AccessData AD Lab 6.3 Release Notes

Document Date: 11/07/2017

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 *OS Support* on the product download page:

http://accessdata.com/product-download

New and Improved in 6.3

The following items are new and improved for this release:

Cloud Hosting

Lab in the Cloud

Lab is now available in the cloud via Amazon Web Services (AWS) using either the AWS Marketplace App or in-house AWS servers. Using cloud servers provides additional distributed processing capabilities. See your sales representative for details.

Customizable Processing

Processing Profiles

The Processing Profile buttons are now customizable. Users have the ability to change the settings and the names of the profile buttons for a new case. This allows administrators to create a list of standards for their individual organization's processing procedures. (7242)

The Forensic Processing option now consists of the previous Baseline processing options. (6090)

Indexing Flexibility

Exclusion Filter

There is a new filter capable of excluding selected files prior to review. This allows users to filter out unnecessary items, items not included in a warrant, or other data they wish to exclude from their evidence review. It also shortens the amount of time spent processing and allows users to get into a case faster than if the full data set were processed. Items can be filtered out based on File Type, File Size, and Date. (8243)

Indexing

There is now greater flexibility in the indexing feature. Users can change indexing options within the additional analysis window, allowing investigators the ability to perform multiple passes on the evidence load as they refine the targeted data. (6733)

Users can also choose specific file categories to index, allowing investigators to index uncommon formats or exclude formats that are slowing down the review process. (6733)

Index Search Regex Support

There is a new import/export feature built into index search that allows users to save, edit, and share regex (TR1) expressions with other investigators. (6611, 7278)

There is a new option, Enable TR1 Expressions, that can be selected during case creation to ensure the use of regex TR1 statements return the expected results. (7279, 7282)

KFF (Known File Filter)

The KFF architecture and features have been updated.

- The KFF Server now runs as a different service.

  In versions 5.6 through 6.2, the KFF Server ran as the AccessData Elasticsearch Windows Service.

  In 6.3 and later, the KFF Server uses the AccessData Cassandra service.

  Important: If you are upgrading from 6.2 or earlier, all KFF data must be created in or migrated into the new KFF Server.

- Hash Manager Migration Tool

  If you are upgrading from 5.6 through 6.2, there is a new tool that lets you migrate custom KFF data to the new KFF Server on 6.3.

  Important: NIST NSRL, NDIC HashKeeper, or DHS library data from 6.2 and earlier will not be migrated when using the Migration Tool. You must re-import those using the 6.3 KFF Import Tool.

- KFF Import Utility

  This utility has been updated to use the new KFF Server.

  If you are upgrading from 5.6 - 6.2, make sure to install and use the new 6.3 version.

- NDIC HashKeeper and DHS libraries

  To use these libraries, you must import new versions of the files using the 6.3 version of the KFF Import Utility.

  NDIC HashKeeper and DHS libraries are now downloaded from AccessData and installed as CSV files.

- NIST NSRL

  To import NSRL data, you can do one of the following:

  - Download version 2.58 or later RDS files from nist.gov and import them.
  - Download version 2.54 files from AccessData and import them.

- Deleting NDIC, DHS, and NSRL libraries.

  You can now delete these libraries from within the AD Lab application.

  Important: Deleting these libraries from the application can take from one to several hours. We recommend that you delete these libraries using the KFF Import Utility.

- Export/Import

  When you export and import KFF data, the Binary format (Entire Library) is no longer available. CSV is the only export format supported.

Job Management Improvements

Processing Management Queue

All users now have the ability to see the full list of active processing jobs for cases they have permissions for, regardless of the case or user that initiated it. They also have the ability to change the order of the processing queue for unstarted jobs in order to move high priority evidence items to the top of the list.(8289, 8242)

Third Party Integration

Belkasoft Integration

When a Belkasoft license is on your dongle, you will now have access to utilize Belkasoft parsing technology, adding 150 additional parsers. Contact your sales rep for details.(3139, 9819)

iSubmit Integration

Users now have the ability to pull pertinent information from iSubmit and auto-create a case with that information, allowing investigators to track a case from start to completion within the iSubmit program. (8238)

- You will need to put the iSubmit key in the registry for this to work. The key is a REG_SZ.
  You will need to create the following:
  [HKEY_LOCAL_MACHINE\SOFTWARE\AccessData\Products\Forensic Toolkit\6.3]
  "iSubmitLicense"=[The iSubmit license number you have obtained from iSubmit]

PhotoDNA

PhotoDNA has been removed as a stand-alone product. It is now part of the Project VIC functionality.

Project Vic Integration

FTK now has the ability to import and export Project Vic data using the new Create Project VIC Bookmark option. (7236, 7237)

Usability Improvements

Audit Log Update

Audit logs now include records for when an administrator changes permissions for a user or group. (8241)

Column Setting for Chat Messages

There is a new Chat Messages column setting option. When applied, this option will automatically populate the File List with the following columns: Name, Item Number, Label, Item Description, Created Date, Accessed Date, Modified Date, Chat To, Chat From, Chat Message, Item Source. (11298)

Email Notifications

Users can be alerted via email when the following items occur: (8248, 8285, 8240)

- A user is granted permissions for a case
- Data is added to or removed from a case a user has permission to access; the email is sent once the job has completed

The notification email includes the case name as well as changes to the case or permissions. Emails can be sent to multiple email addresses at the same time.

Evidence Tracking

Details about when evidence was collected, what version of the software was used, as well as other pertinent details for chain of custody are now automatically recorded for FTK Imager, MPE+, and Cellebrite. (8251)

Weighting Criteria in Search

It is now possible to configure and change the weighting criteria when sorting index search terms. This returns a weighted percentage for each item when the index search results populate. (8259)

Miscellaneous

Agent

There is a new field in the Agent Dialog called Agent Name. This allows investigators to name the agent being installed in order to avoid confusion when IP addresses change. This ‘friendly’ name will apply to the machine on which the agent is located. (9122)

CodeMeter

CodeMeter has been updated to version 6.50b. (6722)

Geolocation

Geolocation data now works directly out of the box. It no longer requires the KFF or separate installations to function. (9768)

Mobile Phone AD1 Import Improvements

FTK has changed the way AD1 files created in MPE+ are uploaded, making it easier to view the file structure and drill down into specific files.

PostgreSQL

PostgreSQL has been updated to version 9.6.3. (6757)

Recycle Bin

Users can now properly parse recycle bin offsets for Windows 10. (5066)

SQLite Query Builder

Users can now produce an HTML report of an unsupported SQLite database. (5943)

System Information Reports

It is now possible to right click on the system information and generate a CSV, XML, or HTML file to be included in reports. (7246)

UI

Users can now alter the standard color template of the file list to their desired colors. (8273)

- The colors must be manually modified within the Preferences.xml file. Please refer to the current user guide for more information.

Windows Creator Edition

Windows Creator Edition is now supported. (5943)

Windows Thumbnail Enhancements

Users can now parse thumbs.db path information for Windows 10.

Users can parse out the path of images from a centralized thumbcache. (5062, 5063)

Fixed Issues in 6.3

- When exporting file list information, a formatting issue in the path column was fixed so that there is no longer a line break in the path. (8565)
- The **Verify Image** option on certain images no longer shows the incorrect name of the item selected for verification and reports properly. (5980)
- Improved handling of FAT16 images when using the **Restore Image** functionality. (5078)
- WeChat support has been updated to include additional formats on both iOS and Android. (9112, 9391)
- Improved handling of FileVault2 files. (2391)
- Visualization no longer crashes when it encounters files it cannot identify. (9120)
- File names now use the setting document numbering tied to page numbering when exporting load files from FTK instead of uniquely sequenced document page numbering. (8562)
- Improved handling of the Chat Count column info for WhatsApp (Android) and WeChat (iOS). (8009)
- Fixed the issue where changing the Processing Profile to certain options caused a database connection error to show in the UI. (8011)
- Improved handling of compressed Mac image files. (6727)
- Fixed a refresh issue between the File List and the Evidence Tree window. (8007)
- The **Merge Case Index** checkbox is now available to users who have the appropriate rights and roles. (7125)
- The Common Temp file is no longer deleted on shutdown, possibly orphaning pending processes. Users are able to delete the temp directory when they deem it safe. (9994)

Important Information

Latest Documentation

- The documentation is sometimes updated. For the latest documentation, see the product download page: http://accessdata.com/product-downloador download the zip file from www.accessdata.com/productdocs/adlab/adlab.zip

Installation and upgrade

- The FTK Suite (FTK, AD Lab, AD Enterprise) no longer supports multiple products of the same version running on the same machine at the same time. The user can only install one of the three products of a specific version on a single machine. (29786, 30927)
- 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.

KFF

- The KFF Server now uses the Apache Cassandra database. The version of Cassandra being used requires 64-bit Java 8. No other version of Java (7 or 9) is currently supported.
  - To install Java, go to: https://java.com/en/download/windows-64bit.jsp
  - If you are using a 32-bit browser, you may automatically download the 32-bit version. You must use the 64-bit version.
- When importing data using the KFF Import Utility, make sure that you get a confirmation that the import is complete before processing data using that KFF data. This is particularly important when importing NSRL data that takes several hours to import.
- Deleting NDIC, DHS, and NSRL KFF libraries.

  As of 6.3, you can delete NDIC, DHS, and NSRL libraries from within the AD Lab application.

  Important: Deleting these libraries from the application can take from one to several hours. We recommend that you delete these libraries using the KFF Import Utility.

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.
- When creating a Custom Data View, the available filter list should not include: Checked Files, Unchecked Files (checked status is not available across users), Bookmarked Files, Labeled Files (too broad and will include all bookmarks or labels). These filters have been removed from the list. (6533)
- Difference in file handling when using Belkasoft parsing:

  If a SQLite database is encountered in the evidence that could have been handled by the Belkasoft parser but the Belkasoft All-in-One processing option was not checked, that SQLite database will get expanded using a generic SQLite expansion that shows tables and rows.

  Any evidence processed in the manner that is later re-processed (using Additional Analysis) with the Belkasoft All-in-One expansion option will NOT be expanded using Belksoft technology but will remain with the original expanded items.

  To expand a SQLite database using Belkasoft technology that has already been expanded as a generic SQLite database, it must be added as a new, different piece of evidence, or a new case must be created.

New AD1 files and Imager 3.4.x

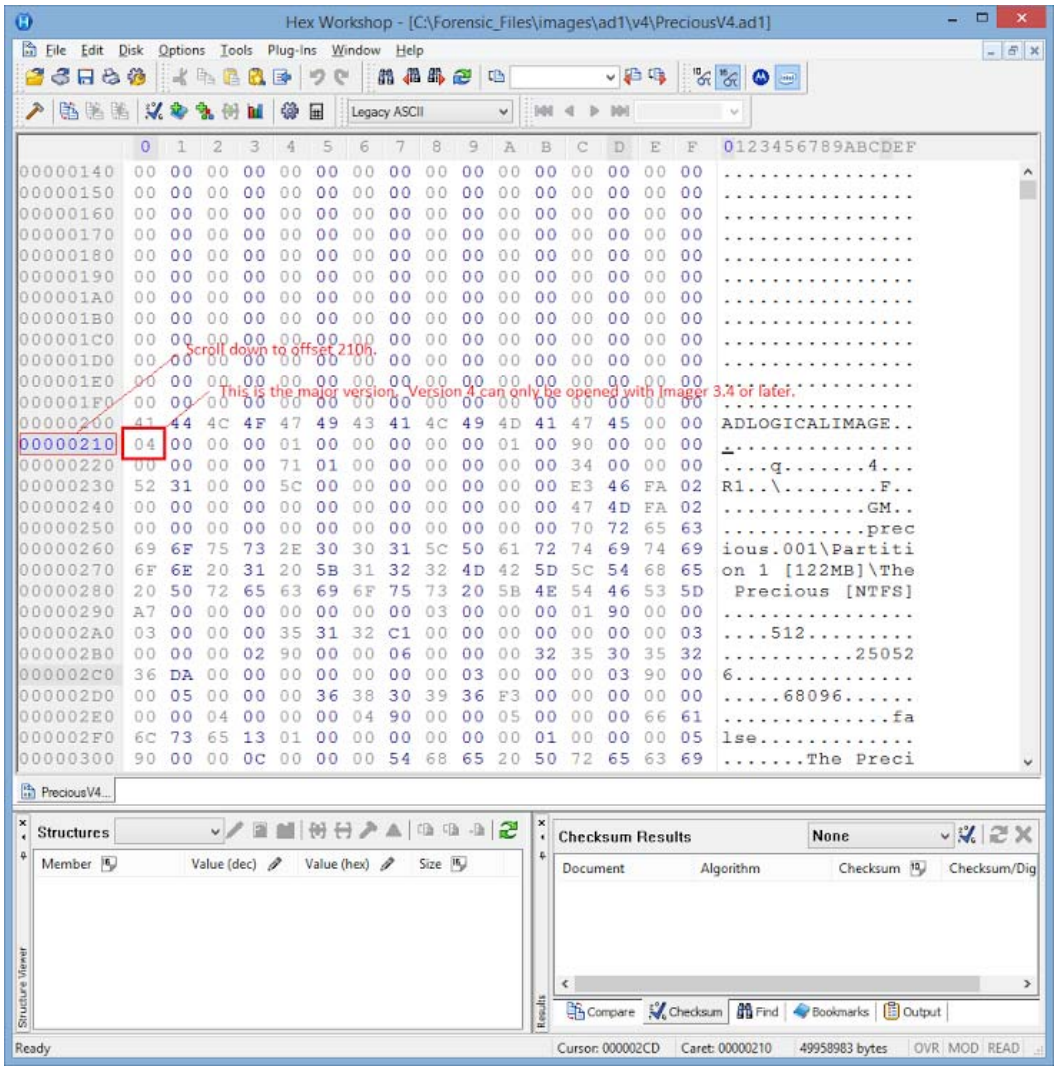
Any AD1 file created by FTK or Summation 6.0 or later can only be opened with Imager 3.4.0 or later.

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.



Known Issues in 6.3

- Lab will freeze momentarily when applying a label on large cases over 60 million objects when the Labels Column is in the grid. It will freeze until labeling completes. (6016)
- Filters created within a case are automatically global, but unable to be used in other cases. (42681/ 41698)
  Workaround: Close the case and close FTK. When you open FTK and a new case the filter will no longer be available.
- If FTK is viewing text at the time the user performs additional analysis on that same text, the additional analysis job will fail. (40598, 1143)
- Some self/user-made certificates may not work in Management Server. (42450, 1202)
  Workaround: Contact AccessData Support for instructions on creating a valid certificate using OpenSSL. (5995)
- When using Credant, if the MS Update KB172605 has been applied to Windows 7, the error “Failed to retrieve keybundle. Check Machine ID and Shield ID” will occur. (5130)
  Workaround: To make sure this is working properly, users need to either acquire the image with the patch installed, or remove the patch from the Evidence Processing machines while processing.
- Custom Data View selections do not work when applied to a group. They must be applied to individual users. (7475)
- Email attachments that haven’t been downloaded by Windows 10 Mail will show an attachment, but it will not be accessible. This is working as designed. (6451)
- Edge browser artifacts are found under the IE database type. (5084)
  Workaround: Data is still parsed but is identified as IE data. Search the IE data for the Edge artifacts you are looking for.
- When pausing a job in the processing list, no other jobs will start processing (if they have not started already) until the paused job is resumed. (11216, 11217)
- Users with the Case Reviewer role are unable to browse PST folders from the Email Tab. (8430)
  Workaround: Add the following Case Rights to the Case Reviewer role: View Ignored Data, View Privileged Data. To do this, select Case Reviewer in the Define Roles dialog, check these two Case Rights and use the Save As button to save it as a new role.
- When importing data into KFF or Project VIC, you may get an error during the import.
  Workaround: Go to the KFF Hash Sets or Project VIC page, delete the hash set, and re-import it.

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 product download page:

http://accessdata.com/product-download

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://accessdata.com/product-download 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*.