Introduction

This guide defines common terms used in the ADF applications.

This document applies to the following applications		
ADFPRO Mobile & Computer Triage	DEI Digital Evidence Investigator	MDI Mobile Device Investigator

Terms

Term	Meaning
Acquisition	The data collected from a device or source and saved by the ADF application in a folder of its own: a mobile device backup or preview, a file collection (Collect Files), screen recordings and screenshots, a data container created through a remote agent, or a drive image. Acquisitions saved in the Acquisitions folder set in Settings, or in a folder chosen on the View Acquisitions screen, are listed on that screen, where they can be reviewed and, if the product and license allow it, scanned.
ADF Data Container	The format in which the ADF application saves an acquisition: a folder with the collected data (for example files.zip, adb_backup.zip or the segments of a drive image) and metadata.zip, which describes the acquisition, the data source and the container. See the ADF Data Container Structure guide.
AirPlay	AirPlay is a proprietary wireless communication protocol developed by Apple Inc. that allows screen mirroring between an Apple device and a display or streaming server (in this case the ADF desktop application).
Artifact	A digital record created by a computer process.
Artifact Capture	An automated process that collects and analyzes artifacts on the target device.
Authentication Key	A USB device that contains a license file or an offline token for the ADF application. The license file is issued by ADF for that device. The token is borrowed from the Token Server with Initialize Authentication Keys with License Tokens and is valid until the end of the current day (a later day, at most 10 days counting today, only if the configuration allows it); only USB devices smaller than 16 GB can be initialized this way.
BIOS	BIOS (basic input/output system) is the program a personal computer's microprocessor uses to get the computer system started after it is powered on.

Copyright ©2016-2026 ADF Solutions, Inc. All rights reserved. U.S. Pat. No. 8,219,588 and 7,941,386. ADF PRO, Digital Evidence Investigator and Mobile Device Investigator are trademarks or registered trademarks of ADF Solutions, Inc. All other trademarks referenced herein are the property of their respective owners.

Boot Scan	A scan of a dead computer starts from a Collection Key: the computer boots the Windows environment on the key instead of its own operating system, and the ADF application on the key scans its drives. In the scan summary, Scan Type is Boot.
CAID	The Child Abuse Image Database (CAID) is a collection of data and technologies to help fight Child Sexual Exploitation and Abuse. The UK Home Office developed CAID in collaboration with the police, industry partners and British and international Small and Medium Sized Enterprises. CAID uses the VICS format.
Carving	Recovering data that has been deleted and no longer referenced by the file system. This is done by searching for file signatures within unallocated space. The ADF application carves pictures (JPEG, PNG, GIF, BMP, TIFF, PSD and WebP) from unallocated space and from the Windows hibernation, page and swap files.
Case Number	An optional identifier of the case, entered when an acquisition is created (Enter Information) or when a scan is set up (Scan Information). The View Acquisitions and Review Scan Results screens group acquisitions and scan results by case number. When every target selected for a scan has the same case number, Scan Information fills it in, unless a case number has already been typed there.
Collection Key	A 16 GB or more USB storage device (as the ADF application counts it: 16 × 1,073,741,824 bytes, so a drive sold as 16 GB is too small) prepared by the ADF desktop application (not available in Mobile Device Investigator) to contain: ● A bootable Windows environment (WinPE) to conduct boot scans: of x64 and ARM64 computers when the key uses the GPT partition scheme, of x64 computers only with MBR. ● The ADF application to conduct live scans of Windows computers. ● The Windows and macOS remote agents, which let the ADF application on another computer scan or image the target computer over the network. ● The selected Search Profiles, the whitelists they use, and the forms. ● It may also contain a license file for that device.
Dead computer	A computer that is powered off.
Drive Image	An E01 or DD image of a drive created with the Image function of the ADF application. Since version 6.4.0 the image is saved with its metadata as an acquisition: if it is saved in the folder shown on the View Acquisitions screen, it is listed there with the acquisition type Drive image (E01) or Drive image (DD) and can be scanned from there (in Mobile Device Investigator, only E01 images, with the External Devices add-on).
Encryption	Data encryption translates data into another form, or code, so that only people with access to a secret key or password can read it.
Entity Extraction (Rosoka Add-on)	This add-on, developed by Rosoka, identifies entities (people, locations, time events, etc.) in text documents in 200+ languages and is capable of normalizing and translating them back into English. In the ADF application it is called Entity Extraction: it requires an add-on license, runs after the scan on the desktop only (automatically when the Search Profile

Copyright ©2016-2026 ADF Solutions, Inc. All rights reserved. U.S. Pat. No. 8,219,588 and 7,941,386. ADF PRO, Digital Evidence Investigator and Mobile Device Investigator are trademarks or registered trademarks of ADF Solutions, Inc. All other trademarks referenced herein are the property of their respective owners.

	option Automatically start Entity extraction when scan finishes is selected), and shows its results on the Entities tab of the Details pane.
Evidence Image File	A forensic image is a container that is used to store a digitally identical copy of the target media.
File Capture	An automated process that searches files by their properties, keywords or hash values (MD5 or SHA1) and can collect the matching files, or compares the pictures found by the other captures of the scan with a provided set of pictures for visual similarity (PhotoDNA).
File Extension	A file extension is typically 3 characters after the full stop in a file name. The extension identifies the file type.
File Header	Generally a short sequence of bytes placed at the beginning of the file used to identify the format of the file.
File identification method - Fast identification	Identifies file types by the file name, normally its extension, without analyzing the file content.
File identification method - Thorough identification for files without extensions	Uses file signature analysis to identify files that have no file extension and fast identification on those that do.
File identification method - Thorough identification for all files	Uses file signature analysis to identify all files; a file whose content matches no known signature is identified by its extension. This will increase the time the scan takes to run.
File Sources - Entire File System	All allocated files.
File Sources - Targeted folders	Specific folders specified by the user. Targeted folders are searched before other folders and are not searched again if both Targeted folders and Entire file system are selected.
File Sources - Files referenced by artifact records	Fourteen artifact captures, Browser Cache, Calendar, Cloud Files, Cloud Storage Files, Download History, Emails, Messages, Notes, Notifications, P2P Files Shared or Downloaded, Recent Files, Reminders, Voicemail and Voice Memos, may refer to files that may exist on the scanned system. If these files are located or extracted, they can be targeted as a file source; the artifact captures must be in the same Search Profile. This option is needed to target email or message attachments and files embedded within browser cache containers.
File Sources - Deleted files	Deleted files whose records can still be found in the file system, for example in the NTFS Master File Table or in directory entries.
File Sources - Carve pictures from Unallocated space	This searches unallocated space for the signatures of JPEG, PNG, GIF, BMP, TIFF, PSD and WebP pictures. The pictures found that match the file types and filters of the capture are added to its results, and collected when Collect matching files is selected.

Copyright ©2016-2026 ADF Solutions, Inc. All rights reserved. U.S. Pat. No. 8,219,588 and 7,941,386. ADF PRO, Digital Evidence Investigator and Mobile Device Investigator are trademarks or registered trademarks of ADF Solutions, Inc. All other trademarks referenced herein are the property of their respective owners.

File Sources - Carve pictures in	Carves pictures in the same way from the selected Windows system cache files: the hibernation file (hiberfil.sys), the page file (pagefile.sys) and the swap file (swapfile.sys).
File System	A File System is used to control how data is stored on and retrieved from digital storage devices.
Firmware	Firmware is a software program or set of instructions programmed onto a hardware device. It provides the necessary instructions for how the device communicates with the other computer hardware.
Gigabyte (GB)	A gigabyte (also referred to as GB) is a unit of data equal to 1,073,741,824 bytes (1,024 MB). The ADF application uses this value for every size it shows. Drive manufacturers count 1 GB as 1,000,000,000 bytes, so a drive sold as 16 GB is shown as 14.9 GB at most.
Hash Hash Value Hashing	A hash value is a numeric value of a fixed length that uniquely identifies data. Hash values are useful to prove that computer data has not changed or to quickly identify certain known files.
HTML	Hyper Text Markup Language (HTML) is the standard markup language for creating web pages and web applications.
Jailbreaking	Jailbreaking is the process of allowing users of iOS devices to attain privileged control over various iOS subsystems. In digital forensics jailbreaking is mostly used to gain access to the entire file system.
JSON	JavaScript Object Notation (JSON) is a lightweight data-interchange format. It is easy for humans to read and write. It is easy for machines to parse and generate. VICS uses the JSON notation.
Kilobyte (KB)	A Kilobyte (KB) is a unit of data equal to 1,024 bytes.
Live computer	A computer that is currently powered on and running on its default Operating System.
Live Scan	A scan of a live computer by the ADF application started from a Collection Key (startWindowsLiveScanner.bat), without restarting the computer. In the scan summary, Scan Type is Live.
Logical Drive	A logical drive is a drive space that is created on top of a physical hard disk drive. A logical drive is a separate partition with its own parameters and functions, and it operates independently. A logical drive can also be called a logical drive partition or logical disk partition.
Megabyte (MB)	A Megabyte (MB) is a unit of data equal to 1,048,576 bytes.
Node	A computer or an Authentication Key registered with the Token Server. Each time the ADF application starts with a Token Server configured, it registers the computer before it borrows a license token, and each Authentication Key initialized with a license token is registered as a node of its own. The Web Platform license defines how many nodes are available in the system.

Copyright ©2016-2026 ADF Solutions, Inc. All rights reserved. U.S. Pat. No. 8,219,588 and 7,941,386. ADF PRO, Digital Evidence Investigator and Mobile Device Investigator are trademarks or registered trademarks of ADF Solutions, Inc. All other trademarks referenced herein are the property of their respective owners.

Partition	A partition is a section of a hard disk that is treated as a separate unit by operating systems and file systems.
PhotoDNA	PhotoDNA is a technology developed by Microsoft and improved by Hany Farid, professor at Dartmouth College, that computes hash values of pictures to identify similar pictures. The ADF application computes the PhotoDNA hash values of the pictures that other captures collect during a scan and compares them with a provided set. The PhotoDNA Distance shows how similar two pictures are: 0 is an exact match, and only matches up to the PhotoDNA Maximum Distance (at most 205) are kept.
Physical Disk	A physical disk is a data storage device, such as a hard disk drive or a solid state drive, as opposed to the partitions, logical drives and volumes created on it.
Pixel	The pixel (a word invented from "picture element") is the basic unit of programmable color on a computer display or in a computer image file.
Regular Expression (Regex)	Regular expressions enable users to create complex search terms following the Regular Expression search pattern language. In a keyword capture, each search expression can also be given an Auto-Tag and an Auto-Comment that are applied to its matches. See the Working with Regular Expressions (Regex) guide.
Remote Agent	A program on the Collection Key, started on a Windows computer with startWindowsAgent.bat or on a Mac with startMacOSAgent, that lets the ADF application on another computer of the same network scan or image that computer (Add Remote Agent on the Scan screen, Remote Agent on the Image screen). The agent must come from a Collection Key prepared with the same version of the ADF application; an agent of another version shows “Remote agent is outdated, create a new Collection Key.”
Rooting	Rooting is the process of allowing users of Android devices to attain privileged control over various Android subsystems. In digital forensics rooting is mostly used to gain access to the entire file system.
Scan Options - Collect protected files	Files that a capture could not fully read because they are password protected (for example protected archives and documents) or encrypted by the file system. With this option, copies of such files smaller than 2 GB are added to the scan results; files encrypted by the file system are copied only if they could be read. The Scan Log lists protected files in any case.
Scan Options - Collect files that crashed the parsers	Files during whose processing the parser process crashed. With this option, copies of such files smaller than 2 GB are added to the scan results. Files that could not be parsed for other reasons are not collected; files skipped because their processing took too long are covered by Collect skipped files.
Scan Options - Collect skipped files	Files whose processing was stopped because it took too long: 5 minutes for every full 10 MB of the file (at least 5 minutes), but no longer than the time set in Skip files processed for more than (10 seconds to 120 minutes). With this option, copies of such files smaller than 2 GB are added to the scan results.

Copyright ©2016-2026 ADF Solutions, Inc. All rights reserved. U.S. Pat. No. 8,219,588 and 7,941,386. ADF PRO, Digital Evidence Investigator and Mobile Device Investigator are trademarks or registered trademarks of ADF Solutions, Inc. All other trademarks referenced herein are the property of their respective owners.

Search Profile	A compilation of Artifact Captures and File Captures, together with the profile options (Scan Information Fields, Scan Options and Whitelists), used to scan a target device.
Solid State Drive (SSD)	A data storage device containing non-volatile flash memory, used in place of a hard disk drive for its much greater speed.
Standalone Viewer	A tool of ADF PRO, Digital Evidence Investigator and Mobile Device Investigator that enables the export of Scan Results for review and analysis on another computer without requiring a license: Create Report with the Standalone viewer option. The exported viewer is started with ADF Viewer.bat.
Substring	A string of characters or symbols that is part of a longer string of characters or symbols.
Token	The Token Server app is designed to lend license tokens to the ADF desktop applications requesting them. The application keeps one token while running, and the token is returned when the application is closed. License tokens can also be used to initialize Authentication Keys, valid until the end of the current day (or of a later day, at most 10 days counting today, if the configuration allows it), to be used offline and on-scene. Collection Keys cannot hold a token. The Cloud Platform license defines how many tokens are available in the system.
UEFI (Unified Extensible Firmware Interface)	Unified Extensible Firmware Interface (UEFI) is a specification that defines a more modernized model for the interface between computer operating systems and platform firmware during the boot, or start-up, process.
Unallocated	Unallocated clusters (also referred to as unallocated space or free space) are the available drive storage space that is not allocated to file storage by a volume. Unallocated clusters can be a valuable source of evidence in a computer forensics examination because they can contain deleted files or remnants of deleted files created by the Operating System and / or computer users.
USB (Universal Serial Bus)	A hardware interface for attaching peripherals to a computer.
VICS	The Project VIC data model, known as VICS (Video Image Classification Standard), has become a standardized model for exchanging information between tools and services specializing in the fight against child abuse. The ADF application imports VICS files into hash sets, PhotoDNA sets and whitelists, and exports scan results in the VICS 1.3 or 2.0 format.
Volume	A volume or logical drive is a single accessible storage area with a single file system, typically (though not necessarily) resident on a single partition of a hard disk.

Copyright ©2016-2026 ADF Solutions, Inc. All rights reserved. U.S. Pat. No. 8,219,588 and 7,941,386. ADF PRO, Digital Evidence Investigator and Mobile Device Investigator are trademarks or registered trademarks of ADF Solutions, Inc. All other trademarks referenced herein are the property of their respective owners.