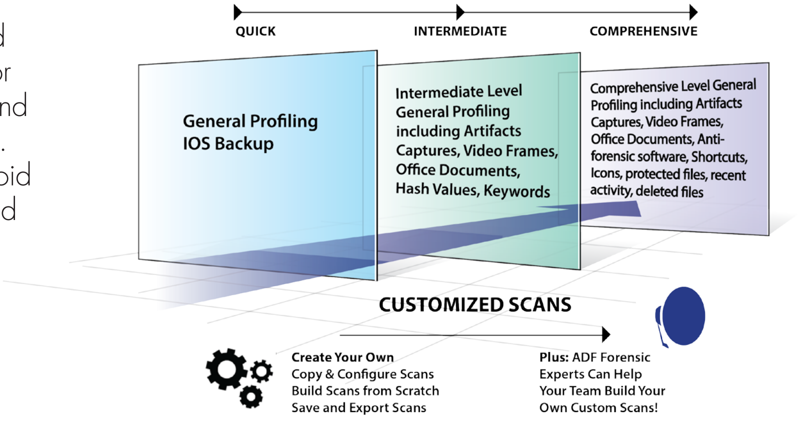
DEI PRO
Digital Evidence Investigator®
Bootable CD
Select "USB" option to boot onto the flash drive
ADF
SAMSUNG
TP-LINK
PRO

DEI PRO provides all of the capabilities of DEI and MDI in a single license.

COLLECT

Prioritize speed in evidence collection and use in the field or in the lab investigations with minimal training. Built-in or custom search profiles help investigators perform triage and early case assessment to quickly identify critical evidence. Comprehensive advanced logical backup for iOS/Android using default platform backup protocol, backup agent and media transfer protocol.

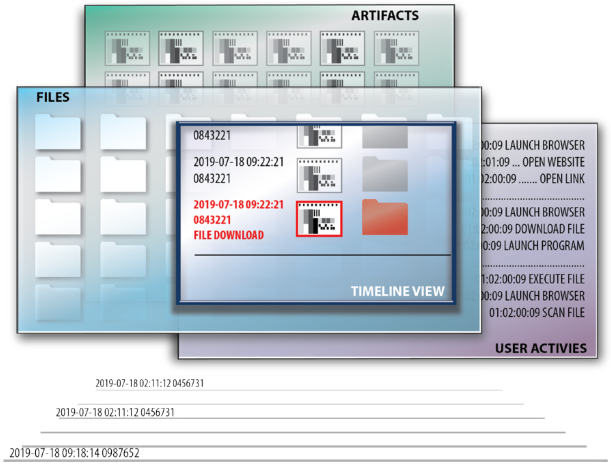
Powerful Search Profiles



ANALYZE

Review files, artifacts and user activities in a timeline view to quickly identify the what, where and who of your case. Quickly go through the recovered data with the powerful results viewer to explore gigabytes of information in minutes. Search for specific information using keywords, regular expressions, hash values and PhotoDNA and view pictures and videos organized by visual classes such as people, faces, currency, weapons, vehicles, indecent pictures of children and categorize files that match Project VIC or CAID datasets in real-time.

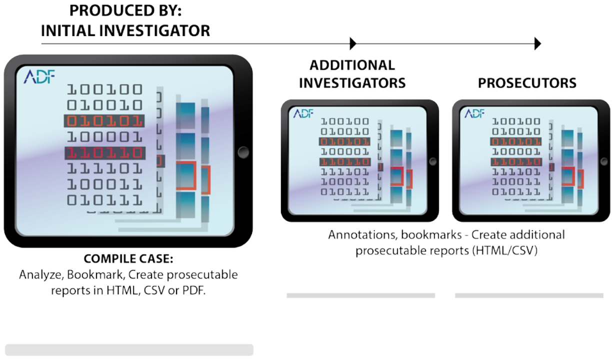
Timeline View: What, Where, and Who

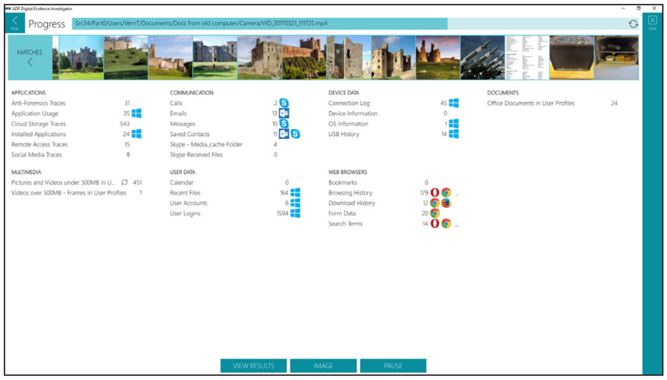


REPORT

Easily create comprehensive reports to highlight your findings and select the format most suitable for your audience. Export reports in HTML, CSV, JSON or use the ADF Standalone Portable Viewer to do case collaboration with prosecutors or fellow investigators.

Portable Reports with Standalone Viewer


PRODUCED BY:
INITIAL INVESTIGATOR
ADDITIONAL
INVESTIGATORS
PROSECUTORS
ADF
COMPILE CASE:
Analyze, Bookmark, Create prosecutable
reports in HTML, CSV or PDF.
Annotations, bookmarks - Create additional
prosecutable reports (HTML/CSV)

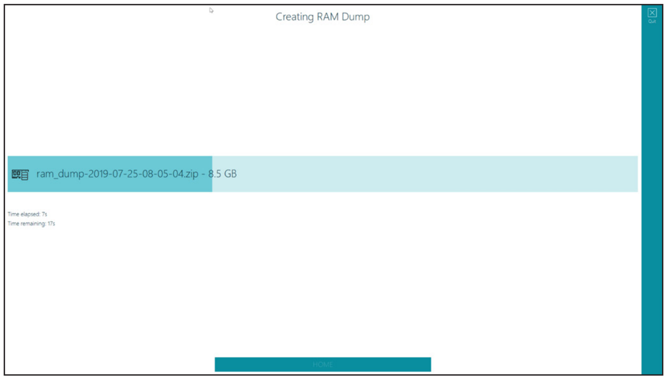


ADF Digital Evidence Investigator

Progress Src34/Part0/Users/VernT/Documents/Docs from old computer/Camera/VID_20170321_111725.mp4

APPLICATIONS		COMMUNICATION		DEVICE DATA		DOCUMENTS	
Anti-Forensics Traces	31	Calls	2	Connection Log	45	Office Documents in User Profiles	24
Application Usage	35	Emails	13	Device Information	0		
Cloud Storage Traces	543	Messages	10	OS Information	1		
Installed Applications	24	Saved Contacts	11	USB History	14		
Remote Access Traces	15	Skype - Media_cache Folder	4				
Social Media Traces	8	Skype Received Files	0				
MULTIMEDIA		**USER DATA**		**WEB BROWSERS**			
Pictures and Videos under 500MB in U...	451	Calendar	0	Bookmarks	0		
Videos over 500MB - Frames in User Profiles	1	Recent Files	164	Browsing History	179		
		User Accounts	6	Download History	12		
		User Logins	1594	Form Data	20		
				Search Terms	14		

Customized Artifact and File Collection

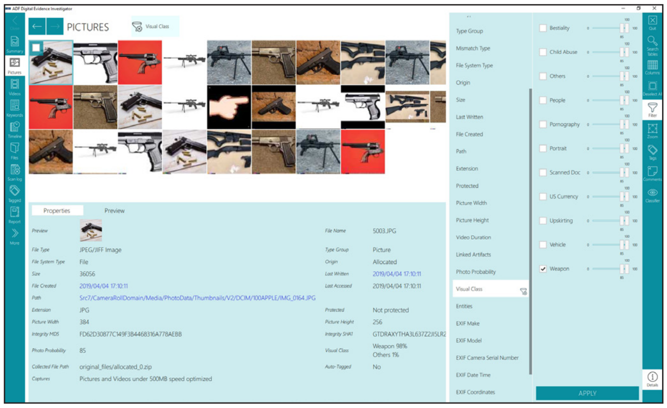


Creating RAM Dump

ram_dump-2019-07-25-08-05-04.zip - 8.5 GB

Time elapsed: 7s
Time remaining: 17s

RAM Capture



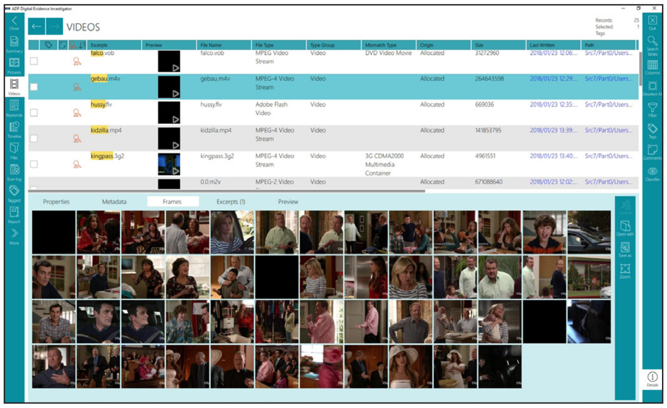
ADF Digital Evidence Investigator

PICTURES

Properties Preview

Preview		File Name	5003.JPG
File Type	JPEG/JIFF Image	Type Group	Picture
File System Type	File	Origin	Allocated
Size	36056	Last Written	2019/04/04 17:10:11
File Created	2019/04/04 17:10:11	Last Accessed	2019/04/04 17:10:11
Path	Src7/CameraRollDomain/Media/PhotoData/Thumbnails/V2/DCIM/100APPLE/IMG_0164.JPG		
Extension	JPG	Protected	Not protected
Picture Width	384	Picture Height	256
Integrity MD5	FD62D30877C149F3B4468316A778AEBB	Integrity SHA1	GTDRAXYTHA3L637Z2JI5LR2
Photo Probability	85	Visual Class	Weapon 98% Others 1%
Collected File Path	original_files/allocated_0.zip	Auto-Tagged	No
Captures	Pictures and Videos under 500MB speed optimized		

Image Classification



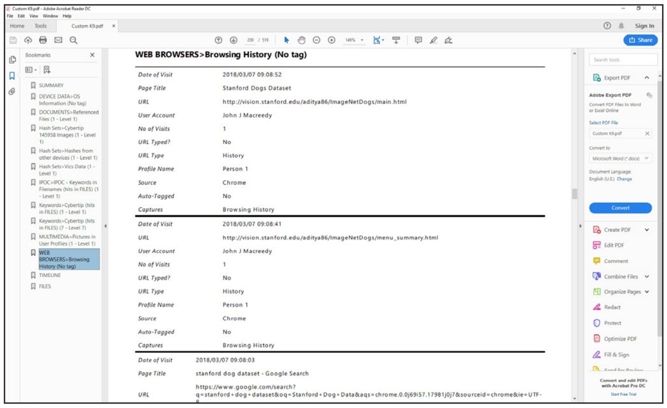
ADF Digital Evidence Investigator

VIDEOS

Records: 25
Selected: 1
Tags:

Excerpts	Preview	File Name	File Type	Type Group	Mismatch Type	Origin	Size	Last Written	Path
falco.vob		falco.vob	MPEG Video Stream	Video	DVD Video Movie	Allocated	31272960	2018/01/23 12:06:...	Src7/Part0/Users...
gebau.m4v		gebau.m4v	MPEG-4 Video Stream	Video		Allocated	264643598	2018/01/23 12:29:...	Src7/Part0/Users...
hussy.flv		hussy.flv	Adobe Flash Video	Video		Allocated	669036	2018/01/23 12:35:...	Src7/Part0/Users...
kidzilla.mp4		kidzilla.mp4	MPEG-4 Video Stream	Video		Allocated	141853795	2018/01/23 13:39:...	Src7/Part0/Users...
kingpass.3g2		kingpass.3g2	MPEG-4 Video Stream	Video	3G CDMA2000 Multimedia Container	Allocated	4961551	2018/01/23 13:40:...	Src7/Part0/Users...
		0.0.m2v	MPEG-2 Video	Video		Allocated	671088640	2018/01/23 12:02:...	Src7/Part0/Users...

Video Frames



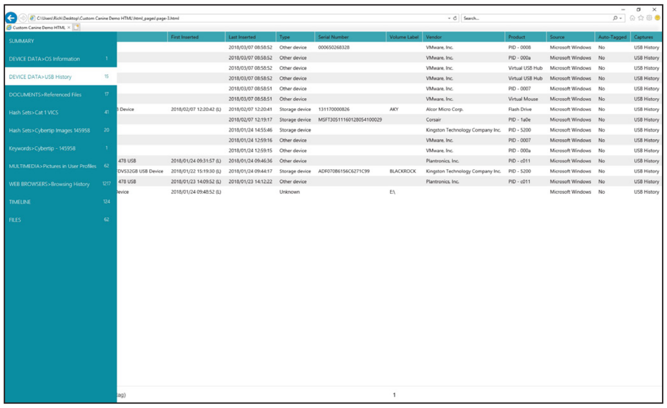
Custom K9.pdf - Adobe Acrobat Reader DC

File Edit View Window Help
Home
Tools
Custom K9.pdf
Sign In
209 / 519
149%
Share
Bookmarks
SUMMARY
DEVICE DATA>OS Information (No tag)
DOCUMENTS>Referenced Files (1 - Level 1)
Hash Sets>Cybertip 145958 Images (1 - Level 1)
Hash Sets>Hashes from other devices (1 - Level 1)
Hash Sets>Vics Data (1 - Level 1)
IPOC>IPOC - Keywords in Filenames (hits in FILES) (1 - Level 1)
Keywords>Cybertip (hits in FILES) (1 - Level 1)
Keywords>Cybertip (hits in FILES) (7 - Level 7)
MULTIMEDIA>Pictures in User Profiles (1 - Level 1)
WEB BROWSERS>Browsing History (No tag)
TIMELINE
FILES
Search tools
Export PDF
Adobe Export PDF
Convert PDF Files to Word or Excel Online
Select PDF File
Custom K9.pdf
Convert to
Microsoft Word (*.docx)
Document Language:
English (U.S.) Change
Convert
Create PDF
Edit PDF
Comment
Combine Files
Organize Pages
Redact
Protect
Optimize PDF
Fill & Sign
Convert and edit PDFs with Acrobat Pro DC
Start Free Trial

WEB BROWSERS>Browsing History (No tag)

Date of Visit	2018/03/07 09:08:52
Page Title	Stanford Dogs Dataset
URL	http://vision.stanford.edu/aditya86/ImageNetDogs/main.html
User Account	John J Macreedy
No of Visits	1
URL Typed?	No
URL Type	History
Profile Name	Person 1
Source	Chrome
Auto-Tagged	No
Captures	Browsing History
Date of Visit	2018/03/07 09:08:41
URL	http://vision.stanford.edu/aditya86/ImageNetDogs/menu_summary.html
User Account	John J Macreedy
No of Visits	1
URL Typed?	No
URL Type	History
Profile Name	Person 1
Source	Chrome
Auto-Tagged	No
Captures	Browsing History
Date of Visit	2018/03/07 09:08:03
Page Title	stanford dog dataset - Google Search
URL	https://www.google.com/search?q=stanford+dog+dataset&oq=Stanford+Dog+Data&aqs=chrome.0.0j69i57.17981j0j7&sourceid=chrome&ie=UTF-

PDF Reporting



C:\Users\Rich\Desktop\Custom Canine Demo HTML\html_pages\page-3.html

SUMMARY	
DEVICE DATA>OS Information	1
DEVICE DATA>USB History	15
DOCUMENTS>Referenced Files	17
Hash Sets>Cat 1 VICS	41
Hash Sets>Cybertip Images 145958	20
Keywords>Cybertip - 145958	1
MULTIMEDIA>Pictures in User Profiles	62
WEB BROWSERS>Browsing History	1217
TIMELINE	124
FILES	62

	First Inserted	Last Inserted	Type	Serial Number	Volume Label	Vendor	Product	Source	Auto-Tagged	Captures
		2018/03/07 08:58:52	Other device	000650268328		VMware, Inc.	PID - 0008	Microsoft Windows	No	USB History
		2018/03/07 08:58:52	Other device			VMware, Inc.	PID - 000a	Microsoft Windows	No	USB History
		2018/03/07 08:58:52	Other device			VMware, Inc.	Virtual USB Hub	Microsoft Windows	No	USB History
		2018/03/07 08:58:52	Other device			VMware, Inc.	Virtual USB Hub	Microsoft Windows	No	USB History
		2018/03/07 08:58:51	Other device			VMware, Inc.	PID - 0007	Microsoft Windows	No	USB History
		2018/03/07 08:58:51	Other device			VMware, Inc.	Virtual Mouse	Microsoft Windows	No	USB History
Device	2018/02/07 12:20:42 (L)	2018/02/07 12:20:41	Storage device	131170000826	AKY	Alcor Micro Corp.	Flash Drive	Microsoft Windows	No	USB History
		2018/02/07 12:19:17	Storage device	MSFT30511160128054100029		Corsair	PID - 1a0e	Microsoft Windows	No	USB History
		2018/01/24 14:55:46	Storage device			Kingston Technology Company Inc.	PID - 5200	Microsoft Windows	No	USB History
		2018/01/24 12:59:16	Other device			VMware, Inc.	PID - 0007	Microsoft Windows	No	USB History
		2018/01/24 12:59:15	Other device			VMware, Inc.	PID - 000a	Microsoft Windows	No	USB History
478 USB	2018/01/24 09:31:57 (L)	2018/01/24 09:46:36	Other device			Plantronics, Inc.	PID - c011	Microsoft Windows	No	USB History
DVS32GB USB Device	2018/01/22 15:19:30 (L)	2018/01/24 09:44:17	Storage device	ADF070B6156C6271C99	BLACKROCK	Kingston Technology Company Inc.	PID - 5200	Microsoft Windows	No	USB History
478 USB	2018/01/23 14:09:52 (L)	2018/01/23 14:12:22	Other device			Plantronics, Inc.	PID - c011	Microsoft Windows	No	USB History
evice	2018/01/24 09:48:52 (L)		Unknown		E:\			Microsoft Windows	No	USB History

HTML Reports

GET YOUR FREE TRIAL TRYADF.com

COMPARE ADF DIGITAL FORENSIC SOFTWARE PRODUCTS

	MDI	DEI	TIINV	TG2
Setup and Configuration				
Define and package custom search criteria (Search Profiles)	Y	Y	N	Y
Create custom data Captures (keywords, SHA-1/MD-5 hash, grep search, file collection)	Y	Y	N	Y
Import VICS and CAID datasets for auto-categorization	Y	Y	N	Y
Customize file headers	Y	Y	N	Y
Configure folders and paths to scan	Y	Y	N	Y
Set filters by file properties (size, timestamps, etc.)	Y	Y	N	Y
Import Captures and Search Profiles	Y	Y	Y	Y
Export Captures and Search Profiles	Y	Y	N	Y
Out-of-the-box Search Profiles for "Media Exploitation"	Y	N	N	Y
Out-of-the-box Search Profiles for "Law Enforcement" (including Indecent Images)	Y	Y	Y	N
Use any USB drive as a Collection Key	N	Y	Y	N
Use BitLocker to protect the Collection Key	N	Y	Y	Y
Searching Digital Devices and Images				
Forensically Sound	N	Y	Y	Y
Scan turned-on Windows computers (live scan)	N	Y	Y	Y
Scan turned-off Windows, Mac, Linux computers (boot scan)	N	Y	Y	Y
Scan multiple computers on-site with a single license dongle	N	Y	Y	N
Scan drive images (e01, dd)	N	Y	Y	Y
Scan connected and unlocked Android/iOS devices	Y	Pro	Pro	Pro
Scan Android/iOS ADF backups	Y	Pro	Pro	Pro
Scan iTunes backup found on target computer	N	Pro	Pro	Pro
Scan NTFS, FAT, ExFAT, HFS+, APFS, EXT2/3/4, YAFFS2 file systems	N	Y	Y	Y
Scan devices connected to suspect computer	N	Y	Y	Y
Scan external devices (USB, CD, DVD, SD cards, etc.) from forensic/friendly computer	N	Y	Y	Y
RAM capture	N	Y	Y	Y
Recover hundreds of file types	Y	Y	Y	Y
Recover communication artifacts (emails, chats, contacts, etc)	Y	Y	Y	Y
Recover system artifacts (user accounts, wifi connections, USB history, installed apps, etc)	Y	Y	Y	Y
Recover application artifacts (peer-to-peer, anti-forensics, crypto-currency, etc)	Y	Y	Y	Y
Recover web browser artifacts (browsing history, bookmarks, search terms, etc)	Y	Y	Y	Y
Prompt for password for encrypted partitions (FileVault2 HFS/APFS, Bitlocker)	N	Y	Y	Y
Conduct live scans in Stealth mode	N	N	N	Y
Automatically start a boot or live scan	N	N	N	Y
Imaging Digital Devices				
Image suspect drives and storage devices	N	Y	Y	Y
Backup Android/iOS devices	Y	Pro	Pro	Pro
Analysis and Reporting				
Review evidence directly on suspect computer	N	Y	Y	Y
Comprehensive filtering of results	Y	Y	Y	Y
Analyze all files, artifacts, and users' activities in a single timeline	Y	Y	Y	Y
View links between files of interest and user's activities	Y	Y	Y	Y
Tag and comment on relevant records to build report	Y	Y	Y	Y
Automatic visual classification of pictures and videos	Y	Y	Y	Y
Create comprehensive reports	Y	Y	Y	Y
Export reports to HTML, PDF, VICS, and CSV formats	Y	Y	Y	Y
Export reports to a standalone viewer executable	Y	Y	Y	Y

www.adfsolutions.com

©2019 ADF Solutions, Inc. All rights reserved. U.S. Pat. No. 8,219,588 and 7,941,386. Digital Evidence Investigator, Triage-Investigator, Triage-G2, and Mobile Device Investigator are registered trademarks or trademarks of ADF Solutions. All other trademarks referenced herein are the property of their respective owners.