

# AccessData Forensic Toolkit 6.1 Release Notes

Document Date: 10/18/2016

©2016 AccessData Group, Inc. All rights reserved

## Introduction

---

This document lists the new features, fixed issues, and known issues for this version of Forensic Toolkit® (FTK®). 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 FTK 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:

### *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 Ignorable 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

- The User Guide is always being updated. For the latest FTK documentation, go to the following link:  
<http://www.accessdata.com/support/product-downloads/ftk-download-page>

## 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.
- For FTK installation and upgrade instructions, see the *FTK Quick Install Guide* and the detailed *FTK Installation Guide* which are available at  
<http://www.accessdata.com/support/product-downloads/ftk-download-page>
- FTK supports Distributed Processing Engines (DPEs).  
Before installing Distributed Processing, see the *Install Guide*.

## Upgrading CodeMeter

- FTK 5.6.1 and later include an updated version of CodeMeter Runtime Kit (5.21).
  - If this is a new installation of FTK you do not need to do anything and the latest version of CodeMeter is installed.
  - If you are upgrading to FTK 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 FTK 5.6.1, manually uninstall CodeMeter first and then install FTK 5.6.1 which will install a clean CodeMeter 5.21. Otherwise, after upgrading to FTK 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

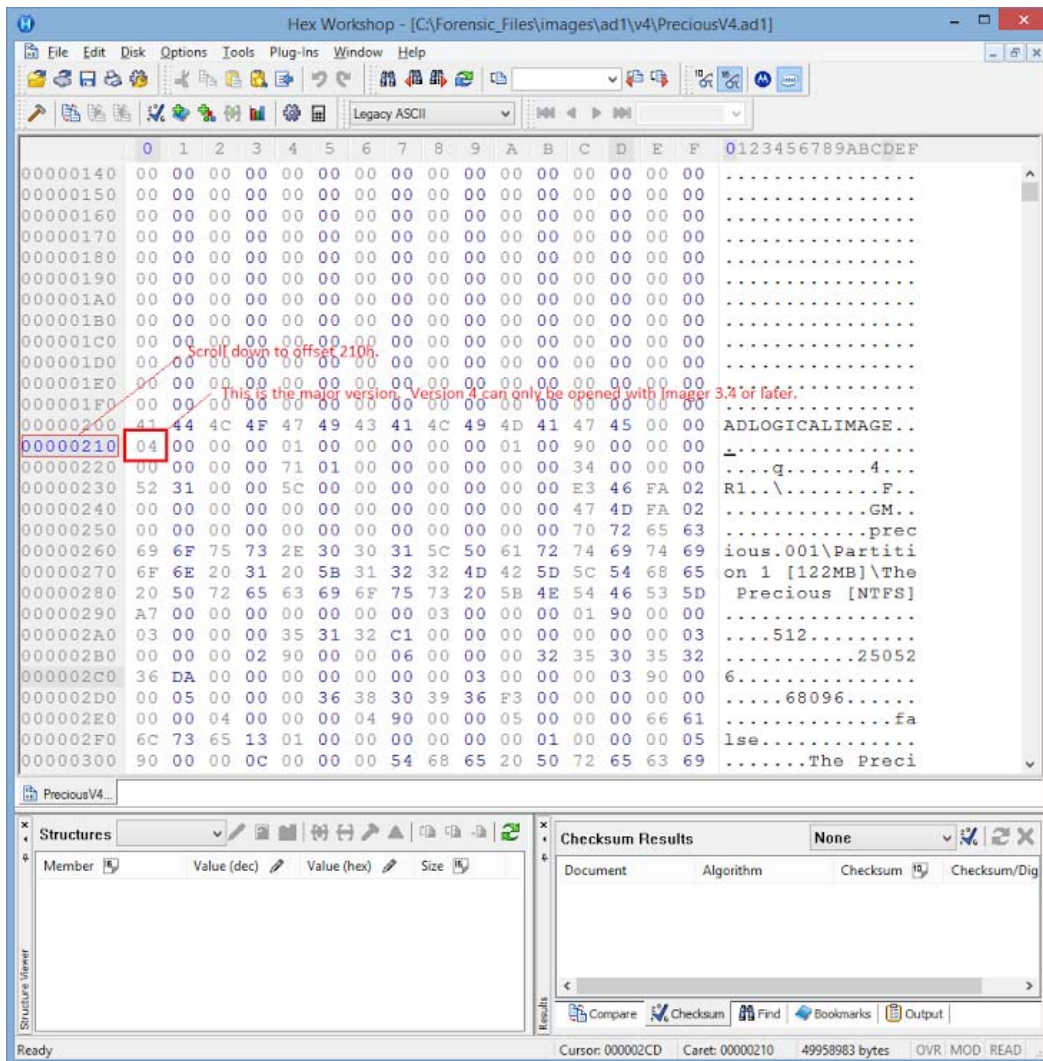
Any AD1 file created by FTK or Summation 6.0 or later can only be opened with Imager 3.4.0 or later.

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.



## 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 FTK.

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

## Comments?

---

We value all feedback from our customers. Please contact us at [support@accessdata.com](mailto:support@accessdata.com), or send documentation issues to [documentation@accessdata.com](mailto:documentation@accessdata.com).