DEI TINV TG2 Technical Specifications

1. Minimum System Requirements

ADF forensics tools are designed to run on the following computers:

Operating System	Minimum System Requirements
Windows 7 64-bit[1] with SP1 and Convenience Rollup (April 2016)	2GB of RAM, 20 GB of free hard drive space
Windows 8.1 64-bit[1]	4GB of RAM, 20 GB of free hard drive space
Windows 10 64-bit	4GB of RAM, 20 GB of free hard drive space

Note [1]: Cannot prepare BitLocker encrypted Collection Keys.

IMPORTANT: The user of the application must have admin privilege to scan targets and prepare Collection Keys.

To make the Collection Key bootable and install WinPE, the ADF tools require the Windows Assessment and Deployment Kit (Windows ADK). We recommend using version 1709 as it is the most stable (please avoid version 1809 for now).

The following devices can be used as Collection Keys:

- Collection Key provided by ADF
- External hard drive with 512 byte sector size
- External hard drive with 4096 byte sector size with logical 512 byte emulation

We do not support external hard drive with 4096 byte native sector size at this time.

2. Supported Target Devices/Operating Systems

ADF forensics tools are designed to scan the following systems:

- Powered-off target computer (boot scan)
  - Firmware: BIOS, UEFI, Secure UEFI, Mac EFI 2.0 (released after 2010)
  - CPU: Intel 64-bit or compatible
  - RAM: 2GB or more
  - File systems: FAT, NTFS, APFS[2] [3], HFS+, EXT2/3/4, ExFAT, YAFFS2[1]
  - RAID: see this section for details
  - Windows Dynamic Disks: not supported
- Powered-on target computer (live scan)
  - Windows Vista[2]/7/8/10 32/64-bit, Server 2008/2012 32/64-bit
  - Windows Dynamic Disks: simple volumes only (no spanned, striped, mirrored, RAID-5 volumes)
- RAM capture
  - Memory capture is supported for live scan only (see above)
- Drive image scan from the Desktop application

    - Format: dd and e01
    - File systems: FAT, NTFS, APFS[2] [3], HFS+, EXT2/3/4, ExFAT, YAFFS2[1]
    - 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
- Operating System Artifacts
    - Windows 7 and newer, MacOS 10.6 to 10.10
- Disk encryption
    - BitLocker: detection and unlocking with passphrase or recovery key. Note that computers with TPM are not supported. Unlocking drive images only works on Windows 8.1 or newer. BitLocker detection fails for target USB flash drives that have only one partition.
    - FileVault2: detection only.

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

3. 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. It is hoped that future versions will be able to overcome this restriction.

Live Mode

ADF forensics tools are accessing the files of the target computer without modifying their timestamps. However, 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

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, 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.EXE-3D353377.pf (File Created)
- C:\Windows\Prefetch PARSER_HOST.EXE-824316AA.pf (File Created)
- C:\Windows\Prefetch SCAN.EXE-AA570DA9.pf (File Created)

- C:\Windows\Prefetch LAZAGNE.EXE-29FABBD7.pf
- C:\Windows\Prefetch LAZAGNE_WRAPPER.EXE-3366C7E7.pf
- 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\services\usbstor\enum
- HKEY_LOCAL_MACHINE\system\controlsetxxx\enum\usbstor\<hardware id>\<serial number>\Device Parameters
- HKEY_LOCAL_MACHINE\system\controlsetxxx\services\ehstorclass\enum
- HKEY_LOCAL_MACHINE\system\controlsetxxx\services\fvevol\enum
- HKEY_LOCAL_MACHINE\system\controlsetxxx\services\iorate\enum
- HKEY_LOCAL_MACHINE\system\controlsetxxx\services\rdyboost\enum
- HKEY_LOCAL_MACHINE\system\controlsetxxx\services\volume\enum
- HKEY_LOCAL_MACHINE\system\controlsetxxx\services\volsnap\enum
- HKEY_LOCAL_MACHINE\system\controlsetxxx\enum\swd\wpdbusenum\
- HKEY_LOCAL_MACHINE\system\controlsetxxx\control\devicecontainers\{GUID}\BaseContainers\{GUID}
- HKEY_LOCAL_MACHINE\system\controlsetxxx\services\wudfwpdfs\enum
- HKEY_LOCAL_MACHINE\system\controlsetxxx\services\wpdupfltr\enum
- HKEY_LOCAL_MACHINE\system\controlsetxxx\enum\swd\wpdbusenum\<hardware id>
- 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\

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

4. Stealth Mode (Triage-G2® only)

Live scans executed with Triage-G2® can operate in “stealth mode”. In this mode, Triage-G2® 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).

5. Default Search Profiles

ADF forensics tools come with ready-to-use default Search Profiles. A Search Profile is a combination of Captures and settings. Artifact Captures recover specific records or information e.g. browsing history records or user account information. Users cannot create or edit Artifact Captures. File Captures recover files matching certain criteria such as file properties, inclusion of keywords or matching hash values. File Captures are supplied with the program and can also be user created.

Search Profile	Description
Quick – IPOC	This Indecent Pictures of Children (IPOC) Search Profile runs all Artifact Captures except email. It collects pictures and video frames in web browser caches, and searches for common IPOC keywords in filenames and artifacts. Only use on computers.
Quick - General Profiling	This General Profiling Search Profile runs all the Artifact Captures except email and P2P Captures. Collects pictures in browser cache and identifies Social Media and Anti- Forensic Traces. Only use on computers.
Quick – Collection - iOS Backup	This file collection profile specifically targets the iOS backup folder and collects all files within. Only use on computers.
Intermediate – IPOC	This Indecent Pictures of Children Search Profile runs all Artifact Captures, collects pictures and video frames in user folders, searches for common IPOC keywords and known hash values in user folders, collects pictures with EXIF and GPS data and collects protected files and files not processed by the parser. Referenced files are collected. Only use on computers.
Intermediate - General Profiling	This general profiling Search Profile runs all Artifact Captures, excluding P2P captures, collects pictures, video frames, and Office documents in user folders. Collects protected files and files not processed by parser. Referenced files are collected. Only use on computers.
Intermediate - Email	This search profile recovers messages and attachments from Outlook, Apple Mail, Windows Mail and Windows Live Mail. Collects protected files and files not processed by parser. Only use on computers.
Comprehensive – IPOC – speed optimized	As Comprehensive – IPOC with the File Processing Timeout reduced to 15 minutes. File capture options changed to Thorough identification of files Without Extension instead of the Thorough identification for all files.
Comprehensive – IPOC	This Indecent Pictures of Children Search Profile runs all Artifact Captures, collects allocated, embedded, deleted pictures and videos. Searches for common IPOC keywords, and searches for known hash values. Collects files from the Skype received files and media cache folders, and also collects protected files and files not processed by parser.
Comprehensive - General Profiling speed optimized	As Comprehensive – General Profiling with the File Processing Timeout reduced to 15 minutes. File capture options changed to Thorough identification of files Without Extension instead of the Thorough identification for all files.

Comprehensive - General Profiling	Runs all artifact captures, excluding P2P captures, collects allocated, embedded, and deleted pictures, videos and video frames from videos over 100MB, and all office documents. Collects Registry files, searches for anti-forensics applications, and collects user Desktop shortcuts. Collects protected files and files not processed by parser.
Comprehensive – Collect Pictures from Free Space	Runs one file capture: Collect Deleted Pictures from Unallocated Clusters.

6. Default Data Captures

The table below lists the Captures that are available out-of-the-box.

Capture	Description
APPLICATIONS > Anti-Forensics Traces	Identifies installed applications that can be used to conceal user's activity. Supported: Windows, MacOS.
APPLICATIONS > Application Usage	Collects applications' usage information for all the users of the targeted Operating Systems. Supported: Windows, MacOS.
APPLICATIONS > Bitcoin Traces	Keyword search (RegEx) for traces of bitcoin installations and wallets. Supported: Windows, MacOS, Linux.
APPLICATIONS > Cloud Storage Traces	Keyword search (RegEx) for traces of Cloud storage and installations. Supported: Windows, MacOS, Linux.
APPLICATIONS > Installed Applications	Collects the list of installed applications on the targeted Operating Systems. Supported: Windows, MacOS.
APPLICATIONS > P2P Files Shared or Downloaded	Collects the list of files shared and downloaded on Peer-to-Peer networks. Supported: BitTorrent, eMule, Gigatribe, Shareaza, uTorrent.
APPLICATIONS > P2P Search Terms	Collects the list of search terms found in Peer-to-Peer applications. Supported: Ares, eMule, Shareaza.
APPLICATIONS > P2P Traces	Keyword search (substring) for installations of P2P applications. Supported: Windows, MacOS, Linux.
APPLICATIONS > Remote Access Traces	Keyword search (substring) for installations of remote computer access applications. Supported: Windows, MacOS, Linux.
APPLICATIONS > Shareaza GUID's	Keyword search (RegEx) for Shareaza GUID's. Supported: Windows, MacOS.
APPLICATIONS > Social Media Traces	Keyword search (RegEx) for traces of the most popular social media sites and activity. Supported: Windows, MacOS.

COMMUNICATION > Apple Lockdown Files collection	Collects iOS devices lockdown files to allow pairing with devices from a different computer. Supported: Windows, MacOS.
COMMUNICATION > Calls	Collects calls metadata from a variety of applications. Supported: Skype.
COMMUNICATION > Emails	Collects individual emails from a variety of email client applications. Supported: MS Outlook (PST, OST: MS Exchange Accounts, no IMAP accounts), Windows Mail (including version 10), Windows Live Mail, Apple Mail, Android Email, iOS Email, Yahoo Mail, Gmail.
COMMUNICATION > Messages	Collects chat and other short messages from a variety of applications. Supported: Skype.
COMMUNICATION > Saved Contacts	Collects saved contact information from a variety of applications. Supported: Skype.
COMMUNICATION > Skype - Media_Cache Folder	A targeted search to collect all files in the Skype “Media_Cache” directory if present. Supported: Windows, MacOS.
COMMUNICATION > Skype - My Received Files Folder	A targeted search to collect all files in the Skype “my skype received files” directory if present. Supported: Windows, MacOS.
COMMUNICATION > iOS MobilSync Collection	A Targeted search that collects all the files in the “MobileSyncBackup” directory if present. Supported: Windows, MacOS.
DEVICE DATA > Connection Log	Collects network connection information from the targeted system. Supported: Windows, MacOS.
DEVICE DATA > Device Information	Collects general information about the connected target device. Supported: Android, iOS.
DEVICE DATA > Large File Locator	A search to detect all files with a size over 1GB. Supported: Windows, MacOS, Linux.
DEVICE DATA > OS Information	Collects general information about the targeted Operating Systems. Supported: Windows, MacOS.
DEVICE DATA > USB History	Collects the history of all USB devices plugged into the targeted system. Supported: Windows, MacOS.
DEVICE DATA > Virtual Machine Image File Locator	Keyword targeted search (RegEx) that identifies Virtual Machine files. Supported: Windows, MacOS, Linux.
DEVICE DATA > Windows Registry Files	Collects NTUSER.DAT, SYSTEM, SOFTWARE, SAM and SECURITY Registry files. Supported: Windows.

DEVICE DATA > Windows.edb Search Database	Collects the Windows.edb file with a file size of 1MB -100GB. Supported: Windows.
DOCUMENTS > Office Documents Comprehensive - speed optimized	A comprehensive search that will identify and collect documents between 10KB and 50MB, including those in archives and those recently deleted. Uses the thorough file identification method on files without extension only. Supported: Windows, MacOS, Linux.
DOCUMENTS > Office Documents Comprehensive thorough ID	A comprehensive search that will thoroughly identify and collect documents between 10KB and 50MB, including those in archives and those recently deleted. Supported: Windows, MacOS, Linux.
DOCUMENTS > Office Documents in User Profiles	A targeted search of the user profiles that will identify and collect documents between 10KB and 50MB, including those in archives. Supported: Windows, MacOS.
DOCUMENTS > Referenced Files	Collects all files referenced by another artifact such as email attachments, files shared via chat, downloaded files, downloaded P2P files, and recently accessed files. Supported: Windows, MacOS, Linux.
INTEL KEYWORDS > Chemical and Biological	A targeted keyword search (RegEx) of documents, internet files, and text files that will identify chemical and biological terms and collect those files. Supported: Windows, MacOS, Linux.
INTEL KEYWORDS > Chemical and Biological - Arabic	A targeted Arabic keyword search (RegEx) of documents, internet files, and text files that will identify chemical and biological terms and collect those files. Supported: Windows, MacOS, Linux.
INTEL KEYWORDS > Chemical and Biological - Russian	A targeted Russian keyword search (RegEx) of documents, internet files, and text files that will identify chemical and biological terms and collect those files. Supported: Windows, MacOS, Linux.
INTEL KEYWORDS > Chemical and Biological - Urdu	A targeted Urdu keyword search (RegEx) of documents, internet files, and text files that will identify chemical and biological terms and collect those files. Supported: Windows, MacOS, Linux.
INTEL KEYWORDS > Domestic Security	A targeted keyword search (RegEx) of documents, internet files, and text files that will identify domestic security terms and collect the files that contain them. Supported: Windows, MacOS, Linux.
INTEL KEYWORDS > Email Addr-US Phone-CC in Browser Cache	A targeted keyword search (RegEx) of documents, internet files, and text files in the browser cache that will identify email addresses, US phone numbers, and CC numbers and collect the files that contain them. Supported: Windows, MacOS, Linux.

INTEL KEYWORDS > Explosive Precursors	A targeted keyword search (RegEx) of documents, internet files, and text files that will identify Explosive Precursor terms and collect the files that contain them. Supported: Windows, MacOS, Linux.
INTEL KEYWORDS > Financial Fraud Traces	A targeted keyword search (RegEx) of documents, internet files, and text files that will identify financial fraud terms and collect the files that contain them. Supported: Windows, MacOS, Linux.
INTEL KEYWORDS > Infrastructure Security	A targeted keyword search (RegEx) of documents, internet files, and text files that will identify infrastructure security terms and collect the files that contain them. Supported: Windows, MacOS, Linux.
INTEL KEYWORDS > Terrorism	A targeted keyword search (RegEx) of documents, internet files, and text files that will identify terrorism terms and collect the files that contain them. Supported: Windows, MacOS, Linux.
INTEL KEYWORDS > US Agencies	A targeted keyword search (RegEx) of documents, internet files, and text files that will identify US agencies and collect the files that contain them. Supported: Windows, MacOS, Linux.
IPOC > IPOC Hash Set Comprehensive Thorough ID	A targeted search for Indecent Pictures of Children (IPOC) based on a predetermined hash set. This search will identify and collect files from the entire file system including deleted files. Supported: Windows, MacOS, Linux.
IPOC > IPOC Hash Set Comprehensive speed optimized	A targeted search for Indecent Pictures of Children (IPOC) based on a predetermined hash set. This search will identify and collect files from the entire file system including deleted files. Uses the thorough file identification method on files without extension only. Supported: Windows, MacOS, Linux.
IPOC > IPOC Hash Set In User Profiles	A targeted search for Indecent Pictures of Children (IPOC) based on a predetermined hash set. This search will identify and collect files from the User profiles. Supported: Windows, MacOS, Linux.
IPOC > IPOC Hash Set without File Sizes	A targeted search for Indecent Pictures of Children (IPOC) based on a predetermined hash set. This search will identify and collect files from the entire file system including deleted files. Note that this set is different from the “IPOC Hash Set Comprehensive” Capture and it does not contain file sizes so it takes longer to scan. Supported: Windows, MacOS, Linux.
IPOC > Keywords Comprehensive Thorough ID	A targeted keyword search (RegEx) of documents, internet files, and text files that will identify terms associated with Indecent Pictures of Children (IPOC) and collect the files that contain them. Supported: Windows, MacOS, Linux.
IPOC > Keywords Comprehensive speed optimized	A targeted keyword search (RegEx) of documents, internet files, and text files that will identify terms associated with Indecent Pictures of Children (IPOC) and collect the files that contain them. Uses the thorough file identification method on files without extension only. Supported: Windows, MacOS, Linux.

IPOC > Keywords in Filenames	A targeted keyword search (substring) of file and folder names and artifacts from other captures, that will identify terms associated with Indecent Pictures of Children (IPOC) and collect the files that contain them. Supported: Windows, MacOS, Linux.
IPOC > Keywords in User Profiles	A targeted keyword search (RegEx) of documents, internet files, and text files in the users profiles, that will identify terms associated with Indecent Pictures of Children (IPOC) and collect the files that contain them. Supported: Windows, MacOS, Linux.
MULTIMEDIA > Collect Deleted Pictures from Unallocated Clusters	Collects picture files after carving them from the unallocated space of the targeted systems. Supported: Windows, MacOS.
MULTIMEDIA > Pictures - with EXIF Data	A targeted search that collects live picture files containing camera brand in their EXIF data. Supported: Windows, MacOS, Linux.
MULTIMEDIA > Pictures - with GPS Location Data	A targeted search that collects live picture files containing GPS location data. Supported: Windows, MacOS, Linux.
MULTIMEDIA > Pictures Comprehensive - speed optimized	Collects picture files from common picture storage folders and the rest of the drive. It collects live, recently deleted and pictures from within containers. Uses the thorough file identification method on files without extension only. Supported: Windows, MacOS, Linux.
MULTIMEDIA > Pictures Comprehensive Thorough ID no carving	Collects picture files from common picture storage folders and the rest of the drive. It collects live, recently deleted and pictures from within containers. Supported: Windows, MacOS, Linux.
MULTIMEDIA > Pictures comprehensive Thorough ID with carving	Collects picture files from common picture storage folders and the rest of the drive. It collects live, recently deleted, carved from unallocated and pictures from within containers. Supported: Windows, MacOS.
MULTIMEDIA > Pictures in Browser Cache	A targeted search that collects pictures files from browser cache, including archives, using thorough file identification. Supported: Windows, MacOS.
MULTIMEDIA > Pictures in User Profiles	A targeted search that collects pictures files from user profiles, including archives, using thorough file identification. Supported: Windows, MacOS.
MULTIMEDIA > Videos over 100MB -	Collects frames from videos over 100MB, using thorough file identification. It processes video files from archives, live file systems, and recently deleted. Supported: Windows, MacOS, Linux.

Comprehensive Frames Thorough	
MULTIMEDIA > Videos over 100MB - Comprehensive Frames speed opt	Collects frames from videos over 100MB, using thorough file identification on files without extension only. It processes video files from archives, live file systems, and recently deleted. Supported: Windows, MacOS, Linux.
MULTIMEDIA > Videos over 100MB - Frames in Browser Cache	A targeted search that collects frames from videos over 100MB, using thorough file identification on files without extension only. It processes video files from archives that are located in common Browser cache folders. Supported: Windows, MacOS, Linux.
MULTIMEDIA > Videos over 100MB - Frames in User Profiles	A targeted search that collects frames from videos over 100MB, using thorough file identification on files without extension only. It processes video files from archives that are located in user profiles folders. Supported: Windows, MacOS, Linux.
MULTIMEDIA > Videos under 100MB - Comprehensive Thorough ID	A targeted search that collects live and recently deleted videos, less than 100MB, using thorough file identification. Supported: Windows, MacOS, Linux.
MULTIMEDIA > Videos under 100MB - Comprehensive speed optimized	A targeted search that collects live and recently deleted videos, less than 100MB, using thorough file identification on files without extension only. Supported: Windows, MacOS, Linux.
MULTIMEDIA > Videos under 100MB - Frames in Browser Cache	A targeted search that collects frames from videos in the browser cache, less than 100MB, using thorough file identification on files without extension only. Supported: Windows, MacOS, Linux.
MULTIMEDIA > Videos under than 100MB - Frames in User Profiles	A targeted search that collects frames from videos in the users profiles, less than 100MB, using thorough file identification on files without extension only. Supported: Windows, MacOS, Linux.
USER DATA > Desktop shortcut files	Collects link (lnk) files found on the users' Desktops. Supported: Windows.
USER DATA > Recent Files	Identifies files that have been accessed recently by the users from the targeted system. Supported: Windows, MacOS.
USER DATA > User Accounts	Collects user information and login data from the targeted Operating Systems. Supported: Windows, MacOS.
USER DATA > User Logins	Collects user login and logoff events from the targeted Operating Systems. Supported: Windows, MacOS.

WEB BROWSERS > Browsing History	Collects the list of URLs saved by various web browsers. Supported: Internet Explorer/Edge, Firefox, Safari, Opera, Chrome.
WEB BROWSERS > Download History	Collects downloaded files metadata and tries to locate them on the targeted system. Supported: Internet Explorer/Edge, Firefox, Safari, Opera, Chrome.
WEB BROWSERS > Saved Credentials	Collects saved logins and passwords saved by various web browsers. This Capture only works on a live Windows target computer. Supported: Internet Explorer/Edge, Firefox, Opera, Chrome.
WEB BROWSERS > Search Terms	Extracts the search terms from saved URLs. Supported: Internet Explorer/Edge, Firefox, Safari, Opera, Chrome.

7. 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:

Archives

- 7zip Archive - 7z[1] [3]
- BZ Archive - bz2
- Compressed ROM - cramfs
- GNU Zip Archive - gz
- GNU Zip Archive - gzip
- Java Archive - jar
- Roshal Archive - rar[1] [3]
- Roshal Archive - r01
- Squash File System - squashfs
- TAR Archive - tar
- ZIP Archive - zip[1] [3]

Document Files

- Apple iWork Numbers 2009 (2014 for collection only) - numbers[1]
- Apple iWork Keynote 2009/2014 - key[1]
- Apple iWork Pages 2009 (2014 for collection only) - pages[1]
- Microsoft Word - doc[1] [2] dot
- Microsoft Word - docm[1] [2] docx[1] [2] dotm dotx
- OpenDocument - odf
- OpenDocument Graphics Document - odg
- OpenDocument Presentation - odp
- OpenDocument Spreadsheet - ods
- OpenDocument Text Document - odt
- Microsoft OneNote Index - onetoc2

- OpenDocument Presentation Template - otp
- OpenDocument Spreadsheet Template - ots
- OpenDocument Text Document Template - ott
- Portable Document Format - pdf
- Microsoft PowerPoint - ppt
- Microsoft PowerPoint - pptm pptx[1 2]
- Microsoft Publisher - pub
- Rich Text Format - rtf
- Data Exchange File - slk
- OpenOffice Text Document - sxw
- Microsoft Excel - xls[1 2]
- Microsoft Excel - xlsm xlsx[1 2]
- Microsoft Works - wps
- XML Paper Specification - xps

Internet Files

- ASP NET Web Page Source - aspx
- HTML Page - shtml html shtm htm
- Javascript Source - js
- Archived Web Page - mht
- PHP Source - php
- Extensible Markup Language - xml

Miscellaneous Artifacts

- Configuration - cfg
- Configuration - conf
- Log - log
- Resource - rc

Thumbnail Cache

- Windows Picture Database - .*/thumbcache_(16|32|48|96|256|1024|sr|wide|exif)\\.db$
- Windows Picture Database - .*/thumbs\\.db$

Picture Files

- Windows OS/2 Bitmap Graphics - bmp
- Corel Photo-Paint - cpt
- Encapsulated PostScript - eps
- Extended Windows Metafile Format - emf
- Graphic Interchange Format - gif
- JPEG/JIFF Image - jpe jpg jpeg
- JPEG/JIFF Image - jpg_320x240 jpg_170x128
- JPEG 2000 - .*\\.m?j((p?(eg)?2((000)|k)?))|(p(c|f|x|m))$
- JPEG - new
- Paintbrush Bitmap Graphic - pcx
- Portable Network Graphic - png
- Photoshop Image - psd

- Truevision Targa Graphic - tga
- Tagged Image Format File - tif tiff
- Windows Metafile - wmf
- UNIX Icon - xpm

Text Files

- Text - txt text

Video Files

- Multimedia Container - 3g2
- Multimedia Container - 3gp
- Audio Video Interleave File - avi
- Adobe Flash - f4p
- Adobe Flash - f4v
- Adobe Flash - flv
- MPEG-2 Video Stream - m2v
- MPEG-4 Video - m4v
- Matroska Video Stream - mkv
- Digital Music Sound Clip - mod
- QuickTime Video - mov
- MPEG-4 Video - mp4
- MPEG 1 System Stream - mpeg mpg
- Video Clip - mts
- Ogg Vorbis Video - ogv
- RealMedia Stream - rm
- DVD Video Movie - vob
- WebM Video Container - webm
- Advanced Streaming Format - asf
- Windows Media File - wmv

Note [1]: the application can detect when such files are password protected
Note [2]: if such files are created with Libre/OpenOffice the password protection is not detected
Note [3]: no multi-volume support

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

8. File Carving

It is possible to carve pictures from the unallocated space of the target devices. When the original size of the picture cannot be determined, a chunk of at most 5MB is carved.

9. Timestamps Management

During the course a scan, many timestamps are collected. They are all saved in the scan results database in UTC so that they can be compared and sorted. Some timestamps, that do not contain timezone information, cannot be easily converted to UTC and require to identify their likely timezone. Determining the likely timezone is done by searching for timezone information on the target devices and using the one from the most recently accessed partition.
When displaying timestamps, this likely timezone is used in order to display local timestamps.

10. Adding Drivers to the WinPE Image

When trying to boot a target computer it is possible that some hardware components are not natively supported by WinPE which is the Operating System used by our application. Advanced users have the ability to add drivers to the WinPE image of the Collection Key.
To add drivers:

- Place the driver files including the *.inf file in a sub-folder of C:\ProgramData\ADF Solutions Inc\v4\WinPE\drivers. Note that the driver cannot be in an archive file.
- Prepare the Collection Key and it will contain the new drivers.

11. 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
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 files 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.

12. Information to Share with Support

During the course of a scan some files with unexpected data structure can cause the parsers in charge of their processing those files 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.

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

The following log files are created:

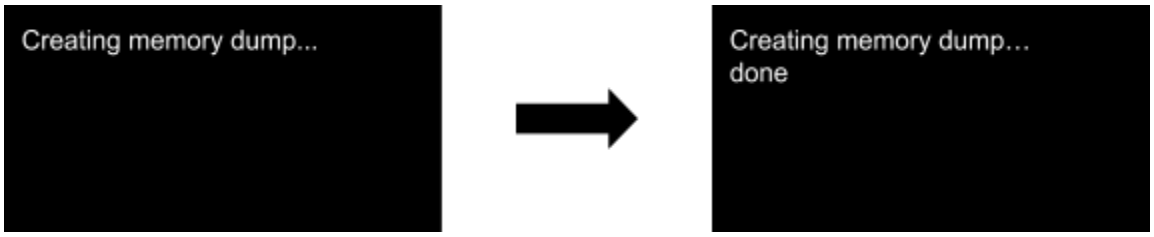
- adf.exe_DATE_TIME.N.log: Log file created by the main application with messages related to Search Profile Management, CK Preparation, Scan Preparation, Device Enumeration, Imager, Licensing, Viewer and Export.
- scan.exe_DATE_time.N.log: Log file created by the scanner with messages related to the 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).

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!



13. 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.
- Documents or pictures that take longer than one hour to process will be skipped.
- When collecting files that are either protected or are corrupted and could not be scanned, only files smaller than 2GB are collected.

14. New Features

DEI 1.4.2, TG2 4.4.2, TINV 4.4.2

NEW	Allow multiple workstations to work from a shared network drive
NEW	Standalone viewer now includes all the Viewer settings (shown/hidden columns, filters, sort order, etc)
NEW	Add progress information at the end of the scan during the database optimization phase
NEW	Set the scan information fields from a json settings file passed to the command line
FIXED	Scan no longer freezes at the end during the database optimization process
FIXED	Empty scan information fields are now properly processed in the VICS json export
FIXED	List all Captures containing file records in the VICS export table
FIXED	Standalone viewer can now be exported to a network drive
FIXED	Output data folders are no longer created if they do not exist (prevents writing data in unexpected places)
FIXED	Some jpg files were not properly identified by the thorough identification method

DEI 1.4.1, TG2 4.4.1, TINV 4.4.1

FIXED	RelativePath attribute of VICS export contained absolute path

DEI 1.4.0, TG2 4.4.0, TINV 4.4.0

NEW	Global: allow Standard User to run the Desktop application (with limitations)
NEW	Artifacts: process web browsers cached files
NEW	Artifacts: Device Data>USB History, User Logins, Connection Log (updated for MAC El Capitan and newer)
NEW	Scan Setup: set file scan timeout and collect skipped files
NEW	Scan Setup: indicate which file types support magic detection
NEW	Scan: view results without stopping the scan
NEW	Scan: support APFS partitions
NEW	Scan: automatically start the scan (Triage-G2 only)
NEW	Scan: compute MD5 and SHA1 on collected files for integrity validation
NEW	Scan: avoid collecting large files that would not fit on the Collection Key but continue the scan
NEW	Scan: Desktop scans require the Authentication Key to be connected for the duration of the scan
NEW	Scanner: start from the Home page
NEW	Scanner: updated WinPE version and various drivers
NEW	Viewer: export in VICS format (can be imported into Griffeye and other forensic tools)
NEW	Viewer: create report in PDF format
NEW	Viewer: add colors to tags
NEW	Viewer: view all records' properties in the new keyword search views
NEW	Viewer: choose thumbnail size in the Pictures and Videos views
NEW	Viewer: improved file explorer view with folder selector
NEW	Viewer: filter out simple pictures like icons and cliparts
NEW	Viewer: view pictures organized by visual classes such as people, faces, weapons, vehicles, indecent pictures of children and more
NEW	Viewer: view videos organized by visual classes
NEW	Viewer: new threaded email view
NEW	Viewer: show all tagged records in one view
NEW	Viewer: new search box in text filters

NEW	Viewer: search scan result for dates
NEW	Viewer: search scan result for hash values
NEW	Imager: verify image checksum after imaging completion
NEW	Imager: produce imaging log file
FIXED	Destination drive not recognized while imaging from a boot scan
FIXED	Improved Thumbcache parsing
FIXED	Improved jpeg carving

DEI 1.3.1, TG2 4.3.1, TINV 4.3.1

FIXED	Manage situation when scan result folder is manually renamed
FIXED	Improve application startup performance when scan result folder contains lots of data
FIXED	Containers referenced by artifact records are now processed
FIXED	Restored automatic software upgrade on connected workstations
FIXED	Keep Preview window on top of the application
FIXED	Use same file identification method for files and containers
FIXED	Corrected PhotoDNA digest computation
FIXED	Improved parsing of thumbnail cache databases
FIXED	Fixed rare situation where Collection Key was added as a scan target

DEI 1.3.0, TG2 4.3.0, TINV 4.3.0

NEW	Installer: move installer to MSI file to support remote software updates
NEW	Artifacts: Communication>Saved Contacts (Outlook on PC)
NEW	Artifacts: Mac Office files are now supported
NEW	Artifacts: Web Browsers>Saved Credentials
NEW	Artifacts: Applications>Remote Access Traces
NEW	Scan setup: use file names to define new file type not just extensions
NEW	Scan setup: compute PhotoDNA on local pictures
NEW	Scan Setup: set file scan timeout

NEW	Scan Setup: hide default Search Profiles
NEW	Scan: add labels to scanned exhibits
NEW	Scan: process files referenced by the Communication>Emails Capture
NEW	Scan: process files referenced by the Communication>Messages Capture
NEW	Scan: process files referenced by the Web Browsers>Downloads Capture
NEW	Scan: process files referenced by the User Data>Recent Files Capture
NEW	Scan: process files referenced by the Applications>P2P Files Shared or Downloaded Capture
NEW	Scan: identify type of files without extensions
NEW	Scan: indicate when files are automatically tagged during the scan
NEW	Scan: prompt for password/recovery key for BitLocker encrypted partitions
NEW	Scan: support ExFat and YAFFS2 partitions
NEW	Scan: support new RAW picture formats
NEW	Viewer: file listing view
NEW	Viewer: view pictures that are visually similar to the PhotoDNA Capture
NEW	Viewer: search the scan result for keywords
NEW	Viewer: move backward and forward through views
NEW	Viewer: see files attached to emails, chat messages, and other artifacts
NEW	Viewer: ability to export record properties in keyword views
NEW	Viewer: export files' metadata in HTML and CSV reports
NEW	Viewer: view current record in Timeline view
NEW	Viewer: show timestamps adjusted to most relevant time zone
NEW	Viewer: view matching file in its folder on the Files view
NEW	Viewer: show most relevant EXIF data fields
NEW	Settings: receive warnings about expiring license files and manage them
NEW	Imager: simplified imaging screen and make it possible to select a folder as destination and case information prior to imaging
NEW	Imager: ask for passwords/recovery key for BitLocker encrypted partitions
FIXED	RAM dump did not collect the expected data

FIXED	Drive images with more than 100 segments were not processed as expected

DEI 1.2.1, TG2 4.2.1, TINV 4.2.1

FIXED	Search Profiles and Captures created in DEI could not be imported in Triage-Investigator®
FIXED	Jar files could not be excluded and were taking a long time to process
FIXED	Added new source of recent files to the User Data>Recent Files Capture
FIXED	Large thumbcache files were not fully parsed
FIXED	Original file time stamps were incorrect when exported with HTML report

DEI 1.2.0, TG2 4.2.0, TINV 4.2.0

NEW	Artifacts: RAM Capture
NEW	Artifacts: Recent Files Capture inclusion of MRUs
NEW	Artifacts: new Peer to Peer applications - Shareaza, uTorrent, Gigatribe, BitTorrent
NEW	Artifacts: improved OS Information Capture with Registered Owner, Registered Organization, Last Shutdown Time, and Computer Name
NEW	Artifacts: improved Skype Messages Capture to include file transferred details
NEW	Scan setup: import/export Search Profiles and Captures
NEW	Scan setup: copy and edit file Captures and Search Profiles
NEW	Scan setup: import Project VIC hash sets
NEW	Scan: automatic tagging of hash and keyword matches
NEW	Scan: scan each file once to improve scan speed
NEW	Scan: collect complete EXIF data including GPS locations
NEW	Scan: run live scan in stealth mode
NEW	Scan: recover from crashes while processing pictures, videos, documents and archives
NEW	Scan: scan network drives
NEW	Scan: hide thumbnails during scan
NEW	Viewer: filter and sort by tags
NEW	Viewer: avoid duplicate files in scan results

NEW	Viewer: simplified keywords view with new excerpt panel
NEW	Viewer: filter records via path explorer
NEW	Viewer: precisely select content to export in reports
NEW	Viewer: sort and filter on any file properties in the Pictures and Videos views
NEW	Viewer: navigate from the Summary view
NEW	Viewer: new file property indicating when files have misleading extensions
NEW	Viewer: open original files from the HTML report
NEW	Viewer: standalone viewer can open scan results from any location
NEW	Settings: access settings menu in Triage-Investigator®
NEW	Home: access user guide

DEI 1.1.2, TG2 4.1.2, TINV 4.1.2

FIXED	4096 byte sectors were not always detected properly

DEI 1.1.1, TG2 4.1.1, TINV 4.1.1

FIXED	Present incorrect video frames and picture previews after video parser crashes

DEI 1.1.0, TG2 4.1.0, TINV 4.1.0

NEW	Artifacts: peer-to-peer Capture
NEW	Artifacts: user login events Capture
NEW	Artifacts: search and collect emails - including Windows Mail 10
NEW	Artifacts: show shared files in Skypes
NEW	Artifacts: apps traces such as social media, bitcoin, cloud storage
NEW	Scan setup: define new file types by extension or magic
NEW	Scan setup: select individual file types to be processed
NEW	Scan setup: convert regular drive into Collection Key
NEW	Scan setup: optionally collect corrupted or password protected files
NEW	Scan: warn when BitLocker and FileVault2 drives are detected

NEW	Scan: modify scan date and time if needed
NEW	Scan: collect protected and corrupted files for later review
NEW	Scan: protect Collection Key with BitLocker (requires Windows 10 when preparing the Collection Key)
NEW	Scan: maintain timestamps of collected files in the zip archive
NEW	Viewer: select which views and records to export in HTML/CSV reports
NEW	Viewer: new list layout view for HTML reports
NEW	Viewer: new view to display scan log messages
NEW	Viewer: filter by picture pixel size
NEW	Viewer: copy/paste text from the Details pane
NEW	Settings: set paths where data (scan results, reports, Search Profiles…) is stored
NEW	Settings: define default tag names

DEI 1.0.1, TG2 4.0.1, TINV 4.0.1

NEW	Display a warning message when the Collection Key runs out of space
FIXED	Drives larger than 2TB were not available for scanning
FIXED	Scanning folders with Unicode characters was not working
FIXED	Video frames were not displayed in case the file was not collected
FIXED	Editing a Capture containing hash values would delete all the hash values
FIXED	Encrypted pptx files were not detected and logged
FIXED	Encrypted docx files were not detected and logged

15. 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.
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.
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: https://github.com/Nevcairiel/LAVFilters/releases.
Viewer thumbnail size	On 4K monitors we recommend setting the thumbnail size to 128 pixels or higher.
macOS	In some instances, the Apple Operating System installation date may be incorrect.
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 C:\Users\<NAME>\AppData\Local\cache\qtshadercache.

16. Data Migration from 4.3 to 4.4

IMPORTANT: You should contact support@adfsolutions.com if you are running a version prior to DEI 1.3.x or Triage-Investigator and Triage-G2 4.3.x.

Version 4.4 will automatically migrate custom-made Search Profiles, file Captures, and Scan Results from the previous version. Some of the default file Captures available in previous versions have been restructured in 4.4. If such Captures were used in your own Search Profiles, they are no longer referenced. It is necessary to edit your Search Profiles and re-select the file Captures needed. The table below indicates which new Captures match the old ones.

Version 4.3 Capture	**Version 4.4 Capture**
Bitcoin Traces	Cryptocurrency Traces
Office Documents Comprehensive thorough ID Note: that Capture’s name contained trailing spaces forcing to manually re-select it after the upgrade.	Office Documents Comprehensive thorough ID

Note: it can take up to 20 minutes to migrate file Captures containing millions of hash values!

17. 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
boost	1.64	Project Page Used Source Link (with Windows-style EOL's)	Boost Software License
FFmpeg	3.3.2	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	License
gsl		Project Page	License
icu	icu4c-59	Project Page	License
libbde	2017/02/04	Project page	LGPLv3
libbfio	2014/10/15	Project Page	LGPLv3
libesedb	2015/12/13	Project Page	LGPLv3
libevtx	2016/01/07	Project Page	LGPLv3
libewf	2014/06/08	Project Page	LGPLv3
libimobiledevice	1.1.6	Git-master with latest commit	LGPL v2.1
liblnk	2016/01/07	Project Page	LGPLv3
libolecf	2016/01/07	Project Page	LGPLv3
libmsiecf		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	license
libvhdi	alpha-20170223	Project Page	LGPLv3

libvmdk	alpha-20170226	Project Page	LGPLv3
libxml2	2.9.4	Project Page	MIT License
minizip	2017/07/26	Project Page	Free to use
openssl	1.0.2l (2017/05/25)	Project Page	OpenSSL License
plop	07/Feb/2012	Project Page	License
prefetch	01/Dec/2018	Project Page	Apache license 2.0
protobuf	2.6.1	Project Page	Protobuf License
Qt		Project Page	LGPLv3
RapidJSON	1.0.2	http://rapidjson.org/	MIT License
RE2		Google RE2	RE2 License
sleuthkit	4.5.0	Project Page	IBM Public License Common Public License
SQLite	59.1	Project Page	Public Domain
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

18. 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 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
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 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
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
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