Glossary

Introduction

This guide defines common terms used in the ADF applications.

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

Terms

Term	Meaning
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.
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.
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.
Collection Key	A 16 GB or more USB storage device prepared by the ADF desktop application to contain: ● A bootable Windows Operating System to conduct boot scans. ● The Windows Scanner to conduct live scans. ● The Mac agent to conduct live macOS scans via the agent. ● It may also contain a license file or an offline token.
Dead computer	A computer that is powered off.

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.
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 collects files based on file properties and or keywords and or hash values.
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 using the file extension only.
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 file identification for all files	Uses file signature analysis to identify all files. 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	Six artifact captures, P2P Files Shared or Downloaded, Emails, Messages, Recent Files, Download History and Browser Cache may refer to files that may exist on the scanned system. If these files are located or extracted we can target them as a file source. This option is needed to target email or message attachments and files embedded within browser cache containers.
File Sources - Deleted files	Deleted files for which references can still be found in the file system directory index.
File Sources - Carve pictures from Unallocated space	This searches unallocated space and collects any picture files where the file header is found in an unallocated sector.
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 1,000,000,000 bytes of data.
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 rooting 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.
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	The Token Server app identifies a node as a computer workstation that has borrowed a license token at least once. The Web Platform license defines how many nodes are available in the system.
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 images, video and audio files to identify similar images.
Physical Disk	A physical disk (also known as hard disk drive) is a data storage device used for storing and retrieving digital information using one or more rigid rapidly rotating disks (platters) coated with magnetic material.
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 and specify what to do when each pattern match is found.
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.
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.
Scan Options - Protected file	A password protected file.
Scan Options - files that crashed the parsers	A file that cannot be read properly by a capture.
Search Profile	A compilation of Artifact Captures and File Captures 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	Digital Evidence Investigator’s tool that enables the export of Scan Results for review and analysis on another computer without requiring a license.
Substring	A string of characters or symbols that is part of a longer string or 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 to be used offline and on-scene. 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, and has become a standardized model for exchanging information from tools and services specializing in this fight against child abuse.
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.