AccessData AD Lab 6.1
Release Notes

Document Date: 10/18/2016

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 6.1

The following items are new and improved for this release:

Permissions/Groups/LDAP

- User groups have been added to FTK Lab. (27210)
- FTK Lab now also supports user management of logins and permissions via LDAP and Active Directory (AD). FTK Administrators can assign users to Lab by simply adding an LDAP/AD group. LDAP/AD users cannot log into Lab until a group in which they have membership has either a global or case role.
- Any group (LDAP or FTK admin-created) assigned to a case will give all members of that group access to the case. Users inherit any roles (and their associated permissions) assigned to any and all groups they are assigned to globally (in the Administer Groups dialog), regardless of which group is assigned to the case.
    - To manage a user’s permissions for all cases to which they are assigned, add roles to the group(s) they belong to in the Administer Groups dialog.
    - To manage a user’s permissions on a case-by-case basis, add roles to the group(s) they belong to when assigning a group a case. (In this case, it is advisable to not assign global roles to any group, except maybe a group intended for application administrators.)

Note: Remember that a user assigned to a case by any means inherits all roles assigned to any group of which they are a member.

Decryption

- FTK now supports Dell Data Protection | Encryption (DDPE) 9.2 Server; formerly called Credant. (33359)

Email

- FTK has added support for FlashMail. (36228)
- FoxMail is now supported. (40316)

Filters

- The following filter options have been added: (41965)
  - From Domain, From Address, From Display Name, To Domain, To Address, To Display Name, CC Domain, CC Address, CC Display Name, BCC Domain, BCC Address, BCC Display Name, To/CC/BCC Domain, To/CC/BCC Address, To/CC/BCC Display Name

Index Merge

- There are now dialogs for the index merge, alerting the user as to whether the merge is currently running or has run into an issue. (42294)

Fixed Issues in 6.1

The following issues have been fixed in this release:

Bookmarks

- Fixed the issue where the AppAdmin was unable to add items to another user's bookmark. (36912)
- Fixed an issue where FTK reports were including thumbnails for all bookmarked videos regardless of what was selected for the report. (40602)

Decryption

- Fixed the issue where, if using creddb.cef files, the Credant shield ID was not read correctly. (40520)

Email

- Improved the CoolHTML rendering of Chinese characters found within email. (35888)

Filters

- If you use two separate include filters and one is from the File Content tab and the other is from the Meta Info or MD5 tab, the non-File Content tab is now included. (41653)

Note: This issue did not occur if both properties were contained within a single filter.

Indexing

- There is no longer an error when trying to save a profile with the Include Extended Information in the Index option selected. (35010)
- Fixed the issue where running indexing for the first time in a case as an Additional Analysis job did not apply the same indexing options applied during initial case processing if indexing was selected there. (42286)

Index Merge

- Index merge has been improved and received a status bar. (39479)
- There is now an in-progress indicator for an index merge job, which can be found under Other Jobs in the progress window; there is also a notification dialog if an index merge runs into an issue. (39480)

KFF

- Fixed the issue where volatile data flagged as ignorable was left out of the case when the Include KFF Ignorabe Files option was selected. (39838)

UI

- Users are now prompted to save changes to bookmarks when going to the report dialog after modifying a bookmark. (36927)
- The content viewer now blocks all Javascript in MHT files from running. (38720)

XRY

- The XRY expansion feature has been updated to include XRY versions 6.15 and 6.16. (39476)

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

- If you use FTK, Lab, or Enterprise together with Summation or eDiscovery, DO NOT upgrade FTK to version 6.1 until you can upgrade the other products to version 6.1.
- 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.

Known Issues

- 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.

New AD1 files and Imager 3.4.x

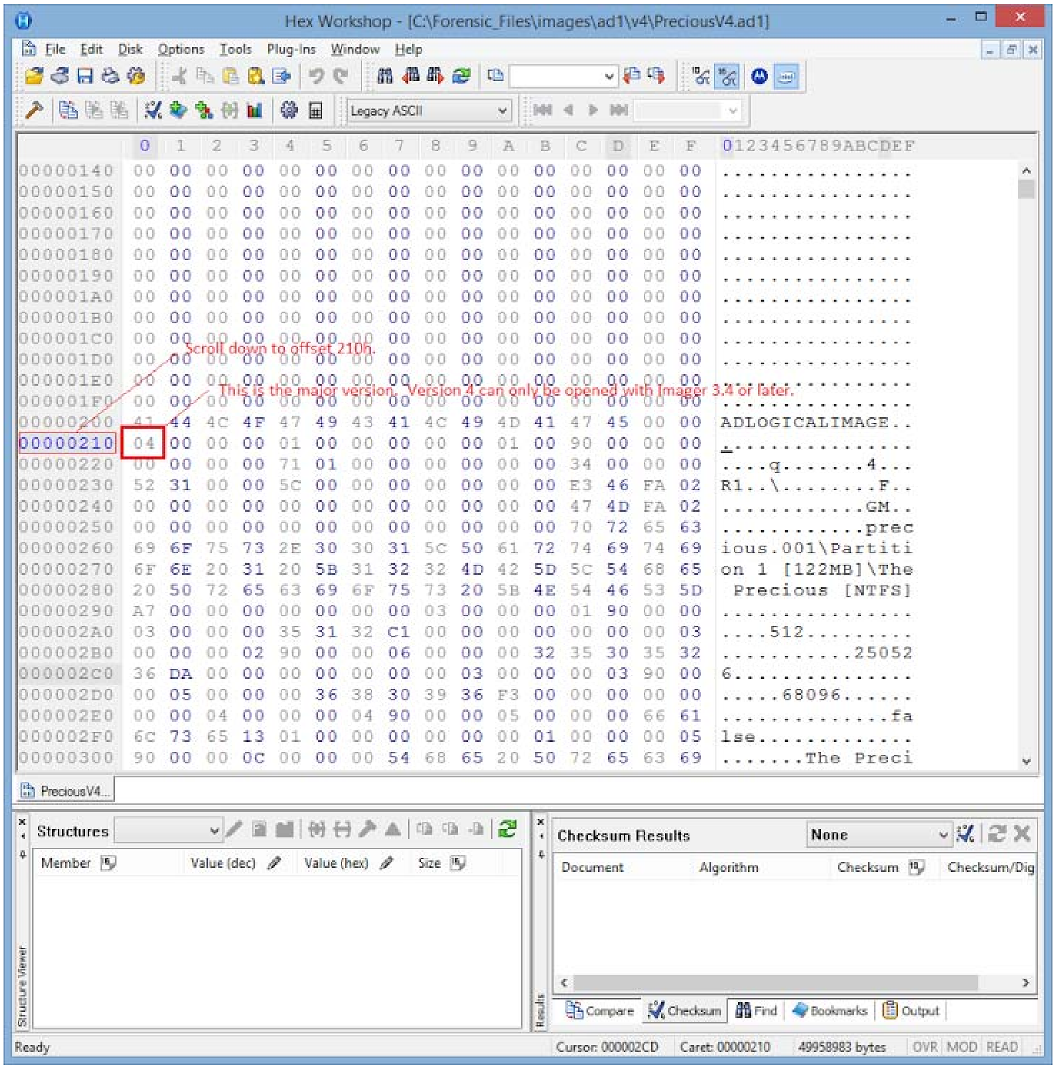
Any AD1 file created by FTK or Summation 6.0 or later can only be opened with Imager 3.4.0 or later.

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.



Hex Workshop - [C:\Forensic_Files\images\ad1\v4\PreciousV4.ad1]

```
          0  1  2  3  4  5  6  7  8  9  A  B  C  D  E  F  0123456789ABCDEF
00000140 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000150 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000160 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000170 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000180 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000190 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000001A0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000001B0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000001C0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000001D0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000001E0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000001F0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000200 41 44 4C 4F 47 49 43 41 4C 49 4D 41 47 45 00 00  ADLOGICALIMAGE..
00000210 04 00 00 00 01 00 00 00 00 00 01 00 90 00 00 00  ................
00000220 00 00 00 00 71 01 00 00 00 00 00 00 34 00 00 00  ....q.......4...
00000230 52 31 00 00 5C 00 00 00 00 00 00 00 E3 46 FA 02  R1..\........F..
00000240 00 00 00 00 00 00 00 00 00 00 00 00 47 4D FA 02  ............GM..
00000250 00 00 00 00 00 00 00 00 00 00 00 00 70 72 65 63  ............prec
00000260 69 6F 75 73 2E 30 30 31 5C 50 61 72 74 69 74 69  ious.001\Partiti
00000270 6F 6E 20 31 20 5B 31 32 32 4D 42 5D 5C 54 68 65  on 1 [122MB]\The
00000280 20 50 72 65 63 69 6F 75 73 20 5B 4E 54 46 53 5D   Precious [NTFS]
00000290 A7 00 00 00 00 00 00 00 03 00 00 00 01 90 00 00  ................
000002A0 03 00 00 00 35 31 32 C1 00 00 00 00 00 00 00 03  ....512.........
000002B0 00 00 00 02 90 00 00 06 00 00 00 32 35 30 35 32  ...........25052
000002C0 36 DA 00 00 00 00 00 00 00 03 00 00 00 03 90 00  6...............
000002D0 00 05 00 00 00 36 38 30 39 36 F3 00 00 00 00 00  .....68096......
000002E0 00 00 04 00 00 00 04 90 00 00 05 00 00 00 66 61  ..............fa
000002F0 6C 73 65 13 01 00 00 00 00 00 00 01 00 00 00 05  lse.............
00000300 90 00 00 0C 00 00 00 54 68 65 20 50 72 65 63 69  .......The Preci
```

Scroll down to offset 210h.

This is the major version. Version 4 can only be opened with Imager 3.4 or later.

Ready | Cursor: 000002CD | Caret: 00000210 | 49958983 bytes | OVR | MOD | READ

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*.