AccessData AD Lab 6.2 Release Notes

Document Date: 4/3/2017

©2017 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

New and Improved in 6.2

The following items are new and improved for this release:

Enhanced Processing

- Distributed Processing Enhancements

  Users can now scale up their environments to handle more than 10 Distributed Processing Engines, doubling their recommended capacity.
- The Processing Manager (ProcessingHost.exe and Distributed Processing Manager) will now allow for updating the database more efficiently and increasing the threading capabilities.
- Mobile Application Parsing is now available for Facebook Messenger on the Android platform.
- Added support for Encrypted Messenger Plus! Log Files and Unencrypted iOS 10 Backups.
- Windows 10 Mail is now supported

  This support includes emails, attachments, and contacts.
- Processing has been updated to identify ELF, Mach-O, and CAF file types.

Automatic Parsing Updates for Modern Operating Systems

- Improvements to the recognition of Windows 8 and Windows 10 keyword searches

  These improvements include parsing searches conducted in both Windows 8 and Windows 10, parsing saved searches, identifying search terms that were used, and displaying date and time for each search.

- DestList Update

  This update includes the file launched, the path to the file, the number of times the file has been launched, whether the file has been pinned to the task bar, the issued entry ID number (a number assigned to the file based upon the order it was launched), how many files are being tracked, and how many ID's have been issued.

- Shell Bag Updates

  These improvements include Prefetch files, number of runtimes, and last runtimes.

- Prefetch Update

  This update includes last run time(s), showing a max of 8 run times within a cool html display.

- Volume Shadow Copy Update

  This update allows parsing of Volume Shadow Copy from Windows 8.1 or later and shows all restore points.

- SAM File Reference Update

  The following items are now included in the SAM File Key Properties: Given Name, Surname, UserPasswordHint, InternetUserName, InternetUID (this is the local ID for cloud storage).The SID unique identifier field name has also been updated to RID unique identifier. The Relative Identifier is the proper name for this ID field.

User Interface Updates

- FTK Lite

  There is a new, simplified FTK interface available for use with Lab. Intended for use when performing large scale reviews in AD LAB, the new template reduces the complexity of the AD LAB interface, allowing less skilled users to interface with the data.

- Baseline Forensic Processing Option

  The new default Baseline Forensic Processing option gives investigators a quick view into the data in the fastest way possible.

  Important: It is recommended that users perform multi-pass review and cull their data before expanding or carving items for their investigation.

- Email Threading Panel

  Users can now take advantage of the same email threading found in Summation and eDiscovery products.

- Geolocation Enhancements

  Users are now able to export KML and KMZ files, which will allow them to view geolocation data in any applications that allow KML imports. For example, Google Earth.

- People Finder

  Users can now scrape contact information from signatures in emails. Once a profile is created for the person of interest, investigators can use filters to search for data within the evidence. This allows investigators to pull contact information from disparate sets of evidence (laptop, mobile phone, email account) and connect information found in all items to one suspect. For example, investigators can pull contact information from an email signature, then filter based on the mobile phone number found there to connect phone calls, chats, or SMS communications to the same person of interest.

- Column Sorting for Case and User Administration

  This feature allows for sorting in the Administration screens, making it easier for clients to find users within a large number of investigators or to review users in the Administration screen.

Note: User and Group sorting is case sensitive since group names are case sensitive.

- Enhanced Active Directory Groups
  Administrators with LDAP turned on will have the ability to pull in Groups from Active Directory.

Deleted Partition Finder

We now support more types of partitions and in more scenarios.

- Both AT and GPT partitioning are now supported.

Save Properties Panel

Information from the Properties Panel can now be exported to either CSV or HTML formats. This functionality can be accessed by right-clicking anywhere in the Properties Panel.

Indexing Enhancements

Unchecked items in the compound file list will no longer index the entire object as a single object. To process these objects, check the compound file option and they will be expanded and indexed.

The following compound files will always be indexed and are exceptions to the rule:

- Chrome Bookmarks
- Chrome Cache
- Chrome SQLite
- EVT
- EVTX
- EXIF
- Firefox Cache
- Firefox SQLite
- IE Cookie Text
- IE Recovery
- IE WebCache
- Internet Explorer Files
- Skype SQLite
- SQLite Databases
- Windows Thumbnails

Enhanced Decryption Support

We have added enhanced support for the following:

- Bitlocker Decryption for Windows 10
- Mac Images Created with FileVault2
- Chrome Password Decryption
- FireFox Password Decryption

Updated Support for Agents

- Agent Support for MacOS 10.11 and 10.12
- Agent Support for Windows Server 2008 R2, 2012 R2, and 2016
- Agent Support for Windows 8, 8.1, and 10
- Agent Support for Linux (Red Hat up to 7)

Updated Install Support

We have added support for the following:

- Official Support for SQL 2014
- Official Support for Windows Server 2016
- Updated NSRL to version 2.54
- Updated Default Settings for SQL Server to improve performance

Removal of Support

- Proxy Agent
- MapQuest Geolocation
- Oracle Database

Support for Microsoft SQL Server

The following changes have been made for support of SQL Server for AD Lab:

- SQL Server 2008 R2 is no longer supported
- SQL Server 2014 is now supported

Updated Agent Modules and Agent Core

The agent has been updated.

Important: If you are upgrading to 6.2, the new agent modules will not run with the agent core from previous versions. When pushing 6.2 agents, you must also push both modules and core.

Removal of Agent Support

- Windows 2000
- Windows XP
- Windows Vista
- Mac OS 10.8 and below
- Solaris

Fixed Issues in 6.2

- Fixed the issue where review was defaulting to the Standard Viewer instead of Alternative, even when the Enable Standard Viewer option was not selected. (42550, 4310)

- The Additional Analysis KFF Group option was not processing the top item in the list if there was an item above the Default group. This has been fixed. (42937)
- Improved handling of nested zip files specifically crafted to crash software tools trying to expand them. (43629, 1080)
- Improved handling of exFAT timestamps reading the Timezone marker. (42459, 1123)
- Fixed an issue where in some instances the file size for some Mac OSX 10.11 native files were showing as 0k. (40374, 1139)
- Improved handling of OCR for Cyrillic (Russian) text. (40598, 1143)
- The Index Search tab now updates the email attachment pane. (42229, 1193)

  Important: There is one exception. If the user selects a hit, selects an attachment, then selects the same hit once more. In this case, the search file will not be reloaded.
- The issue preventing the addition of 3 Distributed Processing Engines has been fixed. (2299)
- The column named App Active Time has been updated to App Activation Time for disambiguation purposes. (3056)
- Mounting more than one device from a remote agent on Server 2016 will now trigger an error message instead of crashing if the mounting fails. (5490)
- Custom Data Views have been fixed to work with filters of bookmarked objects. (6533)
- Custom Case Identifiers no longer reappear after having been deleted. (6749)

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

- The FTK Suite (FTK, Lab, 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.

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)

Known Issues in 6.2

- 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)

New AD1 files and Imager 3.4.x

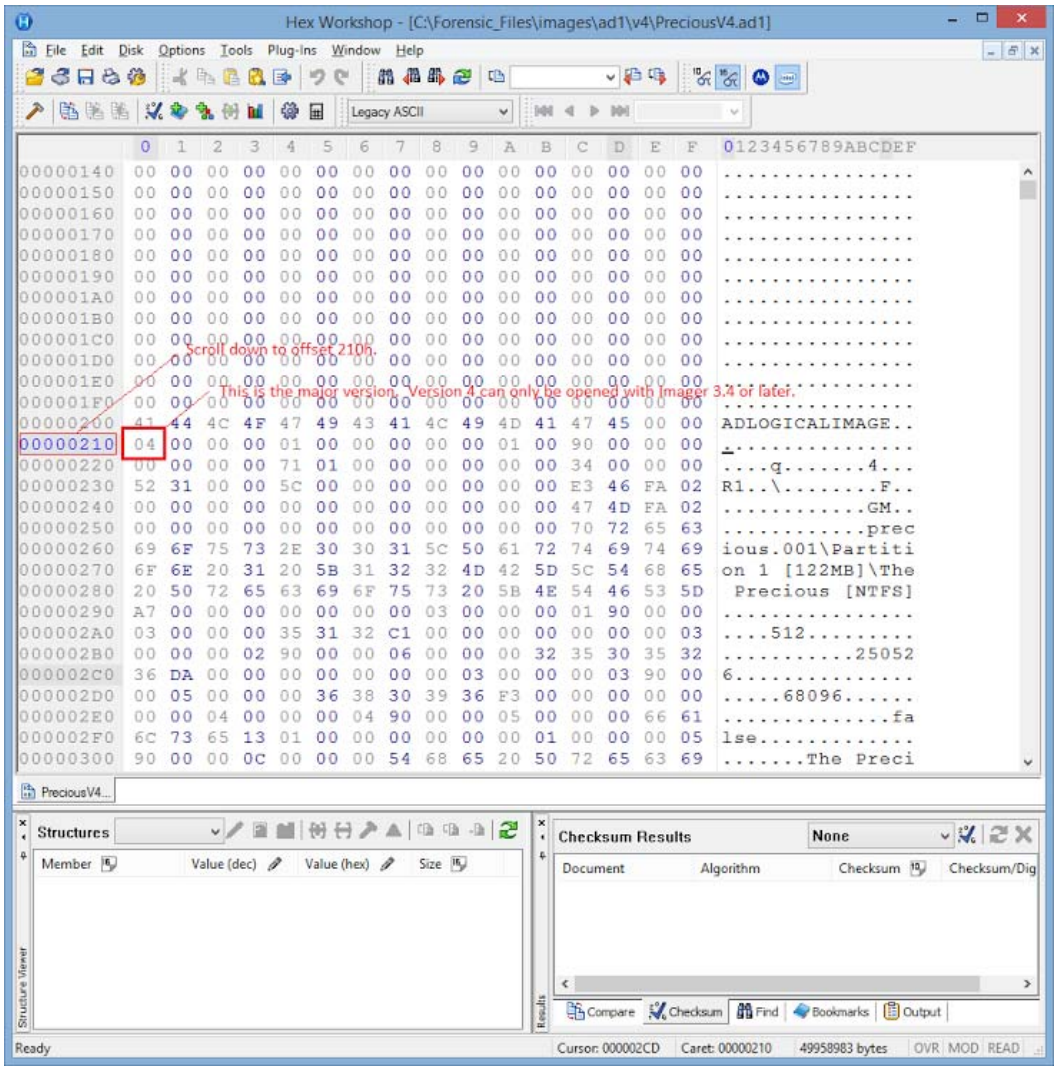
Any AD1 file created by FTK or Summation 6.0 or later can only be opened with Imager 3.4.0 or later.

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*.