AccessData Imager 4.1.1 Release Notes

Document Date: 7/19/2017

Introduction

This document lists the changes in this release of AccessData Imager. All known issues published with previous release notes still apply until they are listed under “Fixed Issues.”

Previous Releases

See AccessData Imager 3.4.3 Release Notes on page 5.

See AccessData Imager 3.4.2 Release Notes on page 6.

See AccessData Imager 3.4.1 Release Notes on page 9.

See AccessData Imager 3.4.0 Release Notes on page 10.

New Features, Updates, and Fixes in 4.1.1

- Application memory usage and stability has been improved.
- Improved handling of compressed files in HFS+ file systems. (1140)
- Improved handling of compressed files in Mac images. (6727/6729)
- Improved handling of deleted partitions in a GPT. (7030)
- The Export Hash List has been updated to better handle Chinese characters. (7364)
- Application Usage times for certain datetime files are displayed completely. (35526)
- Improved handling of AD1 files that have zip files within zip files. (2526)
- Improved stability when performing an Export File Hash List. (7887)
- Improved stability when adding evidence and browsing to a network location. (7887)

Important Things to Know - Imager 4.x

- Image mounting requires the latest Imager drivers be used on the computer. (58791)
  To ensure the latest drivers are used, complete the following steps:
  1. As administrator, open a command prompt, and execute the following commands:
     sc delete cbdisk
     sc delete cbdisk2
  2. Reboot the computer.
- FTK Imager does not have HPA or DCO support but can leverage technology (like some write-blockers) that make the information available during acquisition.
- When installing Imager, a prompt to install device software from the company *EldoS Corporation* appears. In order to complete the Imager install, you must select the option to *Always trust software from EldoS Corporation* and then click **Install**.

Version compatibilty

AccessData has produced a new AD1v4 image format that is different than the previous AD1v3 format. Older versions of AccessData products cannot recognize the new v4 format.

As a result, two versions of Imager are available to download and use:

- Imager 3.4.0
- Imager 3.4.2 (and later - 3.4.3, 4.1.1)

Use the following table to understand which products can use which AD1 format.

AD1 Image versions and supported applications

• Imager 3.4.1, 4.x, and later • FTK 6.0 and later • Summation 6.0 and later • eDiscovery 6.0 and later	• If you create an AD1 using one of these products, it is created only in the new v4 format. • These products can read either AD1v3 or AD1v4 image files.
• Imager 3.4.0	• This version can read either AD1v3 or AD1v4 files but creates only AD1v3 files. • Use this version when working with AD1 files for 5.x versions of FTK, Summation, or eDiscovery • You can use this version to open an AD1v4 file and save it as an AD1v3 file. (See below)
• FTK 5.x and earlier • Summation 5.x and earlier • eDiscovery 5.x and earlier • Imager 3.3.x and earlier	• These products can read only AD1v3 files. • These products can create only AD1v3 files.

Converting v4 image files to v3

It is important to note that AD1 files created in 6.x versions of FTK, Summation, or eDiscovery are the v4 format and cannot be read by 5.x versions and earlier of those products as well as Imager 3.3.x and earlier. Using an older version of Imager will result in an "Image detection failed" error.

However, you can open a v4 file in Imager 3.4.0 (only) and save it as a v3 file.

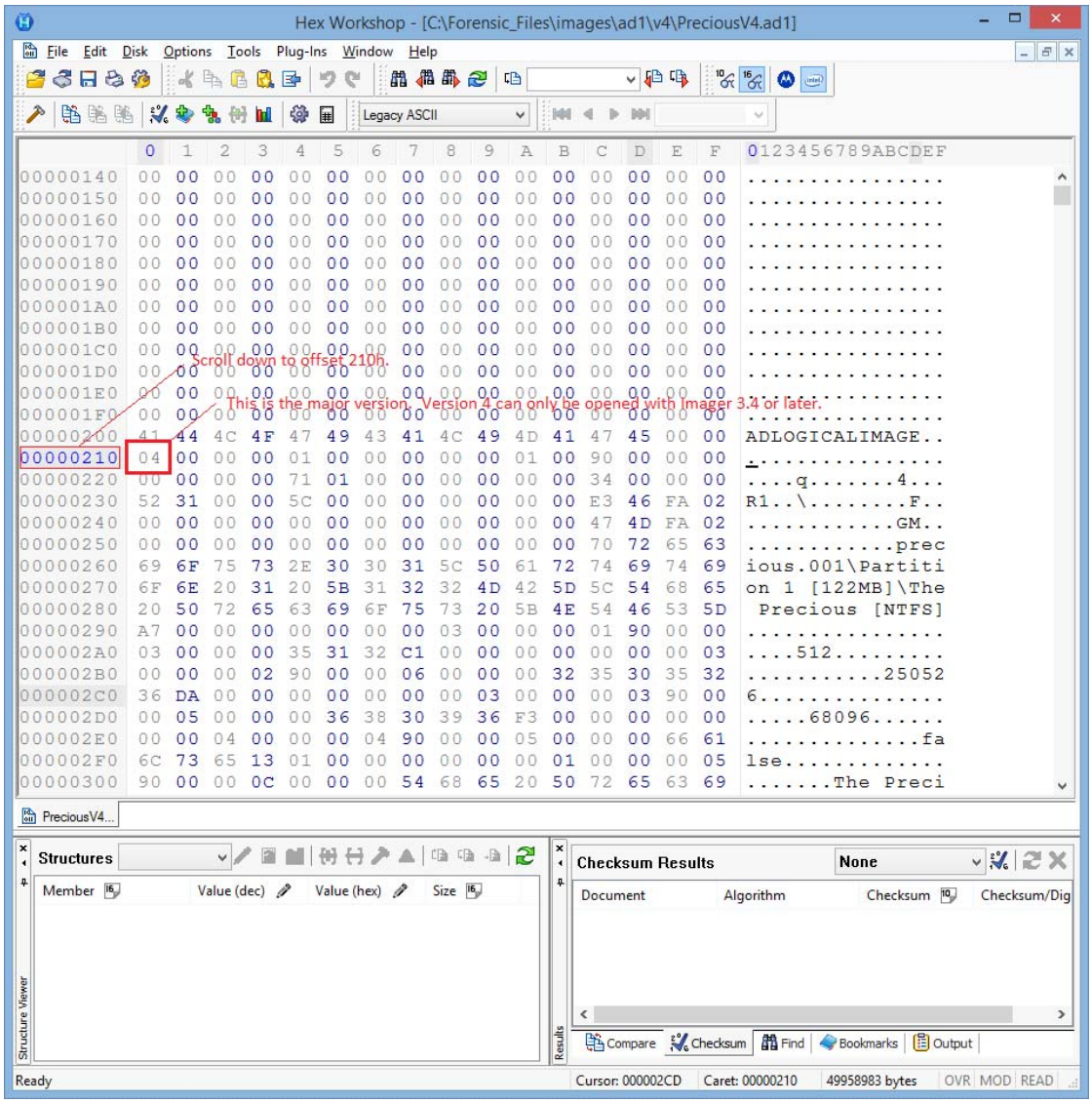
To use Imager 3.4.0 or 4.x to convert a v4 file to a v3 file, note the following:

- The verification hashes will be different because a v4 AD1 includes GUID tables that get hashed.
- To avoid having the top-level (filesystem) node's name changed, the AD1 should be created by doing the following:
  - Correct: **File** > **Create Disk Image** (follow wizard)
  - Incorrect: Add AD1, expand, right click on filesystem node in tree, Export Logical Image (AD1)

    Note: Note: An AD1 image is not really a disk image even though the option you use is *Create Disk Image*.

Determining the Version of an Image File

A hex editor can be used to quickly determine if your AD1 is v3 or v4.



Comments?

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

AccessData Imager 3.4.3 Release Notes

Document Date: 11/4/2016

Introduction

This document lists the changes in this release of AccessData Imager. All known issues published with previous release notes still apply until they are listed under “Fixed Issues.”

New Features and Updates

- Imager has been updated to not be susceptible to the following issue: http://www.kb.cert.org/vuls/id/707943.
  All DLLs are loaded securely.

Important Things to Know

See Important Things to Know - Imager 3.4.2 and later on page 6.

Comments?

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

AccessData Imager 3.4.2 Release Notes

Document Date: 3/29/2016

Introduction

This document lists the changes in this release of AccessData Imager. All known issues published with previous release notes still apply until they are listed under “Fixed Issues.”

New Features and Updates

- This version of Imager creates AD1s in a new AD1 v4 format, which is unreadable by FTK, Summation, or eDiscovery versions 5.6 and earlier.
  See Version compatibilty on page 7.
- Imager is now a 64-bit application.
- The installation files are signed with SHA-256.
- NTFS:
  - Support for more ACE/ACL types.
  - Fixed a divide by zero bug that sometimes caused a disk image to fail to process.
- FAT: Better support for deleted files with Unicode names.
- Fixed an issue that caused an infinite loop when processing Relatek zip files.
- AT/MBR partitioning: Fixed an issue that caused a handle extended partition boot record with invalid entry error. (TFS 31373)

Important Things to Know - Imager 3.4.2 and later

- Image mounting requires the latest Imager drivers be used on the computer. (58791)
  To ensure the latest drivers are used, complete the following steps:
  1. As administrator, open a command prompt, and execute the following commands:
     sc delete cbdisk
     sc delete cbdisk2
  2. Reboot the computer.

- FTK Imager does not have HPA or DCO support but can leverage technology (like some write-blockers) that make the information available during acquisition.
- When installing Imager, a prompt to install device software from the company *EldoS Corporation* appears. In order to complete the Imager install, you must select the option to *Always trust software from EldoS Corporation* and then click **Install**.

Version compatibilty

AccessData has produced a new AD1v4 image format that is different than the previous AD1v3 format. Older versions of AccessData products cannot recognize the new v4 format.

As a result, two versions of Imager are available to download and use:

- Imager 3.4.0
- Imager 3.4.2 (and later)

Use the following table to understand which products can use which AD1 format.

AD1 Image versions and supported applications

• Imager 3.4.1 and later • FTK 6.0 and later • Summation 6.0 and later • eDiscovery 6.0 and later	• If you create an AD1 using one of these products, it is created only in the new v4 format. • These products can read either AD1v3 or AD1v4 image files.
• Imager 3.4.0	• This version can read either AD1v3 or AD1v4 files but creates only AD1v3 files. • Use this version when working with AD1 files for 5.x versions of FTK, Summation, or eDiscovery • You can use this version to open an AD1v4 file and save it as an AD1v3 file. (See below)
• FTK 5.x and earlier • Summation 5.x and earlier • eDiscovery 5.x and earlier • Imager 3.3.x and earlier	• These products can read only AD1v3 files. • These products can create only AD1v3 files.

Converting v4 image files to v3

It is important to note that AD1 files created in 6.x versions of FTK, Summation, or eDiscovery are the v4 format and cannot be read by 5.x versions and earlier of those products as well as Imager 3.3.x and earlier. Using an older version of Imager will result in an "Image detection failed" error.

However, you can open a v4 file in Imager 3.4.0 (only) and save it as a v3 file.

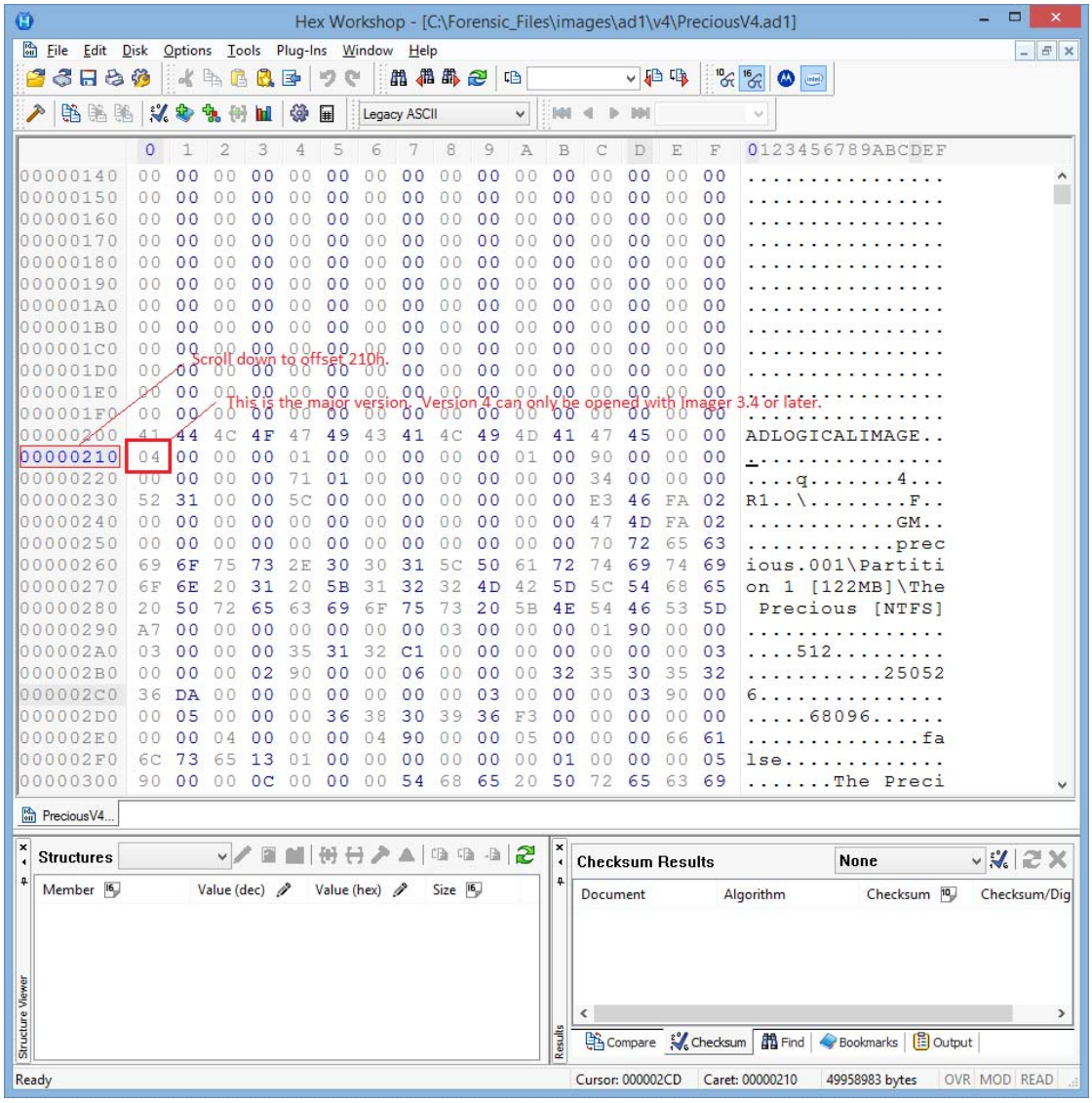
To use Imager 3.4.0 to convert a v4 file to a v3 file, note the following:

- The verification hashes will be different because a v4 AD1 includes GUID tables that get hashed.
- To avoid having the top-level (filesystem) node's name changed, the AD1 should be created by doing the following:
  - Correct: **File** > **Create Disk Image** (follow wizard)
  - Incorrect: Add AD1, expand, right click on filesystem node in tree, Export Logical Image (AD1)

    Note: Note: An AD1 image is not really a disk image even though the option you use is *Create Disk Image*.

Determining the Version of an Image File

A hex editor can be used to quickly determine if your AD1 is v3 or v4.



Comments?

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

AccessData Imager 3.4.1 Release Notes

Document Date: 9/22/2015

Introduction

This document lists the changes in this release of AccessData Imager. All known issues published with previous release notes still apply until they are listed under “Fixed Issues.”

Important Things to Know

- Image mounting requires the latest Imager drivers be used on the computer. (58791)
  To ensure the latest drivers are used, complete the following steps:
  1. As administrator, open a command prompt, and execute the following commands:
     sc delete cbdisk
     sc delete cbdisk2
  2. Reboot the computer.
- FTK Imager does not have HPA or DCO support but can leverage technology (like some write-blockers) that make the information available during acquisition.
- When installing Imager, a prompt to install device software from the company *EldoS Corporation* appears. In order to complete the Imager install, you must select the option to *Always trust software from EldoS Corporation* and then click **Install**.

New Features

- AD1 files are created in a new v4 format.
  See Version compatibilty on page 7.
- The installation files were rebuilt with an updated time stamp on the signature.

Comments?

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

AccessData Imager 3.4.0 Release Notes

Document Date: 4/08/2015

Introduction

This document lists the changes in AccessData Imager 3.4.0. All known issues published with previous release notes still apply until they are listed under “Fixed Issues.”

Important Things to Know

- Image mounting requires the latest Imager drivers be used on the computer. (58791)
  To ensure the latest drivers are used, complete the following steps:
  1. As administrator, open a command prompt, and execute the following commands:
     sc delete cbdisk
     sc delete cbdisk2
  2. Reboot the computer.
- FTK Imager does not have HPA or DCO support but can leverage technology (like some write-blockers) that make the information available during acquisition.
- When installing Imager, a prompt to install device software from the company *EldoS Corporation* appears. In order to complete the Imager install, you must select the option to *Always trust software from EldoS Corporation* and then click **Install**.

New Features

- AccessData Imager has been updated so that it can read AD1 files created by 6.x versions of FTK, Summation, and eDiscovery.

Comments?

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