AccessData AD Lab 6.0.1 Release Notes

Document Date: 11/30/2015

©2015 AccessData Group, Inc. All rights reserved

Introduction

This document lists the new features, fixed issues, and known issues for this version of AD Lab. All known issues published under previous release notes still apply until they are listed under “Fixed Issues.”

For convenience, the Release Notes from previous versions are included at the end of this document.

- AccessData AD Lab 6.0 Release Notes (page 6)

Supported Platforms

For a list of supported platforms for AD Lab see the following:

http://accessdata.com/solutions/digital-forensics/forensic-toolkit-ftk/technical

6.0.1 New and Improved

The following items are new and improved for this release:

Processing

- Carbonite Support

  Support for Carbonite as been added (Personal Backup only).

  A CarboniteConfig.dat file is identified when it is inside of an image, or when files or directories are added individually. CarboniteConfig.dat information is listed as “Carbonite config” and the contents are displayed in html. You can see the User and Directory (path) information for directories that are being backed up.
- XRY Support

  Support for XRY images has been enhanced including support for Motorola DROID and Samsung Start images. (35272, 35276, 35278)
- OCR

  When performing OCR, you no longer choose an OCR engine. LeadTools is now the only engine used. (35610)

Processing Options

- In the *Lab/eDiscovery Processing Options*, the Actual Files Only de-duplication option has ben removed. (34046)

Mobile Support

- Cellebrite® Physical Analyzer Support

  You can now process Cellebrite Physical Analyzer files from versions 4.1 through 4.4.

  (Version 3.0 and 4.0 were previously supported)

Fixed Issues in 6.0.1

The following issues have been fixed in this release:

System

- When using Backup/Restore or Copy Previous Case, moving expanded compound files evidence (such as a UFDR file) from 5.6 to 6.x works correctly. (34754)

Processing

- After performing OCR on a PDF, you can perform an Index Search on embedded text and text from the OCR. (29755)

Decryption

- When selecting to do automatic decryption while setting up the case and only selecting the automatic decryption check box, the status of the automatic decryption and passwords entered are properly saved. (35733)

Examiner

Reports

- When creating a Load File report and exporting emails contained in a pst, choosing to output as msg works correctly. (35074)

Other

- Scroll bars are working properly in the Video tab. (35041)

Important Information

Latest Documentation

To access the latest AD Lab Release Notes and documentation

Download the zip file from www.accessdata.com/productdocs/adlab/adlab.zip

Installation and upgrade

- AD Lab supports Distributed Processing Engines (DPEs).

Upgrading CodeMeter

- AD Lab 5.6.1 and later include an updated version of CodeMeter Runtime Kit (5.21).
  - If this is a new installation of AD Lab you do not need to do anything and the latest version of CodeMeter is installed.
  - If you are upgrading to AD Lab 5.6.1, be aware that a security vulnerability has been detected in Codemeter 4.5. However, if you simply upgrade from CodeMeter 4.5 to 5.21, the vulnerability remains. To fix the vulnerability, you must manually uninstall 4.5 before installing 5.21.

    If you are upgrading to AD Lab 5.6.1, manually uninstall CodeMeter first and then install AD Lab 5.6.1 which will install a clean CodeMeter 5.21. Otherwise, after upgrading to AD Lab 5.6.1, manually uninstall CodeMeter 4.5 and then manually install CodeMeter 5.21.

Running PostgreSQL on a Virtual Machine

- If you run PostgreSQL on a virtual machine with a dynamically allocated virtual hard drive, you must manually stop the PostgreSQL service before rebooting the virtual machine. Otherwise, PostgreSQL will become corrupted.

  If you run PostgreSQL on a virtual machine with a fixed size virtual hard drive, then PostgreSQL will not become corrupted when rebooting.

Recommendations

- Cerberus writes binaries to the AD Temp folder momentarily in order to perform the malware analysis. Upon completion, it will quickly delete the binary. It is important to ensure that your antivirus is not scanning the AD Temp folder. If the antivirus deletes/quarantines the binary from the temp, Cerberus analysis will not be performed.
- If you choose to have a case's database files placed in the case folder, do not move your case folder without first archiving and detaching the case.

New AD1 files and Imager 3.4.x

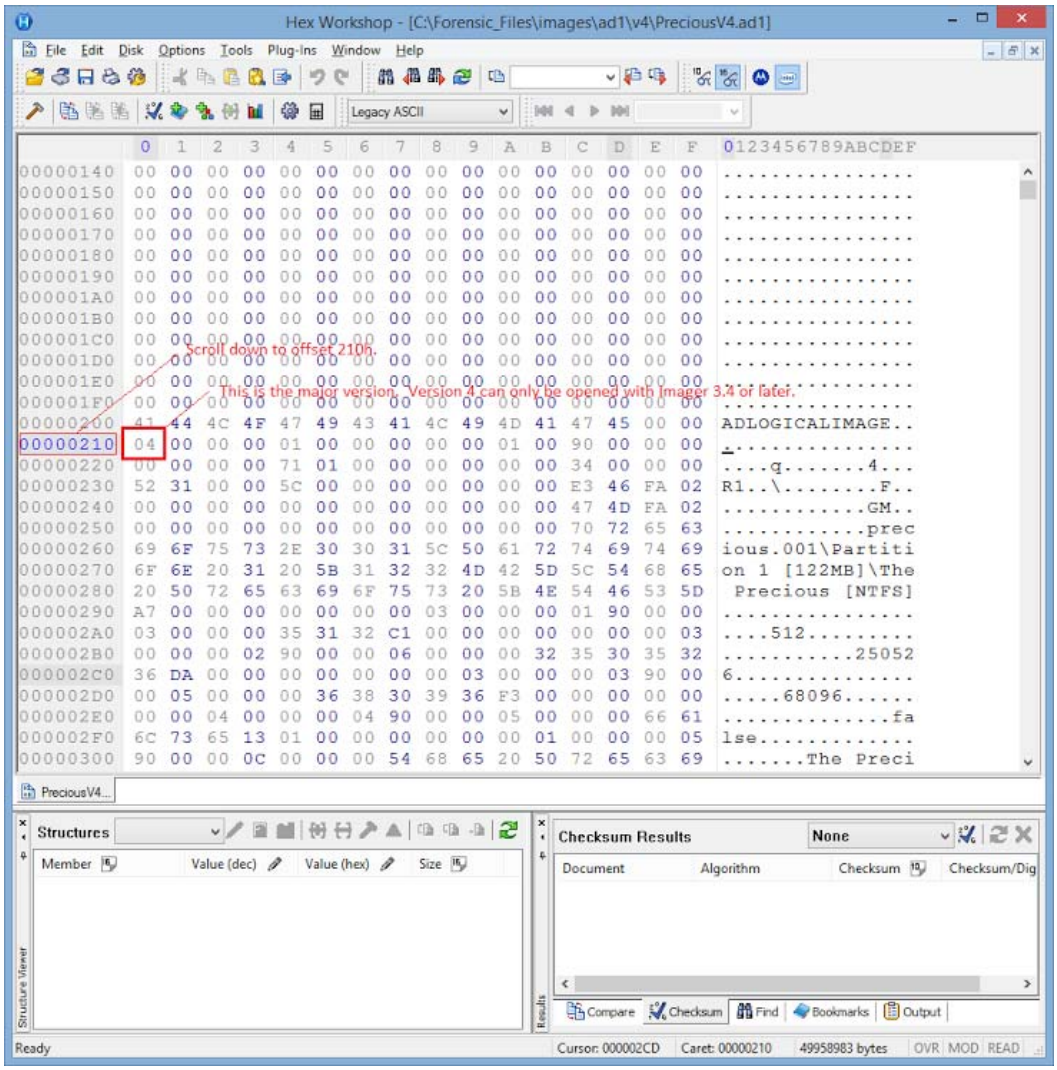
Any AD1 file created by FTK or Summation 6.0 or later can only be opened with Imager 3.4.0 or later.

Imager 3.4 can be freely download from the AD website:

http://accessdata.com/product-download

Using an older version of Imager will result in an “Image detection failed” error.

This happens because the AD1 format was enhanced to support forward compatibility between AccessData products. Newer AD1s have a version 4 in the header instead of 3. A hex editor can be used to quickly determine if your AD1 is v3 or v4.



Where to get more information

Use the following documentation resources to learn more about this product. Each document is available in PDF format in the download ISO file. The *User Guide* is also available through the *Help* menu in AD Lab.

The latest version of each document is available in the *Product Release* pane on the FTK product download page:

http://www.accessdata.com/support/product-downloads/ftk-download-page

Document	Description
Quick Installation Guide	Basic information about how to install and upgrade this and related products.
FTK Installation Guide	Information about how to install and upgrade this and related products.
User Guide	Information about how to use this product, including detailed technical information and instructions for performing tasks.
Upgrading, Migrating, and Moving Cases	Information about upgrading and migrating cases from 4.1 to 4.2, and moving cases from one database to another.
Upgrading Cases	Information about upgrading cases from 4.1 to 4.2.
Migrating Archived Cases	Information about upgrading or migrating cases that you have archived in a previous release.
KFF Quick Install Guide and KFF installation files	For the most current KFF Server and KFF data installation files, as well as the *KFF Quick Install Guide*, visit the AccessData Product Downloads page: http://www.accessdata.com/support/product-downloads Expand the *Known File Filter (KFF)* section and then the *KFF Server* section.

Comments?

We value all feedback from our customers. Please contact us at *support@accessdata.com*, or send documentation issues to *documentation@accessdata.com*.

AccessData AD Lab 6.0 Release Notes

Document Date: 10/27/2015

©2015 AccessData Group, Inc. All rights reserved

Introduction

This document lists the new features, fixed issues, and known issues for this version of AD Lab. All known issues published under previous release notes still apply until they are listed under “Fixed Issues.”

Supported Platforms

For a list of supported platforms for AD Lab see the following:

http://accessdata.com/solutions/digital-forensics/forensic-toolkit-ftk/technical

Important: Future versions of AD Lab will no longer support running on Windows XP.

6.0 New and Improved

The following items are new and improved for this release:

System

Windows 10 Support

- The application and the agent now support Microsoft Windows 10.

Installation

- All installation files have been signed with SHA-256.

Agent

- New Agent Certificate

  To ensure you can continue to integrate with third-party applications, a new agent certificate will be issued to all clients current on their subscription.

Database

- When installing a PostgreSQL database, a newer version (9.3.5.42) is now installed.
- When installing a PostgreSQL database, there is no longer a dialog to choose a method of database optimization. A default setting is now used.
- New *Put each case in its own DB* option (MS SQL and PostgreSQL only)

  To improve performance, when you create new cases, a new database is created for each new case.

  This feature is enabled by default in the following new option:

  Database > Put each case in its own DB

  In addition to improved performance, if you configured the database location to be *In the case folder*, the database files are located under the case folder. This lets you easily back up a case at the folder level as the case data and the database for the case are all under one case folder.

Processing

- Support for Outlook for Mac (OLM) files

  Processing will now detect and enumerate exported Outlook for Mac (OLM) data files.

Processing Options

- The Processing Options interface has been enhanced with pre-defined, one-click options. The following built-in processing option buttons are available:
  - Forensic processing (Default)
  - eDiscovery processing
  - Summation processing
  - Basic assessment
  - Field mode

Mobile Support

- Cellebrite® Physical Analyzer Support

  You can now view Cellebrite Physical Analyzer files within FTK. (Version 3.0 and 4.0)

Decryption

- Decrypting Dropbox databases is supported.

Internet Artifacts

- Support has been added for parsing and viewing the following types of data:
  - Skype
  - DropBox

Imager

- An updated version of AccessData Imager (3.4.2) is available.

  See New AD1 files and Imager 3.4.x on page 11.

Examiner

Web Viewer

- FTK® Web Viewer, Powered by Summation®

  FTK now includes a single license of AccessData Summation.

  You can conduct case assessment earlier with real-time collaboration. Attorneys or other teams now have instant access to case data as it's being identified in FTK while incident responders are in the field or performing on-site collections.

- Multi-Case Search

  Using the Summation web viewer, you can speed up the searching process by searching across multiple cases instead of one case at a time.

Columns

The following columns have been added:

- Microsoft Office document metadata:
  - CreateTime (Content created)
  - EmbeddedComments (PPT files)
  - HiddenColumnsRows (Excel files)
  - HiddenWorkSheets (Excel files)
  - LastPrinted
  - LastSavedTime (Date last saved)
  - RevisionNumber
  - TotalEditingTime (Word and PPT)
  - TrackChanges
- Adobe files metadata:
  - Meta-data - DateCreated
  - Meta-data - DateModified
- Mobile Phones

  Many columns related to Cellebrite support.

- OCR Graphic

  This column provides the OCR confidence % score for each file that has been processed with OCR. This column is sortable which helps you determine which files may need to be manually reviewed for keywords.

- Internet Data
  - Columns for internet data have been grouped into sub-categories to make columns easier to find and identify.
  - New columns have been added for
    - Internet Chat
    - Profile - (Chrome profiles, Skype accounts, and mobile phone user accounts)
    - Offline User Email - (Chrome offline mail database.)
    - Search Terms - (search terms used by internet browsers and mobile phone web searches)

Other

- Various tool tips have been added.

Fixed Issues in 6.0

The following issues have been fixed in this release:

System

Installation/Upgrade/Migration

- Fixed an error that may occur when installing a distributed processing manager. (32938, 33103)
- During the Processing Engine installation, when you customize the path to the temporary files, it now carries over to the AD Lab UI. (27001)

Database

- Updates have been made to improve performance when using a PostgreSQL database.

Processing

- Improved the carving of ZIP files that sometimes caused Additional Analysis jobs to hang. (29824)

Performance

Performance and stability has been improved in the following areas:

- Processing between AD Lab and AccessData Summation. (31583)
- Updating count numbers in the File List. (30016)
- Memory usage when scrolling through thumbnails on the Graphics tab. (30068)
- Multiple users working in the same case. (30725)
- PostgreSQL database with tens of millions of items. (32035)

Examiner

Export

- When exporting decrypted files to an AD1 file, then processing that AD1 file, the files are no longer shown as empty folders or place-holders. (33102)

Other

- AVI files are played properly on the Video tab. (30756)
- INK files that have Russian characters no longer report “Invalid Shortcut File”. (23447)

Important Information

Latest Documentation

To access the latest AD Lab Release Notes and documentation

Download the zip file from www.accessdata.com/productdocs/adlab/adlab.zip

Installation and upgrade

- AD Lab supports Distributed Processing Engines (DPEs).

Upgrading CodeMeter

- AD Lab 5.6.1 and later include an updated version of CodeMeter Runtime Kit (5.21).
  - If this is a new installation of AD Lab you do not need to do anything and the latest version of CodeMeter is installed.
  - If you are upgrading to AD Lab 5.6.1, be aware that a security vulnerability has been detected in Codemeter 4.5. However, if you simply upgrade from CodeMeter 4.5 to 5.21, the vulnerability remains. To fix the vulnerability, you must manually uninstall 4.5 before installing 5.21.

    If you are upgrading to AD Lab 5.6.1, manually uninstall CodeMeter first and then install AD Lab 5.6.1 which will install a clean CodeMeter 5.21. Otherwise, after upgrading to AD Lab 5.6.1, manually uninstall CodeMeter 4.5 and then manually install CodeMeter 5.21.

Running PostgreSQL on a Virtual Machine

- If you run PostgreSQL on a virtual machine with a dynamically allocated virtual hard drive, you must manually stop the PostgreSQL service before rebooting the virtual machine. Otherwise, PostgreSQL will become corrupted.

  If you run PostgreSQL on a virtual machine with a fixed size virtual hard drive, then PostgreSQL will not become corrupted when rebooting.

Recommendations

- Cerberus writes binaries to the AD Temp folder momentarily in order to perform the malware analysis. Upon completion, it will quickly delete the binary. It is important to ensure that your antivirus is not scanning the AD Temp folder. If the antivirus deletes/quarantines the binary from the temp, Cerberus analysis will not be performed.
- If you choose to have a case's database files placed in the case folder, do not move your case folder without first archiving and detaching the case.

New AD1 files and Imager 3.4.x

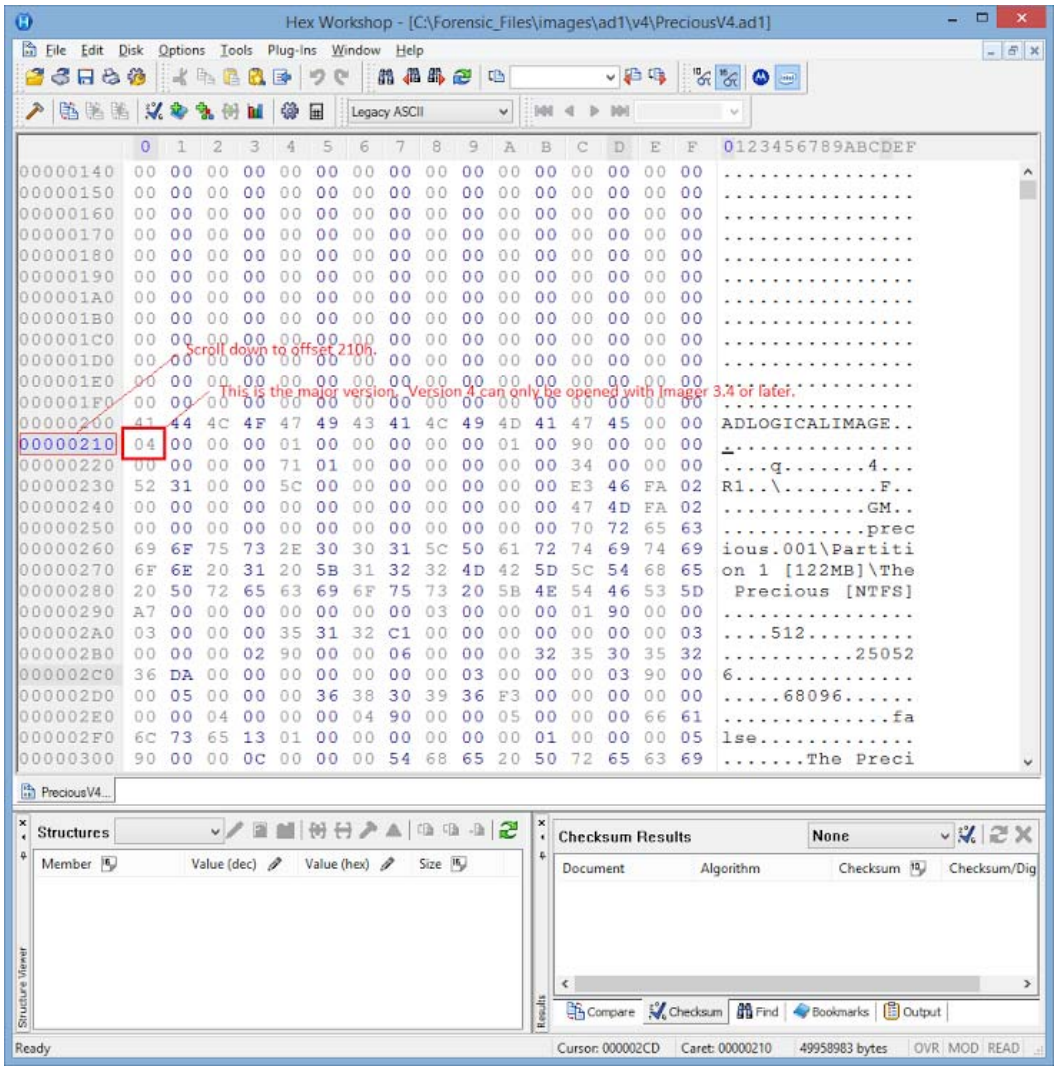
Any AD1 file created by FTK or Summation 6.0 or later can only be opened with Imager 3.4.0 or later.

Imager 3.4 can be freely download from the AD website:

http://accessdata.com/product-download

Using an older version of Imager will result in an “Image detection failed” error.

This happens because the AD1 format was enhanced to support forward compatibility between AccessData products. Newer AD1s have a version 4 in the header instead of 3. A hex editor can be used to quickly determine if your AD1 is v3 or v4.



Where to get more information

Use the following documentation resources to learn more about this product. Each document is available in PDF format in the download ISO file. The *User Guide* is also available through the *Help* menu in AD Lab.

The latest version of each document is available in the *Product Release* pane on the FTK product download page:

http://www.accessdata.com/support/product-downloads/ftk-download-page

Document	Description
Quick Installation Guide	Basic information about how to install and upgrade this and related products.
FTK Installation Guide	Information about how to install and upgrade this and related products.
User Guide	Information about how to use this product, including detailed technical information and instructions for performing tasks.
Upgrading, Migrating, and Moving Cases	Information about upgrading and migrating cases from 4.1 to 4.2, and moving cases from one database to another.
Upgrading Cases	Information about upgrading cases from 4.1 to 4.2.
Migrating Archived Cases	Information about upgrading or migrating cases that you have archived in a previous release.
KFF Quick Install Guide and KFF installation files	For the most current KFF Server and KFF data installation files, as well as the *KFF Quick Install Guide*, visit the AccessData Product Downloads page: http://www.accessdata.com/support/product-downloads Expand the *Known File Filter (KFF)* section and then the *KFF Server* section.

Comments?

We value all feedback from our customers. Please contact us at *support@accessdata.com*, or send documentation issues to *documentation@accessdata.com*.