AccessData Triage 2.4 Release Notes

Document Date: October 25, 2013
©2013 AccessData Group, Inc. All rights reserved

Introduction

These Release Notes cover important information, new features, and fixed issues for the AccessData Triage 2.4 release. Please be aware that all known issues published under previous release notes still apply until they are listed under "Fixed Issues."

Important Information

Triage Receiver Removal

The Triage Receiver has been removed from the current version of Triage. AccessData developed the Triage Receiver in order to export collected data from the target system to a designated location on the same network due to the size limitations of early USB drives. Since you can now export directly to a UNC path, and USB drives have a greater capacity for storage, there is no need to install the Triage Receiver.

Booting from ISO

In order to export, Triage must have a licensed device attached to the system running the agent, even when launching the agent from a cold boot directly from the disk.

Managing Multiple Profiles

If you have two different Triage devices attached to the system at the same time, switching between profiles will properly refresh the user interface.

New and Improved Features for 2.4

The following items are new and improved features or feature enhancements for this release.

For enhancements in the previous releases, see the following:

Data Collection

New Mobile Phone Profiles

You can now collect mobile phone data from a target computer with pre-defined mobile profiles. The following profiles are now available:

- Blackberry backup files - Allows you to collect from backup files associated with Blackberry devices.
- iDevice backup - Allows you to collect data from backup files associated with Apple products that use the "i" prefix in the product name, such as iPhone, iPod, and iPad.
- iOS pairing records - Allows you to collect files that will allow you to unlock the device using Mobile Phone Examiner Plus (MPE+).

   Note: You can add more than one mobile phone profile to a device for collecting.

Enhanced Path Filters

Enhanced file path filtering allows you to locate evidence more quickly and easily. With the enhanced file path filters, you can:

- Search for a specific file using 'Filename' criteria.
- Search a specific path for a specific file by combining 'Filename' and 'Path' criteria. For example, you can search for the path `com.apple.finder.plist` in every user's Preference's file and isolate one PLIST file from the evidence.

Faster Loading Time

- The Triage Agent's load time has decreased significantly.

User Interface Enhancements

New enhancements to the Triage interface provide greater usability. These changes include:

- A new column to the 'Restrict collection by user' list view on the *Profile* tab in Triage Agent's interface that shows the association between users and the system drive.
- The *Queue for Export* dialog (for exporting evidence manually) was streamlined and made more user-friendly.

Fixed Issues for 2.4

The following issues have been resolved for this release.

For fixed issues in the previous 2.x releases, see the following:

Data Collection

- The US Passport RegEx group now has a description attached to the group. (29864)
- There is no longer a 99 file segment limit for E01 and S01 files. (31973)
- Fixed the issue where the Triage agent was not displaying a drive that was mounted by FTK Imager. (17402)
- Fixed the issue where a memory warning occurred when calculating the size of an AD1 file in the Agent. (32348)
- The text of a document viewed in Natural view appears fully without truncation. (29375)
- You can now create images of CD/DVD drives. In previous versions of Triage, these images were corrupted. (15696)

Review

- You can now delete collections after they have been reviewed. (17589)

Comments?

AccessData values feedback from customers. Please contact us at support@accessdata.com, or send documentation issues to documentation@accessdata.com.

AccessData Triage 2.3 Release Notes

Document Date: August 26, 2013

Introduction

These Release Notes cover important information, new features, and fixed issues for the AccessData Triage 2.3 release. Please be aware that all known issues published under previous release notes still apply until they are listed under "Fixed Issues."

New and Improved Features for 2.3

The following items are new and improved features or feature enhancements for this release.

For enhancements in the previous releases, see the following:

General

Chinese Language Support

You can use Triage with a Chinese (Simplified) language interface. The Triage Admin and Receiver can be used directly with a Chinese language interface, and field agents may choose which language the user interface displays in when collecting. To use Triage with the Chinese language interface, click the *Language Selector* button in the *Autorun* menu. Install and run the Language Selector utility before installing the main program.

Data Collection

Custom Path Filtering

Custom path filtering for Macintosh OS has been improved.

Search

You now have the ability to use a non-standard alphabet character as a search term. You can search using characters from languages such as Chinese, Japanese, Arabic, and Welsh.

Fixed Issues for 2.3

The following issues have been resolved for this release.

For fixed issues in the previous 2.x releases, see the following:

General

- Fixed the issue where the client count would drop to zero on the dongle if the user refreshed his or her license dongle twice. (15160)

Data Collection

- Fixed the issue where Triage would crash when attempting to collect routing tables from a system that was disconnected from the network. (20601)

Known Issues for 2.3

The following are known issues for this release:

For known issues found in the previous 2.x releases, see the following:

General

- When selecting Chinese in the Language Selector utility, the user interface will not show that Triage is one of the products supported. This will not prevent the Language Selector from translating the Triage interface.

Data Collection

- The Triage agent cannot display a drive that is mounted by FTK Imager.

  Workaround: In the Browse System option, you can manually add the drive that has been mounted by Imager. (17402)

- If you attempt to perform a cold boot collection of a target machine using the Triage ISO and do not provide a Triage device with an associated profile, the option to add an export path will display an error and you will not be able to export a collection. (26740)

Comments?

AccessData values feedback from customers. Please contact us at support@accessdata.com, or send documentation issues to documentation@accessdata.com.

.

AccessData Triage 2.2.1 Release Notes

Document Date: June 28, 2013

Introduction

These Release Notes cover important information, new features, and bug fixes for the AccessData Triage 2.2.1 release. Please be aware that all known issues published under previous release notes still apply until they are listed under "Fixed Issues."

New and Improved Features for 2.2.1

The following items are new and improved features, or feature enhancements for this release.

For enhancements in the previous releases, see the following:

General

User Interface Changes

Triage's user interface has been modified to make creating collection devices easier and the system more intuitive to use.

Data Collection

Predefined Custom Profiles

Triage now comes with predefined custom profiles. You can select one or more predefined custom profile to apply to your collection device. These custom profiles can be edited and copied, and you can import and export the custom profiles. Available custom profiles include:

- Browser Artifacts: Capture Chrome, Firefox, and Internet Explorer artifacts.
- Clipboard and Screenshots: Capture any clipboard information and screenshots of all open windows. This is a live action.
- Created in the last week: Searches for files created in the last week.
- Encryption tools: Search for common encryption tools by keyword.
- Modified in the last week: Searches for files modified in the last week.
- Desktop Files: List of all files on any desktop.
- Documents: Searches for common document files, including DOC, DOCX, WPD, and ODT.
- Email - All: Searches for common email files, including DBS, Mbox, PST This does not collect OST files.
- Outlook Email: Searches for all PST and OST files.
- Incident Response - Quick Triage: Captures processes, network connections, IP addresses, DNS cache, and routing tables. This is a live action.
- Live System Info: Grab live system information, including DNS caches, remote shares, IP address, screenshots, USB devices, and user accounts.
- Mac or Linux Artifacts: Uses the Mac or Linux Bash history, Log and ETC filters.
- Network Info: Collects network information, including Domain System, Network Adapters, Routing Tables, ARP Tables, and IP Addresses.
- Pictures only: Searches for JPG, JPEG, BMP, PNG, TIF, GIF, PIC, and ICO.
- RAM and Pagefile Capture: Captures RAM and pagefile. This is a live action.
- Recents (LNK) Files. Captures a copy of the LNK files for recent files.
- Software Info: Lists Acrobat history, applications usage, installed software, manually launched apps, Microsoft Management usage, and Startup programs.
- Thumbs DB: Searches for all DB files.
- USB Device information: Captures information about any USB device previously plugged into the system.
- US Passport: A Regular Expression (RegEx) which searches for a 9 digit number.
- User Info: Collects owner information and SAM accounts.
- Video Files: Searches for common video files, including MP4 and AVI.
- Windows Artifacts: Lists all desktop items, LNK files and collect registry files.
- Windows EDB files: Collects all EDB files.
- Wiping Programs: Searches for common wiping programs by keyword search.

Predefined Custom Filters

Triage now comes with predefined custom filters. You can save a predefined custom filter to a profile. Custom filters can be edited, copied, imported, and exported. When you save changes to a custom filter, the interface will let other users know that the filter has been modified. Available custom filters include:

- Wiping Programs: Searches for names of common wiping programs.
- Encryption tools: Searches for names of common encryption programs.
- Common Video Files: Searches for common video files, including MP4 and AVI.
- Created in the last week: Searches for files created in the last week.
- Modified in the last week: Searches for files modified in the last week.
- Documents: Searches for common document files, including DOC, DOCX, WPD, and ODT.
- EDB files: Searches for all EDB files.

- Email - Common file: Searches for common email files, including DBS, Mbox, and PST. This filter does not search for OST files.
- Outlook Mail: Searches for all PST and OST files.
- Mac or Linux Bash History: Collects all .bash_history files.
- Mac or Linux Log files: Collects all /log files.
- Mac or Linux ETC files: Collects all /etc files.
- Pictures only: Searches for JPG, JPEG, BMP, PNG, TIF, GIF, PIC, and ICO.
- Thumbs DB: Searches for all DB files.
- US Passport: A regular expression (RegEx) that searches for a nine digit number.

Paths as Filters

You can now add a custom absolute path as a filter when doing a custom file search. This allows you to collect files that are in subfolders. For example, if you were collecting from a system with a top level folder named photos, with subfolders named utah, colorado, and new mexico, you could collect the whole folder by defining **photos** in the custom file filter. Or, if you want to collect only files from the new mexico folder, you could define the path as **photos/new mexico** in the custom file filter. This filter would only collect files from the new mexico subfolder.

Comments?

AccessData values feedback from customers. Please contact us at support@accessdata.com, or send documentation issues to documentation@accessdata.com.

AccessData Triage 2.2 Release Notes

Document Date: March 29, 2013

Introduction

These Release Notes cover important information, new features, and bug fixes for the AccessData Triage 2.2. release. Please be aware that all known issues published under previous release notes still apply until they are listed under "Fixed Issues."

New and Improved Features for 2.2

The following items are new and improved features, or feature enhancements for this release.

For enhancements in the previous releases, see the following:

Configuration

FTK Imager Support

Triage can now import FTK Imager generated hash lists and use them as hash groups. (6986)

Predefined RegEx Groups

Triage now comes with predefined regular expression (RegEx) groups. You can add RegEx groups when building custom filters. RegEx groups cannot be edited or deleted, but they can be copied and modified. Available predefined RegEx groups include:

- Credit card groups and credit card receipts. There are also groups for specific types of credit cards, such as American Express, Discover, MasterCard, and Visa.
- Domain name groups. In addition to a group for all domain names, there are specific groups for .com, .edu, .gov, .info, .museum, .net, .org, and .tv.
- Email groups. These groups include .com, .edu, .gov, .net, .org, and SMTP signatures.

- Unallocated space groups. These groups include INFO2 and Link file signatures.
- File sharing groups. These groups include Kazaa and Limewire.
- Internet address groups, such as IPv4 address and MAC Address.
- Orphaned index DAT files. These groups include files with date, files without date, cookie files, and history files.
- US and UK phone numbers.
- US Social Security number and US currency.
- The beginning of MSN Hotmail messages and the end of MSN Hotmail messages.
- Web searches. Search engine results include, Google, Ask Jeeves, eBay.com, AOL, and Mamma.com.
- URLs such as HTTP, HTTPS, FTP, and FTPS.

Data Collection

Mac and Linux Support

Triage now supports collecting from Mac and Linux systems when doing a cold boot using the Triage Agent.
- The Admin console for data collected from Mac and Linux must still be run in Windows.
- Actions specific to Windows are not available when running on Mac or Linux.
- Live mode collection for Mac and Linux is not currently supported. (3637)

Review

Native File Export from File Browser

You can now export a file to a disk from within the file browser. The selected file is written to the disk unencrypted and in its native format. (15782)

User Data

SAM (Security Accounts Manager) user information now includes password hashes if available. (10323)

Fixed Issues for 2.2

The following issues have been resolved for this release.
For fixed issues in the previous 2.x releases, see the following:

- A bzip2 file can now be expanded without producing an error. (14911)

| 11

- Returned data for the System Information action will appear correctly when performing a default boot collection. (7034)

- You can now export to a UNC path without producing an error. (15409)

- On a cold boot, the Agent now correctly displays predefined Export Options, such as Network Options or Triage Receiver Options. However, if the agent fails to connect and the predefined options fail to appear after twenty (20) seconds, you need to manually add the export options in the Agent. (15206)

- All timestamps are displayed as local time, unless labeled as a UTC or GMT timestamp in either the column header or in the actual timestamp. The one exception involves timestamps in a Custom File Search. These timestamps are dependent upon the type of file system that is being used. For example, NTFS file systems displays timestamps in UTC, but FAT32 file systems display timestamps in local time. (5743)

- When you perform a search with a custom profile, you can now stop the process before the profile has completed the search. (18303)

Known Issues for 2.2

The following are known issues for this release:

For known issues found in the previous 2.x releases, see the following:

- When browsing through file trees in reviewing a collection, the file tree list will collapse if you switch between **Explore** and **List** file trees. (6981)

- If you refresh your license dongle twice, the client count will drop to zero on the dongle, and you will be unable to create Triage devices. (15160)

    Workaround: Avoid refreshing the dongle more than once. If this occurs, contact support to add the correct client counts to the dongle.

Comments?

AccessData values feedback from customers. Please contact us at support@accessdata.com, or send documentation issues to documentation@accessdata.com.

AccessData Triage 2.1 Release Notes

Introduction

These Release Notes cover important information, new features, and bug fixes for the AccessData Triage 2.1 release. Please be aware that all known issues published under previous release notes still apply until they are listed under "Fixed Issues."

For your convenience, the previous versions of the release notes are included at the end of this document. See the following:

Important Information

When attempting to export a collection using a UNC path that is already mapped on the computer in use (i.e. \\servername\directory), Triage might display an error. If this occurs, disconnect the mapped drive before continuing. Once Triage has finished its collection, you can re-map the drive.

New and Improved Features for 2.1

The following items are new and improved features, or feature enhancements for this release.

For enhancements in the previous releases, see the following:

Select Profile Option (Kiosk Mode)

During evidence collection, a new pop-up window displays if multiple profiles are saved onto the device. The investigator can then select the correct profile from a list of available profiles (for example, Profile A Images, Profile B Volatile Data Capture, etc.).

PDF Viewer

You can now view PDF files in Natural view in addition to hex values. PDF files display in the review in both the Agent and Admin interfaces. If a PDF file does not have the .pdf extension, it will display as a raw stream.

Data Collection

The following data can be collected from the target system:

- Screenshots of individual windows on the target machine, including windows that have been minimized, moved off screen, or are "invisible" (such as windows that are running background processes).
  - Data is collected in live mode only.
  - Some transparent windows may render as solid black or white. Windows may also display with overlapped content or transparent borders.
- Additional data from USB devices.
  - Date when the USB device was first seen by the operating system (localtime).
  - Date when the associated volume was last mounted.
  - The user that mounted the drive.
  - Known drive letters associated with the drive.
  - Known volumes associated with the device. (This is available on Windows 7 and Vista only.)
- DNS cache data from the system.
  - Data is collected in live mode only.

Expanded Export Options

You can now set the target export destination when creating a Triage device.

- Administrators have the ability to validate UNC credentials before creating a Triage device.
- UNC and Receiver targets can be specified in two locations: in the Admin console during the Triage device creation process and in the Agent from the Evidence window.

USB 3.0 Device Support

Triage follows the USB 3.0 standard and can read and write to USB 3.0 devices. This allows Triage to take advantage of USB 3.0's faster transfer rates.

Fixed Issues for 2.1

The following issues have been resolved for this release.
For fixed issues in the previous 2.x releases, see the following:

| 14

- Fixed the issue where the collection list in Manage Triage Devices failed to update when a drive with no collections was selected. (10556)
- Fixed the issue where a user was unable to navigate to a recently exported collection when the collection was exported with a UNC path. (13913)
- Fixed the issue that occurred when performing a collection using the "Users Home Directory" default filter and the Explore node would fail to appear. (9805)
- Fixed the issue where Triage did not display the correct data size for logical data queued for export. (7812)
- Clarified terminology in the Admin user interface so that the wording is consistent throughout the user interface. (13895)
- Fixed the issue where an error would post when the user ran Triage with a virtual Codemeter. (14603)

Known Issues for 2.1

The following are known issues for this release:

For known issues found in the previous 2.x releases, see the following:

Known Issues for 2.0 (page 19)

- A user may experience difficulty when attempting to expand a BZip2/BZ2 file. (14911)
- In some cases, when upgrading from Triage 1.x to 2.x, the license count in the Admin console will show '0.'
  Workaround: Call support and they will refresh your counts.
- A user may be unable to export to a network location (i.e. \\servername\directory) which is already mapped to a local drive. (13857)
  Workaround: Disconnect the mapped drive in Windows, configure the Triage Export option, and execute your collection. When the collection is finished, you can re-map your network drive in Windows.
- Upon a cold boot, the Agent may not display the predefined Export Options (i.e., Network Options or Triage Receiver options).
  Workaround: Manually add the export options in the Agent under the Evidence tab > Export Options.

Comments?

AccessData values feedback from customers. Please contact us at support@accessdata.com, or send documentation issues to documentation@accessdata.com.

AccessData Triage 2.0 Release Notes

Introduction

These Release Notes cover important information, new features, and bug fixes for the AccessData Triage 2.0 release. Please be aware that all known issues published under previous release notes still apply until they are listed under "Fixed Issues."

Important Information for 2.0

Triage 2.0 does not have backwards compatibility with earlier versions of Triage. However, 2.0 may be installed in tandem with 1.x versions on the same system, because the 2.0 version uses a separate database from 1.x.

New and Improved Features for 2.0

Ability to Expand, Search, and Extract from Compound Files/ Archives

You can now collect more information from the investigated system:

- Using the Agent file system browser, a user can navigate through the archives and choose to save files within the archives.
- Triage now has the ability to expand compound files (archives) during search and filter operations.
- If you choose to Enable Archive Expansion during device creation and you select to save the entire archive within file system browser, Triage will only export out of the child item, not the root archive. To save the root archive, a user should not enable archive expansion during device creation.

Enhanced Search

- Search text is no longer case sensitive when you search for terms while reviewing data in the Triage Admin interface. This allows you to get more results on your searches.
- New filtered keyword support allows you to search files for keywords and values, similar to using the native application.

- All files are now searched from a binary and filtered text perspective.

Updated Email Search and Export

When an email or an email attachment within an email archive matches the search criteria, the email message and its attachments will be collected as an MSG per responsive message.

Detect Encrypted Devices and Partitions

Triage now searches for encrypted drives before you start a collection. You will receive a notification of encrypted drives/devices/partitions/volumes detected with the following types of encryption:

- Safeguard (Utimaco)
- Safeguard Enterprise (Utimaco)
- PGP
- McAfee Safeboot
- Guardian Edge
- Point Sec
- Bitlocker (Vista only)

Prevent File System Browsing

You now have the option to prevent the investigator from browsing the file system during collection. This is a per device option, so you can enable this option when you create a Custom Triage Device.

Multiple Profiles Support

You now have the ability to save multiple profiles on a single device. When you execute Triage on a target, you can choose which profile to run.

Custom File Filter Columns

Columns for Keyword List and Explicit Image Detection (EID) have been added to the Custom File Search tab of the review. This allows you to quickly find files that were flagged for Keyword or EID matches when reviewing collected data.

Core Code Improvements

Updates to the core code allow Triage to operate with greater accuracy for filtering, and to use memory more efficiently.

- File pointers are stored in memory instead of whole files.
- Triage leverages the same agent code for filtering and searching.

Compatibility with other AccessData Products

Triage's image evidence that's encrypted with a user supplied password is now compatible with other AccessData products, such as Imager. This feature is not in the international version.

Expanded Support with Triage Receiver

- Triage Receiver now supports multiple concurrent connections.
- Triage Receiver now supports IPv6 (Internet Protocol Version 6).
- Triage Receiver now supports encrypted communication with Triage Agent (not in the international version).

Updated SQLite Parser

An updated SQLite engine allows you to open newer versions of SQLite, including Firefox databases.

Fixed Issues for 2.0

- Fixed the issue where running multiple searches while reviewing a collection resulted in incorrect search results. (6970)
- Fixed the issue where deselecting a checked option in the Custom Filter Wizard did not remove the option from the filter as expected. (7042)
- Fixed the issue where the search field was active when a parent node was selected when reviewing a collection. (7287)
- Added a dialog box to warn the user that a device was being overwritten.
- Fixed the issue with the autorun executable. (8754)
- Fixed the issue where attempting to collect twice in the same day, on the same computer, using the same profile would overwrite the first collection, rather than creating a second collection. (62063) (58138)
- Fixed the issue where a user could not retrieve an image from a device that was created on a different Admin computer unless the device has a password. (63511)
- Fixed the issue where collecting to the receiver from an IP more than once per day would overwrite data each time it was collected. (63746)
- Fixed the issue where physical images that were acquired manually could not be reported on or reviewed in the Admin console. (63635)
- Fixed the issue where stopping a physical export of an E01 or S01 will cause an error to appear on the Receiver. (61633)
- Fixed the issue where if the USB is booted on a target device, then switched to another USB once the agent is open, Triage would not recognize the profile of the new USB. (61545)
- Fixed the issue where only one physical collection could be done per instance of opening the agent. (58478)
- Fixed the issue where failure to select a profile in the Manage Triage Devices dialog, when saving a collection, produces the message, "collection has already been saved," rather than, "no selections were made." (56294)

- Fixed the issue where if the Triage Admin machine had multiple partitions, the partitions would appear in the devices list on the Manage Licenses dialog. (56612)

- Fixed the issue where clipboard data collected from a live machine and reviewed in the Recover Evidence dialog might appear multiple times in the review. (58416)

- The user interface was changed to avoid confusion when recovering a remote collection. (58414)

- Fixed the issue where when a collection was stored on a removable device, the collection can only be viewed in the Admin console in the device was connected to computer. (58347)

- Fixed the issue where including a forward or back slash in the name of a profile would cause report generation to fail. (58402)

- Fixed the issue where the Triage profile collecting keyword only group was not finding DOCX, PPTX, PDF, or XLSX files containing known keywords. (55210)

- Fixed the issue where history filtering in the Manage Saved Collections dialog had to be an exact match to find metadata. (56291)

- It is now possible to cancel a collection during Custom File Search without having to wait for search to complete. (6972)

- Now you are able to query a remote receiver, even if it is in use. (7023)

- Fixed the issue where stopping a collection on a cold booted machine took an extended period of time just to stop collecting. (6972)

- Fixed the issue where deleted files show up in reports with an incorrect date. (6988)

- Fixed the issue where disabling the default options when making a custom profile did not remain disabled if you moved forward and then back again in the wizard. (7009)

Known Issues for 2.0

- Timestamps displayed in Triage are a mixture of local time and UTC time. (5743)

- Exports to the Receiver using IPv6 may fail in some cases, but not all. (8034)

- When importing a large file, the progress bar will sit at 0% progress. Once the collection has been imported, the progress window will update and show 100% progress. (7066)

- Filters are not getting connected by an OR. All the criteria from all filters are aggregated and then connected by an AND. Workaround: To run an OR search, use multiple profiles on a device, instead of multiple filters in one profile. Note: Each profile must be run one at a time, per instance of the Agent, or else data will be overwritten. (9814)

- When you perform a collection using the "Users Home Directory" default filter, the results do not show an Explore node as a way to view evidence; only a List node is available. (9805)

- When browsing a system to manually collect items, the Expand Compound Files setting in the device creation step has the following behavior: when checked, files or emails within archive files can be collected individually, but the archive file cannot be collected. When unchecked, items within an archive cannot be viewed or collected, but the archive file can be collected. (10992)

Comments?

AccessData values feedback from customers. Please contact us at support@accessdata.com, or send documentation issues to documentation@accessdata.com.