Technical Specifications

Introduction

This guide covers the technical specifications of the ADF application.

This document applies to the following applications		
ADF PRO	Digital Evidence Investigator	Mobile Device Investigator

Supported Target Devices/Operating Systems

The ADF application is designed to scan and image the following systems:

- Android
  - Advanced logical acquisition from the Desktop application
  - Scan of the ADF advanced logical acquisition
  - Preview from the Desktop application
  - **BETA**: scan of acquisitions from GrayKey, UFED
- ChromeOS
  - Advanced logical acquisition from the Desktop application
  - Scan of the ADF advanced logical acquisition
- iOS
  - Advanced logical acquisition from the Desktop application
  - Scan of the ADF advanced logical acquisition
  - Preview from the Desktop application
  - **BETA**: scan of acquisitions from GrayKey, UFED
- macOS (version 10.7 or newer on Intel and Apple Silicon)
  - Logical imaging from the remote agent running live
  - Scan from the remote agent running live
- KaiOS
  - Logical acquisition via MTP protocol from the Desktop application
- Windows (Intel 64-bit, Windows 64-bit)
  - Physical imaging from the Collection Key boot and live modes
  - Logical imaging from the remote agent running live
  - Scan from the Collection Key boot and live modes
  - Scan from the remote agent running live
  - Limitation when booting from the Collection Key:
    - Firmware: BIOS, UEFI, Secure UEFI
    - CPU: Intel 64-bit, AMD-64 or compatible

        - RAM: 2GB or more
        - File systems: FAT[4], NTFS, EXT2/3/4, ExFAT[4], YAFFS2[1]
        - RAID: see this section for details
        - Windows Dynamic Disks: not supported
    - Limitations when running live from the Collection Key:
        - Windows Vista2/7/8/10/11 64-bit, Server 2008/2012/2016/2019 64-bit
        - Windows Dynamic Disks: simple volumes only (no spanned, striped, mirrored, RAID-5 volumes)
- Windows (Windows 32-bit)
    - Logical acquisition from the remote agent running live
    - Scan from the remote agent running live
- Windows (ARM processor)
    - Logical acquisition from the remote agent running live
    - Scan from the remote agent running live
- Drive image scan in the Desktop application
    - Format: dd and e01, ex01 (except compressed and encrypted), L01 (EnCase Logical Evidence File), AFF4, ADF Data Container (using the standard zip format)
    - File systems: FAT[4], NTFS, APFS[2][3], HFS+, EXT2/3/4, ExFAT[4], YAFFS2[1]
    - Scan: recover deleted partitions by locating filesystem tables in unallocated space
    - OS: Windows, Mac, Linux, iOS, Android
    - RAID: rebuilding RAID is not supported, so image must represent a logical disk
- Folder scan from the Desktop application
    - OS: Windows, Mac, Linux, iOS, Android
- Network share from the Desktop application
    - OS: Windows, Mac
- RAM capture
    - Memory capture is supported for live Windows scan only (see above)
- Disk encryption
    - BitLocker: detection and unlocking with passphrase or recovery key (mandatory for TPM protected volumes). BitLocker detection does not work for target USB flash drives that have only one partition. Unlocking BitLocker encrypted drive images is not supported.
    - TPM Chip: volumes protected by the TPM chip are supported.
    - FileVault2 over HFS+, FileVault2 over APFS, T2 chip: need to be unlocked on the live Mac prior to running the remote agent.

Note [1]: Can only detect YAFFS2 on partitions smaller than 32GB. Timezone detection is not supported on these partitions.
Note [2]: Timezone detection may not work properly
Note [3]: Compressed files cannot be read yet
Note [4]: Volume larger than 1TB can take hours to cache during the scan

Information to Share with ADF's Technical Support

Most issues are not reproducible in-house because they depend on specific data and environment unavailable to ADF's technical support team. For this reason we need as much information from you as possible. We may also have follow-up questions or tests for you to perform.

When encountering an issue, please collect the following information and share it with the support team:

- Step by step instructions on how to reproduce the issue.
- A screenshot or photo of the error message or problem.
- The log files container (press Ctrl + Alt + L from the screen showing the error message to create this container).
- The crash dump if any (see the section below to locate it).
- Go to this link to upload the support files and share them with the support team (a Google account is needed - go here to create one if needed).

Enabling Debug Mode

In order for ADF to learn more about the specific conditions of an issue to eventually reproduce it in-house, it is often useful to obtain a more detailed log file. If the support team asks for the debug log file, please follow this procedure:

- Start the ADF desktop application.
- Activate the debug log level by pressing Ctrl + Alt + D from the Home screen.
- Rerun through the steps that caused the issue in the first place.
- See below how to share the debug log files.

To obtain more detailed log information related to the file system decoding, it is possible to start the Desktop application from the command line and use the -fslib-debug parameter:

```
adf.exe -fslib-debug
```

Log Files

The application creates multiple log files that are useful to identify the source of potential issues. These files do not contain scan results and are safe to share with ADF’s support team. Log files can be found in:

- Log files created by the desktop application:
  - C:\ProgramData\ADF Solutions Inc\v4\ScanResults\<SCAN NAME>\SysLogs
  - C:\ProgramData\ADF Solutions Inc\v4\SysLogs
- Log files created by the scanner application on the Collection Key:
  - \ScanResults\<SCAN NAME>\SysLogs
  - \SysLogs
- Audit Logs:
  - C:\ProgramData\ADF Solutions Inc\v4\AuditTrail

The following log files are created:

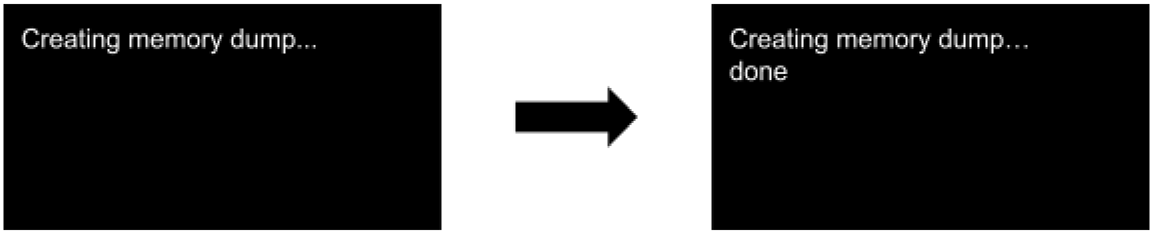
- adf.exe_DATE_TIME.N.log: Log file created by the main application with messages related to Search Profile Management, CK Preparation, Scan Preparation, Device Enumeration, Imager, Licensing, Viewer and Export.
- scan.exe_DATE_TIME.N.log: Log file created by the scanner with messages related to the scan (Captures, file type detection, space on the drive where scan result go, etc).
- parser_host.exe_DATE_time.N.log: Log file created by the parser crash recovery process during a scan with messages related to parsing libraries (Oracle OI, ffmpeg, FreeImage, etc).
- adfsvc_DATE_TIME.N.log: Log file created by the service running in the background allowing a Windows Standard User to access a physical drive.
- audit_trail_DATE_TIME.N.log: Log file with usage information.

Crash Dump

In case the application crashes, a process memory dump is created in the following locations:

- Desktop application:
  - ○ C:\ProgramData\ADF Solutions Inc\v4\CrashDump
  - ○ C:\ProgramData\ADF Solutions Inc\v4\ScanResults\<SCAN NAME>\CrashDump
- Scanner application on the Collection Key:
  - ○ \CrashDump
  - ○ \ScanResults\<SCAN NAME>\CrashDump

NOTE: Wait until the application is done creating the crash dump before closing it!



```
Creating memory dump...
```

```
Creating memory dump…
done
```

Forensic Integrity

Boot Mode

ADF forensics tools are forensically sound in boot mode. This means that no changes are made to the disks. Any issues that may compromise this situation have been disabled. For example disks formatted as Microsoft Dynamic disks are not supported at the current time because mounting such disks would entail writing to the drive. We hope to overcome this limitation in a future version.

Live Mode

ADF forensics tools are forensically sound in live mode as the changes made to the running system are well understood and documented below. It should be expected that running the ADF application on a live system will leave trace related to:

- The insertion of the flash drives (Collection Key and Authentication Key)
- The execution of the ADF application

Windows Computer

On a Windows computer, the timestamps of the files accessed by the ADF application are not modified as only the storage media blocks are accessed.

The below listed locations were created, modified, or deleted upon the insertion of the USB key and execution of the ADF application. Testing shows that changes are made to Temporary files, Prefetch files, Event Logs, and the System, Software, and NTUser.dat registry files. The results below are from a specific machine and actual modifications will depend on specific computer configurations, controlset in use, and software applications running.

Windows files created, modified, and deleted:

- C:\Windows\Prefetch\ADF_PYCAPT_APP.EXE-XXXXXXXX.pf (File Created)
- C:\Windows\Prefetch ADF.EXE-XXXXXXXX.pf (File Created)
- C:\Windows\Prefetch PARSER_HOST.EXE-XXXXXXXX.pf (File Created)
- C:\Windows\Prefetch SCAN.EXE-XXXXXXXX.pf (File Created)
- C:\Windows\INF setupapi.dev.log (Modified unless key was previously in log)

Windows Registry Keys created or keys added upon introduction of USB Device:

- HKEY_LOCAL_MACHINE\system\controlsetxxx\enum\pci\<hardware id>\<serial number>\Device Parameters\{GUID}
- HKEY_LOCAL_MACHINE\system\controlsetxxx\enum\usb\<hardware id>\<instance id>\Device Parameters
- HKEY_LOCAL_MACHINE\system\controlsetxxx\enum\usbstor\<hardware id>\<serial number>\Device Parameters
- HKEY_LOCAL_MACHINE\software\microsoft\windows\currentversion\explorer\desktop\namespace
- HKEY_LOCAL_MACHINE\software\microsoft\windows\currentversion\explorer\desktop\namespace\delegatefolders
- HKEY_USERS\<computername>\<USER>\software\microsoft\windows\currentversion\explorer\mountpoints2\
- HKEY_USERS\<computername>\<USER>\software\microsoft\windows\currentversion\explorer\desktop\namespace
- HKEY_USERS\<computername>\<USER>\software\microsoft\windows\currentversion\explorer\sessioninfo\2\applicationviewmanagement\
- HKEY_USERS\<computername>\<USER>\software\microsoft\windows\currentversion\explorer\sessioninfo\2\applicationviewmanagement\
- HKLM\Software\Python\PythonCore\3.8\PythonPath\
- HKLM\SOFTWARE\Microsoft\Cryptography\

- HKLM\System\CurrentControlSet\Services\bam\State\UserSettings\XXXX\\Device\HarddiskVolume10\win\x64\pycapt\adf_pycapt_app.exe
- HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Compatibility32\adf_pycapt_app
- HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\adf_pycapt_app.exe
- HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\scan.exe
- HKLM\Software\Microsoft\Windows\CurrentVersion\App Paths\scan.exe
- HKLM\System\CurrentControlSet\Enum\SCSI\Disk&Ven_XXXXXXXXXXXXXXX (Ven = vendor of collection key)
- HKLM\System\CurrentControlSet\Control\Class\{xxxxxxxxx}\0000\@adf.exe
- HKCR\AppID\adf.exe
- HKLM\Software\Microsoft\Windows\CurrentVersion\App Paths\adf.exe
- HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\adf.exe

Windows Event Logs modified if enabled:

- Microsoft-Windows-DriverFrameworks-UserMode/Operational - If enabled
- Microsoft-Windows-DeviceSetupManager - Admin.evtx
- Microsoft-Windows-DeviceSetupManager - Operational.evtx
- Microsoft-Windows-Kernel-PnP - Configuration.evtx
- Microsoft-Windows-Ntfs - Operational.evtx
- System.evtx

macOS Computer

On a macOS computer, the ADF remote agent uses the native system API to list the files and read their content. The exact API calls are open(O_RDONLY), close(), lstat(), read(), opendir(), readdir(), exec(). These functions trigger a change in the Modified timestamp of all the files accessed which should reflect the time of the scan.

MacOS files modified:

- File System files
  - /Catalog - the main catalog file of the file system
- Log files
  - /private/var/db/diagnostics/logdata.statistics.0.txt
  - /private/var/db/diagnostics/Persist/0000000000000060.tracev3
  - /private/var/log/DiagnosticMessages/2021.06.21.asl
- Settings
  - /private/var/db/SystemPolicyConfiguration/ExecPolicy

macOS Computer in Recovery Mode

In Recovery mode, the Modified timestamp of all the files accessed by the ADF remote agent is not modified.
MacOS files modified:

- /BOOTLOG - contains a reference to the Collection Key
- /EFI/APPLE/CACHES/CAFEBEEF/xxxxx.cbl - contains a reference to the Collection Key
- /.fseventsd/* - multiple files logging file system events

Files Integrity

When collecting files from a target device, their MD5 and SHA1 hash values are computed and saved in the scan results. This makes it possible to verify their integrity at a later point in time.

Drive Image Integrity

When imaging a volume or a drive, an MD5 hash value and a SHA1 hash value are computed on all the sectors being read. These hash values are stored in the image log file. It is also possible to recompute these hash values from the image to verify that they match the original hash values.

Stealth Mode

This section applies to the following applications		
ADF PRO PRO	Digital Evidence Investigator DEI	

Live scans can operate in “stealth mode”. In stealth mode, the ADF application makes it difficult to locate traces it leaves on the target computer. Here is a list of traces left and how they are concealed:

- Collection Key name is changed from “CKY” to “Removable Drive”.
- All executable names (adf.exe, scan.exe, etc) are renamed to use common Windows application names (cmd.exe, svchost.exe, etc).
- Files saved in temporary storage (Temp OEgetPrivileges.vbs) are renamed (prncnfg.vbs).

File Parsers

Parsers are used to access files embedded in other files, or to access data encoded in files. The following file formats have a dedicated parser:

Group	Name	Extension	File Name	Password Protection Detection	Carving	Thorough Detection Method
Archive	7zip Archive	7z		Yes		Magic
Archive	BZ Archive	bz2				Magic
Archive	Compressed ROM	cramfs				Magic
Archive	GNU Zip Archive	gz gzip				Magic
Archive	Java Archive	jar				Heuristic

Archive	Roshal Archive	rar r01		Yes		Magic
Archive	Squash File System	squashfs				Magic
Archive	Tar Archive	tar				Heuristic
Archive	ZIP Archive	zip		Yes		Magic
Audio File	Adaptive Multi-Rate Codec	amr				Magic
Audio File	MP4 Audio Stream	f4a				None
Audio File	MP4 Audio eBook	f4b				None
Audio File	MP4 Audio File	m4a				None
Audio File	MPEG Audio Stream	mp3 mpga				Magic
Audio File	Ogg Vorbis	ogg				Magic
Audio File	Ogg Vorbis Audio File	ogg oga				Magic
Audio File	Opus	opus				Magic
Audio File	Waveform Audio	wav				Magic
Audio File	Apple Core Audio	caf				Magic
Audio File	3G UMTS Multimedia Container Audio Only	3ga				None
Audio File	Music File Format	669				None
Audio File	Advanced Audio Coding File	aac				None
Audio File	Audio Codec 3 File	ac3				None
Audio File	Audio Data Transport Stream Format	adt adts				None
Audio File	Audio Interchange File Format	aif aiff				None
Audio File	Compressed Audio Interchange File Format	aifc				None
Audio File	Ambisonic File Format	amb				None
Audio File	Audio Object File Format	aob				None
Audio File	Monkey's Audio File Format	ape				None
Audio File	Sun Microsystems Audio File Format	au				None
Audio File	Adaptive Multi-Rate File Format with WideBand support	awb				None
Audio File	Free Lossless Audio Codec	flac				None
Audio File	Digital Theater Systems File Format	dts				None
Audio File	MPEG-4 Audiobook File Format	m4b				None
Audio File	iTunes Audio File Format	m4p				None

Audio File	Musical Instrument Digital Interface File Format	mid				None
Audio File	Matroska Audio File Format	mka				None
Audio File	Meridian Audio File Format	mlp				None
Audio File	MPEG-2 Compression File Format	mpa				None
Audio File	MPEG-1 Compression File Format	mp1				None
Audio File	MPEG Layer 2 Audio File Format	mp2				None
Audio File	Sony CONNECT Music Store Audio File	oma				None
Audio File	PureVoice Audio File Format	qcp				None
Audio File	RealAudio File Format	ra				None
Audio File	Speex Compression Ogg Vorbis Audio Format	spx				None
Audio File	Tom's lossless Audio Kompressor	tak				None
Audio File	Dolby TrueHD Audio File Format	thd				None
Audio File	True Audio Codec	tta				None
Audio File	Wave 64 Audio File Format	w64				None
Audio File	WavPack Hybrid Audio File Format	wv				None
Audio File	Audio Visual Research Format	avr				None
Audio File	GSM 06.10 Lossy Speech Compression	cdda				None
Audio File	Continuously Variable Slope Delta Modulation	cvs cvsd				None
Audio File	Continuously Variable Slope Delta Modulation (unfiltered)	cvu				None
Audio File	Variable Slope Delta Modulation Audio	dvms				None
Audio File	PARIS Audio File Format	fap				None
Audio File	FSSD Sound	fsdd				None
Audio File	Grandstream Ring-tone Files	gsrt				None

Audio File	Portable Voice Format	pvf				None
Audio File	Dialogic Voice Audio File	vox				None
Binary File	Java Class	class				Magic
Binary File	Dynamic Link Library	dll				Heuristic
Binary File	Executable	exe				Heuristic
Binary File	ELF Binary	so				Magic
Database File	Microsoft Access 2007	accdb accde accdr				Magic
Database File	Comma-Separated Values	csv				None
Database File	Generic Database	db				None
Database File	xBASE Database	dbf				None
Database File	ESE Database	edb				Magic
Database File	Microsoft Money Backup	mbf				Magic
Database File	Microsoft Access Database	mdb mde				Magic
Database File	Microsoft Money	mny				Magic
Database File	QuickBooks Backup	qbb				None
Database File	QuickBooks	qbw				None
Database File	Quicken	qdf				Magic
Database File	Quicken Interchange Format	qif				None
Database File	sqlite Database	sqlite				Magic
Database File	VersaCheck Backup	vbf				None
Database File	VersaCheck File	vdf				None
Disk Image	GNU Raw Multivolume Image	001	(?i:.*\.dd$)			None
Disk Image	CD Image Track Info	cue				None
Disk Image	GNU Raw Image	dd				None
Disk Image	Apple Disk Image	dmg				Magic
Disk Image	Expert Witness Format Image	ewf e01				Magic
Disk Image	Expert Witness Format Image v2	Ex01				None
Disk Image	Disk Image	img				None
Disk Image	ISO-9660 CD Image	iso				Magic
Disk Image	Encase Logical Image	L01				Magic
Disk Image	SMART Disk Image	S01				None
Disk Image	Sparse Image	sparseimage				Magic
Disk Image	VirtualBox Image	vdi				None
Disk Image	VMWare Image	vmdk				Magic
Document	Microsoft Word (Binary)	doc dot		Yes (No for Libre/OpenOffice)		Heuristic

Document	Microsoft Word (XML-based)	docm docx dotm dotx		Yes (No for Libre/OpenOffice)		Heuristic
Document	Apple iWork Keynote	key		Yes		Heuristic
Document	Apple iWork Numbers	numbers		Yes		Heuristic
Document	OpenDocument Formula	odf				Heuristic
Document	OpenDocument Graphics	odg				Heuristic
Document	OpenDocument Presentation	odp				Heuristic
Document	OpenDocument Spreadsheet	ods				Heuristic
Document	OpenDocument Text Document	odt				Heuristic
Document	Microsoft OneNote Index	onetoc2				Magic
Document	OpenDocument Presentation Template	otp				Heuristic
Document	OpenDocument Spreadsheet Template	ots				Heuristic
Document	OpenDocument Text Document Template	ott				Heuristic
Document	Apple iWork Pages	pages		Yes		Heuristic
Document	Portable Document Format	pdf				Magic
Document	Microsoft PowerPoint (Binary)	ppt		Yes (No for Libre/OpenOffice)		Heuristic
Document	Microsoft PowerPoint (XML-based)	pptm pptx		Yes (No for Libre/OpenOffice)		Heuristic
Document	Microsoft Publisher	pub				Heuristic
Document	Rich Text Format	rtf				Magic
Document	Data Exchange File	slk				Magic
Document	StarOffice XML Writer document	sxw				Heuristic
Document	Microsoft Works	wps				Heuristic
Document	Microsoft Excel (Binary)	xls		Yes (No for Libre/OpenOffice)		Heuristic
Document	Microsoft Excel (XML-based)	xlsm xlsx		Yes (No for Libre/OpenOffice)		Heuristic
Document	XML Paper Specification	xps				Heuristic

Email File	Microsoft Outlook Express	dbx				Magic
Email File	Electronic Mail	eml				None
Email File	Mailbox Message File	mbx				Magic
Email File	Outlook Mail Message	msg				Heuristic
Email File	Microsoft Outlook	ost pst				Magic
Email File	vCard	vcf vmg v				Magic
Internet File	ASP.NET Web Page Source	aspx				Heuristic
Internet File	Javascript	js				Heuristic
Internet File	MHTML Web Archive	mht				None
Internet File	PHP script	php				Heuristic
Internet File	HTML Page	shtml html shtm htm				Heuristic
Internet File	Extensible Markup Language	xml				Heuristic
MAC OS Artefact	Apple Keychain Data	keychain				None
MAC OS Artefact	Apple Property List	plist				Magic
Misc Artefact	Configuration	cfg				None
Misc Artefact	Configuration	conf				None
Misc Artefact	Shortcut	lnk				Magic
Misc Artefact	Log	log				None
Misc Artefact	Resource	rc				None
P2P File	P2P Cache	met				None
P2P File	Torrent	torrent				Magic
Picture	Hasselblad 3F RAW Image	3fr				Magic
Picture	ARRI RAW Image	ari				None
Picture	Sony Digital Camera Image	arw srf sr2				None
Picture	Windows OS/2 Bitmap Graphics	bmp			Yes	Heuristic
Picture	Corel Photo-Paint	cpt				Magic
Picture	Canon Raw Image	cr2				Magic
Picture	Canon Raw Image	crw				None
Picture	Kodak RAW Image	dcr kdc				None
Picture	Digital Negative Image	dng				None
Picture	Enhanced Windows Metafile	emf				Heuristic
Picture	Encapsulated PostScript	eps				Heuristic
Picture	Epson RAW Image	erf				Magic
Picture	Graphic Interchange Format	gif gifv			Yes	Heuristic

Picture	High Efficiency Image Container	heic heif				Magic
Picture	Phase One RAW Image	iiq				Magic
Picture	JPEG/JIFF Image	jpe jpg jpeg jfif jpg_320x240 jpg-320x240 jpg_170x128 jpg-170x128 new jfi jif			Yes	Heuristic
Picture	Minolta Agfa RAW Image	mdc				None
Picture	Mamiya RAW Image	mef				Magic
Picture	JPEG 2000	mj2 mpj2 jp2 j2k jpf jpx jpm jpc jpp jpa jpeg2k jpg2k jpeg2000 jpg2000				Magic
Picture	Leaf Camera RAW Image	mos				None
Picture	Minolta Raw Image	mrw				None
Picture	Nikon Raw Image	nef nrw				Heuristic
Picture	Olympus RAW Image	orf				None
Picture	Paintbrush Bitmap Graphic	pcx				Heuristic
Picture	Pentax RAW Image	pef				Magic
Picture	Portable Network Graphic	png			Yes	Heuristic
Picture	Portable Pixmap Image	ppm				None
Picture	Photoshop Format	psd			Yes	Heuristic
Picture	Fuji RAW Image	raf				None
Picture	Panasonic RAW Image	rw2 raw				None
Picture	Leica RAW Image	rwl				None
Picture	Samsung RAW Image	srw				Magic
Picture	Truevision Targa Graphic	tga				Heuristic
Picture	Tagged Image Format	tiff			Yes	Heuristic
Picture	WebP Image Format	webp wep			Yes	None
Picture	Windows Metafile	wmf				Heuristic
Picture	SIGMA X3F Camera RAW Image	x3f				None
Picture	X11 Pixmap Graphic	xpm				Magic
Picture	Casio RAW	bay				None
Picture	BMQ File Format	bmq				None
Picture	Canon Raw Imaget	cr3				None

Picture	Camera RAW Image File(Capture Shop) file	cs1				None
Picture	RAW file format for Kodak digital camera	dc2				None
Picture	Hasselblad RAW Image	fff				None
Picture	High Dynamic Range	hdr				None
Picture	Kodak DC25 RAW	k25				None
Picture	Logitech Camera Raw(PXN)	pxn				None
Picture	Rollei RDC images	rdc				None
Picture	CINE format	cine				None
Picture	IA format	ia				None
Picture	KC2 format	kc2				None
Picture	Apple QuickTake Picture	qtk				None
Picture	STI format	sti				None
Picture	Kodak Pro Back RAW	drf				None
Picture	Digital Still Camera	dsc				None
Picture	Pentax RAW images	ptx				None
Picture	CAP format	cap				None
Picture	Rawzor Compressed Raw Image file	rwz				None
Picture	Kodak digital camera RAW file format	dib				None
Picture	CIN(Kodak Cineon) Files	cin				None
Picture	Digital Imaging and Communications in Medicine(DICOM) images	dcm				None
Picture	Digital Picture Exchange	dpx				None
Picture	Flexible Image Transport System	fits				None
Picture	Radiance RGBE Image Format	rgbe				None
Picture	AV1 Image File Format	avif				None
Picture	Icon Image(ICO)	ico				None
Picture	Interchange File Format	iff				None
Picture	J2C format	j2c				None
Picture	JPEG XL file format	jxl				None
Picture	OpenEXR Bitmap File Format	exr sxr mxr				None

Picture	Volume sparse data file format	vdb				None
Picture	Portable Graymap Image(PGM), Portable Any Map Image(PNM)	pgm pbm pnm pfm				None
Picture	PSD formats	pdd psb				None
Picture	Per - Face Texture Mapping(PTEX)	ptex				None
Picture	REDCODE RAW(R3D)	r3d				None
Picture	Run - Length Encoded, version A(RLA)	rla				None
Picture	Silicon Graphics Image File	sgi rgb rgba bw int inta				None
Picture	PIC format	pic				None
Picture	Truevision(TARGA) Raster Graphics File Format	tpic				None
Picture	TIFF formats	tx env sm vsm				None
Picture	HEIC formats	heics hif				None
Picture DB File	Windows Picture Database	db	(?i:.*(thumb|icon)cache_(16|32|48|96|256|768|1024|1280|1600|1920|2560|sr|wide|exif))			Magic
Picture DB File	Windows XP Picture Database	db	thumbs			None
Picture DB File	iOS Thumbnail Database	ithmb				None
Text File	Text	txt text				None
Video	3G CDMA2000 Multimedia Container	3g2 3gp2 3gpp2				Heuristic
Video	3G UMTS Multimedia Container	3gp 3gpp				Heuristic
Video	Microsoft Advanced Systems Format	asf wma wmv				Magic
Video	Audio Video Interleave File	avi divx xvid				Magic
Video	Adobe Flash Protected MPEG-4	f4p				None
Video	Adobe Flash MPEG-4	f4v				Heuristic
Video	Adobe Flash Video	flv				Magic
Video	MPEG-2 Video Stream	m2v mp2v mpg2 mpv2				None
Video	MPEG-4 Video Stream	m4v				Magic

Video	Matroska Video Stream	mkv				Heuristic
Video	Camcorder Video	mod tod dv				None
Video	QuickTime Video	mov qt movie				Magic
Video	MPEG-4 Video Stream	mp4				Magic
Video	MPEG-4 Video Stream	mp4v				None
Video	MPEG Video Stream	mpeg mpg mpe				Magic
Video	AVCHD Video Stream	mts avchd				Magic
Video	Ogg Vorbis Video File	ogv				Magic
Video	RealMedia Video Stream	rm				Heuristic
Video	DVD Video Movie	vob				None
Video	HEVC Video	hevc				Magic
Video	WebM Video Container	webm				Heuristic
Video	Adobe Flash	swf				Magic
Video	Actions Media Video	amv mtv				None
Video	Blu-ray BDAV Video File	m2ts bdav				None
Video	Dirac Video File	diarc				None
Video	H.264 Encoded Video File	h264				None
Video	H.265 Encoded Video File	h265				None
Video	Video Transport Stream	ts				None
Video	NUT Multimedia Container	nut				None
Video	Material Exchange Format	mxf				None
Video	Motion JPEG Format	mjpeg				None
Video	Windows Recorded TV show	wtv				None
Windows Registry	Current User Hive	dat	ntuser			Magic
Windows Registry	SAM Hive		SAM			Magic
Windows Registry	Security Hive		SECURITY			Magic
Windows Registry	Software Hive		SOFTWARE			Magic
Windows Registry	System Hive		SYSTEM			Magic

Default Keyword Search Parser

When searching for keywords in files that do not have a dedicated parser, a default parser is used that tries to locate ASCII and UTF-8 characters.

File Identification

File types are determined based on the file extension or by analyzing the file's header (this is called the thorough identification method because it is more accurate but also more time consuming).
When a file matches several file type definitions, only one is assigned based on the order defined in this list:

1. User created - sorted alphabetically
2. Default file type with specific parser in this order: document, picture, video, archive
3. All other default file types

Failover Capability

During the course of a scan some files with unexpected data structure can cause the parsers in charge of their processing to crash, forcing the application to terminate unexpectedly. To circumvent this situation, the ADF forensics tools include a crash management system that isolates the parsers most susceptible to crash so the running application is not affected. Currently, the documents, pictures, and video files parsers are isolated.

Additionally, isolating the parsers allows the application to monitor how long a file takes to be processed and detect if and when the processing has stopped. Each parser is allowed 5 minutes per 10MB of data to complete the processing of each file. If this timeout is reached or one hour has passed, the parser is terminated allowing the scan to proceed.
All files that are not successfully scanned are entered in the scan log.

Captures Execution Sequence

The ADF forensic tools are designed to find relevant data as quickly as possible while still performing a thorough scan of the target devices. This is accomplished by carefully sequencing the target drive areas and the types of files to process.
The scan follows this sequence:

1. Execute each artifact Capture
2. Process the files referenced by the artifact records collected previously against the file Captures
3. Scan the allocated files in the targeted folders on each partition
4. Scan allocated files in the other folders on each partition
5. Scan the allocated containers in the targeted folders on each partition
6. Scan allocated containers in the other folders on each partition
7. Scan deleted files
8. Carve pictures from allocated container files on each partition
9. Carve pictures from unallocated space for each Capture

To increase scan performance, Captures should search a narrow file set, and avoid overlaps between Captures or the same file could be processed multiple times.

Supported Apps

The table below lists all the artifacts that the Captures can collect from Operating Systems, smartphone apps, and computer applications. The versions listed are the ones that were tested but the Captures probably support older and newer versions as well.

App/OS	Platform	Capture
android	Android File System Limited	Application Usage
android	Android File System Limited	Device Information
android	Android File System Limited	OS Information
android	Android File System Limited	Installed Applications
android	Android File System Limited	Network Connection Activity
android	Android File System Limited	Bluetooth Devices
android	Android File System Limited	Application Permissions
android	Android File System Complete	Recent Files
android	Android File System Complete	Application Permissions
android	Android File System Complete	Saved Networks
android	Android File System Complete	Bluetooth Devices
androidcalls	Android File System Limited	Calls
androidcalls	Android File System Complete	Calls
androidmessages	Android File System Limited	Messages
androidmessages	Android File System Complete	Messages
app	platform	capture
applefiles	iOS File System Limited	Cloud Files
applefiles	iOS File System Complete	Cloud Files
applehealth	iOS File System Limited	Health Profiles
applehealth	iOS File System Limited	Health Metrics
applehealth	iOS File System Complete	Health Profiles
applehealth	iOS File System Complete	Health Metrics
applemessages	macOS File System	Messages
applemessages	iOS File System Limited	Messages
applemessages	iOS File System Complete	Messages
applenotes	iOS File System Limited	Notes
applenotifications	macOS File System	Notifications

applenotifications	iOS File System Complete	Notifications
ares	Windows File System	P2P Search Terms
ares	Windows File System	P2P Files Shared or Downloaded
bittorrent	Windows File System	P2P Files Shared or Downloaded
bittorrent	Windows Live	P2P Files Shared or Downloaded
bittorrent	macOS File System	P2P Files Shared or Downloaded
brave	Windows File System	Bookmarks
brave	Windows File System	Synced Tabs
brave	Windows File System	Top Sites
brave	Windows File System	Download History
brave	Windows File System	Form Data
brave	Windows File System	Session
brave	Windows File System	Browsing History
brave	Windows File System	Browser Cache
brave	Windows File System	Search Terms
brave	Windows File System	Browser Extensions
brave	macOS File System	Bookmarks
brave	macOS File System	Synced Tabs
brave	macOS File System	Top Sites
brave	macOS File System	Download History
brave	macOS File System	Form Data
brave	macOS File System	Session
brave	macOS File System	Browsing History
brave	macOS File System	Browser Cache
brave	macOS File System	Search Terms
brave	macOS File System	Browser Extensions
brave	iOS File System Limited	Bookmarks
brave	iOS File System Limited	Synced Tabs
brave	iOS File System Limited	Top Sites
brave	iOS File System Limited	Download History
brave	iOS File System Limited	Form Data
brave	iOS File System Limited	Browsing History
brave	iOS File System Limited	Session
brave	iOS File System Limited	Search Terms

brave	iOS File System Complete	Bookmarks
brave	iOS File System Complete	Synced Tabs
brave	iOS File System Complete	Top Sites
brave	iOS File System Complete	Download History
brave	iOS File System Complete	Form Data
brave	iOS File System Complete	Browsing History
brave	iOS File System Complete	Session
brave	iOS File System Complete	Search Terms
brave	Android File System Complete	Bookmarks
brave	Android File System Complete	Synced Tabs
brave	Android File System Complete	Top Sites
brave	Android File System Complete	Download History
brave	Android File System Complete	Form Data
brave	Android File System Complete	Session
brave	Android File System Complete	Browsing History
brave	Android File System Complete	Browser Cache
brave	Android File System Complete	Search Terms
chrome	Windows File System	Bookmarks
chrome	Windows File System	Synced Tabs
chrome	Windows File System	Top Sites
chrome	Windows File System	Download History
chrome	Windows File System	Form Data
chrome	Windows File System	Session
chrome	Windows File System	Browsing History
chrome	Windows File System	Browser Cache
chrome	Windows File System	Search Terms
chrome	Windows File System	Browser Extensions
chrome	macOS File System	Bookmarks
chrome	macOS File System	Synced Tabs
chrome	macOS File System	Top Sites
chrome	macOS File System	Download History
chrome	macOS File System	Form Data
chrome	macOS File System	Session
chrome	macOS File System	Browsing History

chrome	macOS File System	Browser Cache
chrome	macOS File System	Search Terms
chrome	macOS File System	Browser Extensions
chrome	macOS Live	Bookmarks
chrome	iOS File System Limited	Bookmarks
chrome	iOS File System Limited	Synced Tabs
chrome	iOS File System Limited	Top Sites
chrome	iOS File System Limited	Download History
chrome	iOS File System Limited	Form Data
chrome	iOS File System Limited	Browsing History
chrome	iOS File System Limited	Session
chrome	iOS File System Limited	Search Terms
chrome	iOS File System Complete	Bookmarks
chrome	iOS File System Complete	Synced Tabs
chrome	iOS File System Complete	Top Sites
chrome	iOS File System Complete	Download History
chrome	iOS File System Complete	Form Data
chrome	iOS File System Complete	Browsing History
chrome	iOS File System Complete	Session
chrome	iOS File System Complete	Search Terms
chrome	Android File System Complete	Bookmarks
chrome	Android File System Complete	Synced Tabs
chrome	Android File System Complete	Top Sites
chrome	Android File System Complete	Download History
chrome	Android File System Complete	Form Data
chrome	Android File System Complete	Session
chrome	Android File System Complete	Browsing History
chrome	Android File System Complete	Browser Cache
chrome	Android File System Complete	Search Terms
chromium	Windows File System	Bookmarks
chromium	Windows File System	Synced Tabs
chromium	Windows File System	Top Sites
chromium	Windows File System	Download History
chromium	Windows File System	Form Data

chromium	Windows File System	Session
chromium	Windows File System	Browsing History
chromium	Windows File System	Browser Cache
chromium	Windows File System	Search Terms
chromium	Windows File System	Browser Extensions
chromium	macOS File System	Bookmarks
chromium	macOS File System	Synced Tabs
chromium	macOS File System	Top Sites
chromium	macOS File System	Download History
chromium	macOS File System	Form Data
chromium	macOS File System	Session
chromium	macOS File System	Browsing History
chromium	macOS File System	Browser Cache
chromium	macOS File System	Search Terms
chromium	macOS File System	Browser Extensions
chromium	iOS File System Limited	Bookmarks
chromium	iOS File System Limited	Synced Tabs
chromium	iOS File System Limited	Top Sites
chromium	iOS File System Limited	Download History
chromium	iOS File System Limited	Form Data
chromium	iOS File System Limited	Browsing History
chromium	iOS File System Limited	Session
chromium	iOS File System Limited	Search Terms
chromium	iOS File System Complete	Bookmarks
chromium	iOS File System Complete	Synced Tabs
chromium	iOS File System Complete	Top Sites
chromium	iOS File System Complete	Download History
chromium	iOS File System Complete	Form Data
chromium	iOS File System Complete	Browsing History
chromium	iOS File System Complete	Session
chromium	iOS File System Complete	Search Terms
chromium	Android File System Complete	Bookmarks
chromium	Android File System Complete	Synced Tabs
chromium	Android File System Complete	Top Sites

chromium	Android File System Complete	Download History
chromium	Android File System Complete	Form Data
chromium	Android File System Complete	Session
chromium	Android File System Complete	Browsing History
chromium	Android File System Complete	Browser Cache
chromium	Android File System Complete	Search Terms
discord	iOS File System Limited	Messages
discord	iOS File System Complete	Messages
dropbox	iOS File System Limited	Cloud Files
dropbox	iOS File System Complete	Cloud Files
edge	Windows File System	Bookmarks
edge	Windows File System	Synced Tabs
edge	Windows File System	Top Sites
edge	Windows File System	Download History
edge	Windows File System	Form Data
edge	Windows File System	Session
edge	Windows File System	Browsing History
edge	Windows File System	Browser Cache
edge	Windows File System	Search Terms
edge	Windows File System	Browser Extensions
edge	macOS File System	Bookmarks
edge	macOS File System	Synced Tabs
edge	macOS File System	Top Sites
edge	macOS File System	Download History
edge	macOS File System	Form Data
edge	macOS File System	Session
edge	macOS File System	Browsing History
edge	macOS File System	Browser Cache
edge	macOS File System	Search Terms
edge	macOS File System	Browser Extensions
edge	iOS File System Limited	Bookmarks
edge	iOS File System Limited	Synced Tabs
edge	iOS File System Limited	Top Sites
edge	iOS File System Limited	Download History

edge	iOS File System Limited	Form Data
edge	iOS File System Limited	Browsing History
edge	iOS File System Limited	Session
edge	iOS File System Limited	Search Terms
edge	iOS File System Complete	Bookmarks
edge	iOS File System Complete	Synced Tabs
edge	iOS File System Complete	Top Sites
edge	iOS File System Complete	Download History
edge	iOS File System Complete	Form Data
edge	iOS File System Complete	Browsing History
edge	iOS File System Complete	Session
edge	iOS File System Complete	Search Terms
edge	Android File System Complete	Bookmarks
edge	Android File System Complete	Synced Tabs
edge	Android File System Complete	Top Sites
edge	Android File System Complete	Download History
edge	Android File System Complete	Form Data
edge	Android File System Complete	Session
edge	Android File System Complete	Browsing History
edge	Android File System Complete	Browser Cache
edge	Android File System Complete	Search Terms
facebook	Android File System Complete	Messages
facebook	Android File System Complete	Saved Contacts
facebook	iOS File System Limited	Messages
facebook	iOS File System Limited	Saved Contacts
facebook	iOS File System Complete	Messages
facebook	iOS File System Complete	Saved Contacts
facebook	Windows File System	Messages
facebook	Windows File System	Saved Contacts
facebook	macOS File System	Messages
facebook	macOS File System	Saved Contacts
firefox	Windows File System	Bookmarks

firefox	Windows File System	Synced Tabs
firefox	Windows File System	Download History
firefox	Windows File System	Form Data
firefox	Windows File System	Session
firefox	Windows File System	Browsing History
firefox	Windows File System	Browser Cache
firefox	Windows File System	Search Terms
firefox	Windows File System	Browser Extensions
firefox	macOS File System	Bookmarks
firefox	macOS File System	Synced Tabs
firefox	macOS File System	Download History
firefox	macOS File System	Form Data
firefox	macOS File System	Session
firefox	macOS File System	Browsing History
firefox	macOS File System	Browser Cache
firefox	macOS File System	Search Terms
firefox	macOS File System	Browser Extensions
firefox	Android File System Complete	Bookmarks
firefox	Android File System Complete	Synced Tabs
firefox	Android File System Complete	Download History
firefox	Android File System Complete	Form Data
firefox	Android File System Complete	Session
firefox	Android File System Complete	Browsing History
firefox	Android File System Complete	Browser Cache
firefox	Android File System Complete	Search Terms
firefox	Android File System Complete	Browser Extensions
firefox	iOS File System Limited	Search Terms
firefox	iOS File System Limited	Browsing History
firefox	iOS File System Limited	Bookmarks
firefox	iOS File System Complete	Form Data
firefox	iOS File System Complete	Search Terms
firefox	iOS File System Complete	Browsing History
firefox	iOS File System Complete	Bookmarks
googlecalendar	Android File System Limited	Calendar

googlecontacts	Android File System Limited	Saved Contacts
googlemessages	Android File System Complete	Messages
grindr	iOS File System Limited	Messages
grindr	iOS File System Limited	Saved Contacts
grindr	iOS File System Complete	Messages
grindr	iOS File System Complete	Saved Contacts
instagram	iOS File System Complete	Messages
instagram	iOS File System Complete	Saved Contacts
ios	iOS File System Complete	Reminders
ios	iOS File System Complete	Application Usage
ios	iOS File System Complete	Saved Networks
ios	iOS File System Complete	Searched Locations
ios	iOS File System Complete	Trip History
ios	iOS File System Complete	Location History
ios	iOS File System Complete	Installed Applications
ios	iOS File System Complete	WiFi Locations
ios	iOS File System Complete	Bluetooth Devices
ios	iOS File System Complete	Application Permissions
ios	iOS File System Complete	Network Usage
ios	iOS File System Complete	Saved Locations
ios	macOS File System	Reminders
ios	macOS File System	Application Usage
ios	macOS File System	Saved Networks
ios	macOS Live	Application Usage
ios	macOS Live	Saved Networks
ios	iOS File System Limited	Reminders
ios	iOS File System Limited	Saved Networks
ios	iOS File System Limited	Installed Applications
ios	iOS File System Limited	Bluetooth Devices
ios	iOS File System Limited	Network Usage

ios	iOS File System Limited	Voice Memos
ioscalendar	iOS File System Complete	Calendar
ioscalls	iOS File System Complete	Calls
ioscalls	iOS File System Limited	Calls
ioscalls	iOS File System Limited	Voicemail
ioscontacts	iOS File System Limited	Saved Contacts
kikmessenger	Android File System Complete	Messages
kikmessenger	Android File System Complete	Saved Contacts
line	iOS File System Limited	Messages
line	iOS File System Limited	Saved Contacts
line	iOS File System Complete	Messages
line	iOS File System Complete	Saved Contacts
macos	macOS File System	User Logins
macos	macOS File System	Calendar
macos	macOS File System	Recent Files
macos	macOS File System	Application Usage
macos	macOS File System	Reminders
macos	macOS File System	Saved Networks
macos	macOS File System	User Accounts
macos	macOS File System	OS Information
macos	macOS File System	Terminal History
macos	macOS File System	Installed Applications
macos	macOS File System	Network Interfaces
macos	macOS File System	Application Permissions
macos	iOS File System Complete	Reminders
macos	iOS File System Complete	Application Usage
macos	iOS File System Limited	Reminders
macoscontacts	macOS File System	Saved Contacts
macoscontacts	macOS Live	Saved Contacts
mega	Windows File System	Cloud Files
mega	Windows Live	Cloud Files

opera	Windows File System	Bookmarks
opera	Windows File System	Synced Tabs
opera	Windows File System	Top Sites
opera	Windows File System	Download History
opera	Windows File System	Form Data
opera	Windows File System	Session
opera	Windows File System	Browsing History
opera	Windows File System	Browser Cache
opera	Windows File System	Search Terms
opera	Windows File System	Browser Extensions
opera	macOS File System	Bookmarks
opera	macOS File System	Synced Tabs
opera	macOS File System	Top Sites
opera	macOS File System	Download History
opera	macOS File System	Form Data
opera	macOS File System	Session
opera	macOS File System	Browsing History
opera	macOS File System	Browser Cache
opera	macOS File System	Search Terms
opera	macOS File System	Browser Extensions
opera	iOS File System Limited	Bookmarks
opera	iOS File System Limited	Synced Tabs
opera	iOS File System Limited	Top Sites
opera	iOS File System Limited	Download History
opera	iOS File System Limited	Form Data
opera	iOS File System Limited	Browsing History
opera	iOS File System Limited	Session
opera	iOS File System Limited	Search Terms
opera	iOS File System Complete	Bookmarks
opera	iOS File System Complete	Synced Tabs
opera	iOS File System Complete	Top Sites
opera	iOS File System Complete	Download History
opera	iOS File System Complete	Form Data
opera	iOS File System Complete	Browsing History

opera	iOS File System Complete	Session
opera	iOS File System Complete	Search Terms
opera	Android File System Complete	Bookmarks
opera	Android File System Complete	Synced Tabs
opera	Android File System Complete	Top Sites
opera	Android File System Complete	Download History
opera	Android File System Complete	Form Data
opera	Android File System Complete	Session
opera	Android File System Complete	Browsing History
opera	Android File System Complete	Browser Cache
opera	Android File System Complete	Search Terms
safari	iOS File System Limited	Bookmarks
safari	iOS File System Limited	Synced Tabs
safari	iOS File System Limited	Top Sites
safari	iOS File System Limited	Download History
safari	iOS File System Limited	Browsing History
safari	iOS File System Limited	Session
safari	iOS File System Limited	Search Terms
safari	macOS File System	Search Terms
safari	macOS File System	Browser Cache
safari	macOS File System	Browsing History
safari	macOS File System	Bookmarks
safari	iOS File System Complete	Session
safari	iOS File System Complete	Browser Cache
safari	iOS File System Complete	Search Terms
signal	Android File System Complete	Messages
signal	Android File System Complete	Saved Contacts
signal	Windows File System	Messages
signal	Windows Live	Messages
signal	macOS File System	Messages
signal	macOS Live	Messages
signal	iOS File System Complete	Messages
signal	iOS File System Complete	Saved Contacts

snapchat	Android File System Complete	Messages
snapchat	Android File System Complete	Saved Contacts
snapchat	iOS File System Complete	Messages
snapchat	iOS File System Complete	Saved Contacts
tango	iOS File System Limited	Messages
tango	iOS File System Limited	Saved Contacts
tango	iOS File System Limited	Calls
tango	iOS File System Complete	Messages
tango	iOS File System Complete	Saved Contacts
tango	iOS File System Complete	Calls
telegram	macOS File System	Messages
telegram	macOS File System	Saved Contacts
telegram	macOS File System	Calls
torbrowser	Windows File System	Bookmarks
torbrowser	Windows File System	Synced Tabs
torbrowser	Windows File System	Download History
torbrowser	Windows File System	Form Data
torbrowser	Windows File System	Session
torbrowser	Windows File System	Browsing History
torbrowser	Windows File System	Browser Cache
torbrowser	Windows File System	Search Terms
torbrowser	macOS File System	Bookmarks
torbrowser	macOS File System	Synced Tabs
torbrowser	macOS File System	Download History
torbrowser	macOS File System	Form Data
torbrowser	macOS File System	Session
torbrowser	macOS File System	Browsing History
torbrowser	macOS File System	Browser Cache
torbrowser	macOS File System	Search Terms
torbrowser	Android File System Complete	Bookmarks
torbrowser	Android File System Complete	Synced Tabs
torbrowser	Android File System Complete	Download History

torbrowser	Android File System Complete	Form Data
torbrowser	Android File System Complete	Session
torbrowser	Android File System Complete	Browsing History
torbrowser	Android File System Complete	Browser Cache
torbrowser	Android File System Complete	Search Terms
utorrent	Windows File System	P2P Files Shared or Downloaded
utorrent	macOS File System	P2P Files Shared or Downloaded
viber	iOS File System Limited	Messages
viber	iOS File System Limited	Saved Contacts
viber	iOS File System Complete	Messages
viber	iOS File System Complete	Saved Contacts
vkontakte	Windows File System	Saved Contacts
vkontakte	macOS File System	Saved Contacts
waze	iOS File System Complete	Searched Locations
waze	iOS File System Limited	Searched Locations
waze	Android File System Complete	Searched Locations
whatsapp	Android File System Complete	Messages
whatsapp	Android File System Complete	Saved Contacts
whatsapp	iOS File System Limited	Messages
whatsapp	iOS File System Limited	Saved Contacts
whatsapp	iOS File System Complete	Messages
whatsapp	iOS File System Complete	Saved Contacts
windows	Windows File System	Recent Files
windows	Windows File System	Saved Networks
windows	Windows File System	OS Information
windows	Windows File System	Terminal History
windows	Windows File System	Installed Applications
windows	Windows File System	Network Interfaces
windows	Windows File System	Bluetooth Devices
windows	Windows File System	Notifications

windows	Windows File System	Application Permissions
windows	Windows File System	Clipboard History
windows	Windows Live	Encrypted Drive

Scan Limitations

Some limitations are in place to prevent the application from running out of resources during the scan. When a limit is reached, a message is added to the scan log.

- When using the "thorough" file type identification method, documents that are bigger than 100MB will be detected as zip files if these documents are zip based.
- Files that take longer than the timeout defined in each Search Profile to process will be skipped. The timeout does not apply to containers.
- When collecting files that are either protected or are corrupted and could not be scanned, only files smaller than 2GB are collected.
- When processing a document, only the first 1000 embedded objects are processed (embedded objects can be pictures, but also metadata blocks).
- Scanning a running 32-bit Windows computer is no longer supported. Here are some workarounds.

Known Issues

Topic	Issue
Collection Key Preparation	When using a BitLocker locked Collection Key, the application cannot detect scan results that have not been backed up. Make sure to unlock your Collection Key before preparing it again!
Collection Key Preparation	It is not possible to prepare a Collection Key if the system volume of your computer is compressed. This is due to the fact that VHD images cannot be created on compressed volumes. The only workaround is to remove the compression setting for that volume.
Collection Key Preparation	Software write blockers can prevent the preparation of the Collection Key and should be disabled prior to creating a key.
Collection Key Preparation	Anti-virus can prevent the preparation of the Collection Key and should be disabled prior to creating a key.
Collection Key Preparation	If you installed Windows ADK version 1703 and are using Secure Boot, it needs to be disabled the first time you prepare a Collection Key.
Boot Scan	If the BIOS does not offer the option to reboot from a USB flash drive, we recommend creating a bootable CD with the Plop Boot Manager. See the Knowledge Base article.

RAM Dump	The RAM dump process will not work on old computers that have not been updated in a long time and in particular if patch KB3033929 is missing. Please contact support@adfsolutions.com for a workaround if needed.
Bitlocker protected target	When unlocking a BitLocker partition, if the passphrase fails, try using the Recovery Key.
Network drive access	If a mounted network drive is not visible in the ADF application, it is because the application is executed in an elevated context but the network drive was not mounted in the same context. Make sure the network drives you try to access are mapped in an elevated context as well. See this page for details.
Video playback	Videos may not be able to play if the codecs are missing. If the error message “The media cannot be played due to a problem allocating resources.” is displayed in the Preview tab of the Details pane, try installing codecs from this link.
Viewer thumbnail size	On 4K monitors we recommend setting the thumbnail size to 128 pixels or higher.
Target drives with native 4K sector and MBR	Partitions are not properly detected on these drives and they should not be scanned. A fix will be released in version DEI 2.1 and TINV/TG2 5.1.
macOS	In some instances, the Apple Operating System installation date may be incorrect.
macOS Sonoma Recovery Mode not seeing the Collection Key	In Recovery Mode, the Collection Key which is formatted with ExFAT and contains the Mac agent is no longer mounted. To avoid this issue, you can copy the agent to a FAT flash drive. After preparing a Collection Key, copy the startMacOSAgent and the Mac folder to the flash drive.
APFS	Carving pictures from unallocated space is not yet supported on APFS.
APFS	Timezone is not identified from APFS partitions (UTC is used by default in this case).
Crash at startup	If the Desktop application crashes immediately after starting, it is possible that some cached files got corrupted. In this case, simply delete the files in: \Users\<NAME>\AppData\Local\cache\qtshadercache.
Multivolume archives	Multivolume archives are currently not supported.
Application Usage Capture	When running on Windows 7, if you are scanning a Windows 10 image, some records will be missing. It is best to use a Windows 10 computer to install the ADF application.
Touch screen	To avoid having the touch keyboard appear when a new screen is displayed make sure you are not in Windows Tablet mode and make sure this setting is off: Settings > Devices > Typing > Show the touch keyboard when not in tablet mode and there’s no keyboard attached
iOS device phone number	Make sure you have the latest version of iTunes (see download instructions) or the phone number of the device may not be collected by the Device Information Capture.
Unreadable error	Some error messages in the Desktop application may be unreadable when Windows is

messages in the Desktop application	using a different language than English. To solve this issue, open the Windows Settings and search for "region settings". Click on the "Administrative language settings" > "Change system locale…" and check the "Beta: Use Unicode UTF-8 for worldwide language support" checkbox.

Open-Source Libraries

The ADF applications use the open source libraries listed in the table below.

Name	Version	Source URL	License
7z	16.04 (2016/10/04)	Project Page	LGPL + UnRAR restrictions
airplay2-win		Github project page	MIT license
better-enums	0.11.1	Project Page	BSD
boost	1.64	Project Page Used Source Link (with Windows-style EOL's)	Boost Software License
FFmpeg	6.1.1#11	Project Page	LGPL 2.1
FreeImage	3.17.0 (2015/03/15)	Project Page Used Source Link	FreeImage Public License
gmock and gtest	1.7.0(both gmock and gtest)	Project Page	BSD 3-Clause
grpc	v1.60.0#1		Apache License 2.0
gsl	v2.8#0	Project Page	MIT license
icu	icu4c-59	Project Page	License
libaeskeywrap		Project Page	MIT License
libbde	2017/02/04	Project page	LGPLv3
libbfio	2014/10/15	Project Page	LGPLv3
libde265	1.0.15	Project Page	LGPLv3
libesedb	2015/12/13	Project Page	LGPLv3
libevtx	2016/01/07	Project Page	LGPLv3
libewf	2014/06/08	Project Page	LGPLv3

libfvde	2019/12/21	Project Page	LGPLv3
libheif	v1.17.6#2	Project Page	LGPLv3
libimobiledevice	1.1.6	Git-master with latest commit	LGPL v2.1
liblnk	2016/01/07	Project Page	LGPLv3
libmsiecf		Project Page	LGPLv3
libolecf	2016/01/07	Project Page	LGPLv3
libphonennumber	r666	Project Page	Apache license 2.0
libplist	2.0.0	Project Page	LGPLv2.1
libregf	2015/07/04	Project Page	LGPLv3
libssh2	1.8.0	Project page	
libusbmuxd	2019/01/18	Project page	LGPLv2.1
libvhdi	alpha-20170223	Project Page	LGPLv3
libvmdk	alpha-20170226	Project Page	LGPLv3
libxml2	2.9.4	Project Page	MIT License
mapbox_jni	4.0.0	Project Page	
minizip	2017/07/26	Project Page	Free to use
minizip-ng	v4.0.7#0	Project Page	zlib license
nlohmann_json	3.1.2	Project Page	MIT License
OpenImageIO	3.0.1.0#0	Project Page	License
openssl	1.1.1n#1 and v3.3.2#0	Project Page	OpenSSL License
plop	07/Feb/2012	Project Page	License
prefetch	01/Dec/2018	Project Page	Apache license 2.0
protobuf	v4.25.1#1	Project Page	Protobuf License
Qt	5.15.14	Project Page	LGPLv3
RapidJSON	1.0.2	http://rapidjson.org/	MIT License
RE2	v2024-07-02#0	Google RE2	RE2 License

Realm Core	5.23.5	Project Page	Apache License 2.0
sleuthkit	4.5.0	Project Page	CPL-1.0
SQLite	3.29.0	Project Page	Public Domain
tensorflow	1.6.0	Project Page	Apache license 2.0
Tesseract	4.0.0	Project Page	Apache License 2.0
uriparser	0.8.2	Project Page	New BSD License
winpmem	1.3	Project page	Apache license 2.0
wkHtmlToPdf	0.12.5	Project page	LGPLv3
zlib	1.2.11	Project Page	zlib license

RAID Support

The ADF tools support a wide variety of RAID controllers and configurations. To find out which ones are supported go to http://sysdev.microsoft.com/en-US/Hardware/LPL/DEFAULT.ASPX and enter the following in the form:

- Select a group: Device
- Select an OS: Windows 10 Client
- Select a product type: Adapters & Controllers
- Select a feature or AQ: Device.Storage.Controller.Raid

Then press the Search button.

In addition to the controllers supported by default by Windows 10, the ADF tools support the following controllers:

Adaptec SCSI Card 39160 - Ultra160 SCSI (Generic)
Adaptec AIC-7899 Ultra160 PCI SCSI Card
Adaptec AIC-7892 Ultra160 PCI SCSI Card
Adaptec SCSI Card 29160 - Ultra160 SCSI (Generic)
Adaptec SCSI Card 19160 - Ultra160 SCSI (Generic)
Adaptec SCSI Card 39160 - Ultra160 SCSI
Compaq 64-bit/66MHz Dual Channel Wide Ultra3 SCSI Adapter
Adaptec SCSI Card 29160 - Ultra160 SCSI
Compaq 64-bit/66MHz Wide Ultra3 SCSI Adapter
Adaptec SCSI Card 29160N - Ultra160 SCSI
Adaptec SCSI Card 29160LP - Ultra160 SCSI
Adaptec SCSI Card 19160 - Ultra160 SCSI
Adaptec 2915/2930LP PCI SCSI Controller
Adaptec AIC-7892 - Ultra160 SCSI
Asmedia 106x SATA Controller
RocketRAID 172x SATA Controller
HighPoint RCM Device
RocketRAID 174x SATA Controller
RocketRAID 231x SATA Controller
RocketRAID 230x SATA Controller
RocketRAID 2210 SATA Controller
RocketRAID 2782 SAS Controller
RocketRAID 620 SATA Controller
RocketRAID 622 SATA Controller
Intel(R) 8 Series/C220 Chipset Family SATA AHCI Controller
Intel(R) 8 Series Chipset Family SATA AHCI Controller
Intel(R) 9 Series Chipset Family SATA AHCI Controller
Intel(R) 6th Generation Core Processor Family Platform I/O SATA AHCI Controller
Intel(R) 100 Series/C230 Chipset Family SATA AHCI Controller
Intel Chipset SATA RAID Controller
JMB36X Standard Dual Channel PCIE IDE Controller
JMicron JMB36X Controller
JMicron JMB37X Controller
JMicron JMB368 Controller
JMicron JMB36X RAID Processor
LSI Embedded MegaRAID
LSI MegaRAID SAS 1064E
LSI MegaRAID SAS 8208XLP and 8204XLP
LSI MegaRAID SATA 300S-XLP
LSI MegaRAID SAS 8208ELP and 8204ELP
LSI Logic MegaRAID SATA 350-4ELP RAID Controller
LSI Logic MegaRAID SAS 8704ELP RAID Controller
LSI Logic MegaRAID SAS 8708EM2 RAID Controller
LSI Logic MegaRAID SAS 8808EM2 RAID Controller
LSI Logic MegaRAID SAS 8780EM2 RAID Controller
LSI Logic MegaRAID SAS 8880EM2 RAID Controller
LSI Logic MegaRAID SAS 8744EM2 RAID Controller
LSI Logic MegaRAID SAS 8844EM2 RAID Controller
LSI Logic MegaRAID SAS 8744ELP RAID Controller
LSI Logic MegaRAID SAS 8844ELP RAID Controller
LSI Logic MegaRAID SAS 8008EM2 RAID Controller
Intel(R) RAID Controller SRCSAS18E
Intel(R) RAID Controller SRCSAS144E
Intel(R) RAID Controller SROMBSAS18E
Intel(R) RAID Controller SRCSASRB
Intel(R) RAID Controller SRCSASJV
Intel(R) RAID Controller SRCSATAWB
Intel(R) RAID Controller SRCSASPH16I
Intel(R) RAID Controller SRCSASBB8I
Intel(R) RAID Controller SRCSASLS4I
Integrated Intel(R) RAID Controller SROMBSASFC
LSI Logic MegaRAID SAS PCI Express ROMB

RocketRAID 2320 SATA Controller
RocketRAID 2322 SATA Controller
RocketRAID 2340 SATA Controller
RocketRAID 2522 SATA Controller
RocketRAID 3220 SATA Controller
RocketRAID 3320 SATA Controller
RocketRAID 3520 SATA Controller
RocketRAID 4320 SAS Controller
RocketRAID 3510 SATA Controller
RocketRAID 3511 SATA Controller
RocketRAID 3521 SATA Controller
RocketRAID 3522 SATA Controller
RocketRAID 3410 SATA Controller
RocketRAID 3540 SATA Controller
RocketRAID 3530 SATA Controller
RocketRAID 3560 SATA Controller
RocketRAID 4322 SAS Controller
RocketRAID 4321 SAS Controller
RocketRAID 4210 SAS Controller
RocketRAID 4211 SAS Controller
RocketRAID 4310 SAS Controller
RocketRAID 4311 SAS Controller
RocketRAID 44xx Series SAS Controller
RocketRAID 182x/181x SATA Controller
RocketRAID 222x SATA Controller
RocketRAID 2710 SAS Controller
RocketRAID 2711 SAS Controller
RocketRAID 2720 SAS Controller
RocketRAID 2721 SAS Controller
RocketRAID 2722 SAS Controller
RocketRAID 2730 SAS Controller
RocketRAID 2740 SAS Controller
RocketRAID 2744 SAS Controller
RocketRAID 2760 SAS Controller

LSI MegaRAID SATA 300S-ELP
Intel Embedded Server RAID Technology II
LSI MegaRAID Software RAID
ServeRAID C105
LSI Logic MegaRAID SAS 8408E RAID Controller
LSI Logic MegaRAID SAS 8480E RAID Controller
LSI Logic MegaRAID SAS 8344ELP RAID Controller
LSI Logic MegaRAID SAS 8308ELP RAID Controller
LSI Logic MegaRAID SATA 300-4ELP RAID Controller
LSI Logic MegaRAID SATA 300-12E RAID Controller
LSI Logic MegaRAID SATA 300-16E RAID Controller
LSI Logic MegaRAID SAS 84016E RAID Controller
LSI Logic MegaRAID SATA 300-8ELP RAID Controller
LSI Logic MegaRAID SAS 8300XLP RAID Controller
LSI Logic MegaRAID SAS 8888ELP RAID Controller
LSI Logic MegaRAID SAS 8708ELP RAID Controller
LSI Logic MegaRAID SAS 8884E RAID Controller
LSI Logic MegaRAID SAS 8708E RAID Controller
LSI Logic MegaRAID SATA 350-8ELP RAID Controller

RAID 5/6 SAS based on LSI MegaRAID
IBM ServeRAID-MR10i SAS/SATA Controller
IBM ServeRAID-MR10il SAS/SATA Controller
IBM ServeRAID-MR10M SAS/SATA Controller
IBM ServeRAID-MR10k SAS/SATA Controller
IBM ServeRAID-MR10is SAS/SATA Controller
IBM ServeRAID-MR10ie SAS/SATA Controller
Intel(R) RAID Controller SROMBSASMP2
Intel(R) RAID Controller SROMBSASBN
LSI MegaRAID SAS 8704EM2 RAID Controller
Intel(R) RAID Controller SROMBSASMR
IBM SystemX MegaRAID SAS 8884E RAID Controller
Marvell 91xx Config Device
Marvell Unify Configuration
Silicon Image SiI 3124 SoftRaid 5 Controller