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.”

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

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

- 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

- 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

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

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

- 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

- 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.