AccessData

Triage

User Guide

AccessData®
A Pioneer in Digital Investigations Since 1987

AccessData Legal and Contact Information

Document date: October 16, 2013

Legal Information

AccessData Group, LLC makes no representations or warranties with respect to the contents or use of this documentation, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, AccessData Group, LLC reserves the right to revise this publication and to make changes to its content, at any time, without obligation to notify any person or entity of such revisions or changes.

Further, AccessData Group, LLC makes no representations or warranties with respect to any software, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, AccessData Group, LLC reserves the right to make changes to any and all parts of AccessData software, at any time, without any obligation to notify any person or entity of such changes.

You may not export or re-export this product in violation of any applicable laws or regulations including, without limitation, U.S. export regulations or the laws of the country in which you reside.

AccessData Group, LLC.
588 West 400 South
Suite 350
Lindon, Utah 84042
U.S.A.

www.accessdata.com

AccessData Trademarks and Copyright Information

- AccessData® is a registered trademark of AccessData Group, LLC.
- Distributed Network Attack® is a registered trademark of AccessData Group, LLC.
- DNA® is a registered trademark of AccessData Group, LLC.
- Forensic Toolkit® is a registered trademark of AccessData Group, LLC.
- FTK® is a registered trademark of AccessData Group, LLC.
- Password Recovery Toolkit® is a registered trademark of AccessData Group, LLC.
- PRTK® is a registered trademark of AccessData Group, LLC.

- Registry Viewer® is a registered trademark of AccessData Group, LLC.

A trademark symbol (®, ™, etc.) denotes an AccessData Group, LLC. trademark. With few exceptions, and unless otherwise notated, all third-party product names are spelled and capitalized the same way the owner spells and capitalizes its product name. Third-party trademarks and copyrights are the property of the trademark and copyright holders. AccessData claims no responsibility for the function or performance of third-party products.

Third party acknowledgements:

- FreeBSD ® Copyright 1992-2011. The FreeBSD Project .
- AFF® and AFFLIB® Copyright® 2005, 2006, 2007, 2008 Simson L. Garfinkel and Basis Technology Corp. All rights reserved.
- Copyright © 2005 - 2009 Ayende Rahien

Documentation Conventions

In AccessData documentation, a number of text variations are used to indicate meanings or actions. For example, a greater-than symbol (>) is used to separate actions within a step. Where an entry must be typed in using the keyboard, the variable data is set apart using [*variable_data*] format. Steps that required the user to click on a button or icon are indicated by **Bolded text**. This *Italic* font indicates a label or non-interactive item in the user interface.

A trademark symbol (®, ™, etc.) denotes an AccessData Group, LLC. trademark. Unless otherwise notated, all third-party product names are spelled and capitalized the same way the owner spells and capitalizes its product name. Third-party trademarks and copyrights are the property of the trademark and copyright holders. AccessData claims no responsibility for the function or performance of third-party products.

Registration

The AccessData product registration is done at AccessData after a purchase is made, and before the product is shipped. The licenses are bound to either a USB security device, or a Virtual CmStick, according to your purchase.

Subscriptions

AccessData provides a one-year licensing subscription with all new product purchases. The subscription allows you to access technical support, and to download and install the latest releases for your licensed products during the active license period.

Following the initial licensing period, a subscription renewal is required annually for continued support and for updating your products. You can renew your subscriptions through your AccessData Sales Representative.

Use LicenseManager to view your current registration information, to check for product updates and to download the latest product versions, where they are available for download. You can also visit our web site, www.accessdata.com anytime to find the latest releases of our products.

For more information, see Managing Licenses in your product manual or on the AccessData web site.

AccessData Contact Information

Your AccessData Sales Representative is your main contact with AccessData Group, LLC. Also, listed below are the general AccessData telephone number and mailing address, and telephone numbers for contacting individual departments.

Mailing Address and General Phone Numbers

You can contact AccessData in the following ways:

AD Mailing Address, Hours, and Department Phone Numbers

Corporate Headquarters:	AccessData Group, LLC. 588 West 400 South Suite 350 Lindon, UT 84042 USA *Voice*: 801.377.5410 *Fax*: 801.377.5426
General Corporate Hours:	Monday through Friday, 8:00 AM – 5:00 PM (MST) AccessData is closed on US Federal Holidays
State and Local Law Enforcement Sales:	*Voice*: 800.574.5199, option 1 *Fax*: 801.765.4370 *Email*: Sales@AccessData.com
Federal Sales:	*Voice*: 800.574.5199, option 2 *Fax*: 801.765.4370 *Email*: Sales@AccessData.com
Corporate Sales:	*Voice*: 801.377.5410, option 3 *Fax*: 801.765.4370 *Email*: Sales@AccessData.com
Training:	*Voice*: 801.377.5410, option 6 *Fax*: 801.765.4370 *Email*: Training@AccessData.com
Accounting:	*Voice*: 801.377.5410, option 4

Technical Support

Free technical support is available on all currently licensed AccessData products.
You can contact AccessData Customer and Technical Support in the following ways:

AD Customer & Technical Support Contact Information

Domestic Support Americas/Asia-Pacific	
Standard Support:	Monday through Friday, 5:00 AM – 6:00 PM (MST), except corporate holidays. *Voice*: 801.377.5410, option 5 *Voice*: 800.658.5199 (Toll-free North America) *Email*: Support@AccessData.com

AD Customer & Technical Support Contact Information (Continued)

After Hours Phone Support:	Monday through Friday 6:00 PM to 1:00 AM (MST), except corporate holidays. *Voice*: 801.377.5410, option 5
After Hours Email-only Support:	Monday through Friday 1:00 AM to 5:00 AM (MST), except corporate holidays. *Email*: afterhours@accessdata.com
International Support Europe/Middle East/Africa	
Standard Support:	Monday through Friday, 8:00 AM – 5:00 PM (UK-London), except corporate holidays. *Voice*: +44 207 160 2017 (United Kingdom) *Email*: emeasupport@accessdata.com
After Hours Support:	Monday through Friday, 5:00 PM to 1:00 AM (UK/London), except corporate holidays. *Voice*: 801.377.5410 Option 5*.
After Hours Email-only Support:	Monday through Friday, 1:00 AM to 5:00 AM (UK/London), except corporate holidays. *Email*: afterhours@accessdata.com
Other	
Web Site:	http://www.AccessData.com/Support
	The Support web site allows access to Discussion Forums, Downloads, Previous Releases, our Knowledgebase, a way to submit and track your “trouble tickets”, and in-depth contact information.
AD SUMMATION	Americas/Asia-Pacific: 800.786.2778 (North America). 415.659.0105. Email: support@summation.com
Standard Support:	Monday through Friday, 6:00 AM– 6:00 PM (PST), except corporate holidays.
After Hours Support:	Monday through Friday by calling 415.659.0105.
After Hours Email-only Support:	Between 12am and 4am (PST) Product Support is available only by email at afterhours@accessdata.com.
AD Summation CaseVault	866.278.2858 Email: support@casevault.com
	Monday through Friday, 8:00 AM – 6:00 PM (EST), except corporate holidays.
AD Summation Discovery Cracker	866.833.5377 Email: dcsupport@accessdata.com
Support Hours:	Monday through Friday, 7:00 AM – 7:00 PM (EST, except corporate holidays.

Note: All support inquiries are typically responded to within one business day. If there is an urgent need for support, contact AccessData by phone during normal business hours.

Documentation

Please email AccessData regarding any typos, inaccuracies, or other problems you find with the documentation: *documentation@accessdata.com*

Professional Services

The AccessData Professional Services staff comes with a varied and extensive background in digital investigations including law enforcement, counter-intelligence, and corporate security. Their collective experience in working with both government and commercial entities, as well as in providing expert testimony, enables them to provide a full range of computer forensic and eDiscovery services.

At this time, Professional Services provides support for sales, installation, training, and utilization of FTK, FTK Pro, Enterprise, eDiscovery, and Lab. They can help you resolve any questions or problems you may have regarding these products

Contact Information for Professional Services

Contact AccessData Professional Services in the following ways:

AccessData Professional Services Contact Information

Contact Method	Number or Address
Phone	Washington DC: 410.703.9237
	North America: 801.377.5410
	North America Toll Free: 800-489-5199, option 7
	International: +1.801.377.5410
Email	*adservices@accessdata.com*

Table of Contents

Chapter 1

Introduction

About AD Triage

AD Triage is designed to collect and review data/artifacts from a live or powered down target system and facilitate the transfer of that data to an administrator system. An AD1 logical image of the system's artifacts can then be written to the destination of your choice. From there, the data can be decrypted and imported into the administrator's interface for further review and reporting or can be consumed by FTK for more advanced analysis.

Components of AD Triage

AD Triage is made up of two interfaces, the *Admin* interface, and the *Collection* interface. The *Admin* interface is what you install on your machine. You will use this interface to review and store all the data that you collect.

The *Collection* interface is what you boot to on the target system. You can use this interface to collect and export data to a USB device or a specified computer on the same network as the target system.

Launching AD Triage Admin

To launch AD Triage Admin

- ❖ Do one of the following:
  - Select **Start > Programs > AccessData > Triage > Triage Admin**.
  - Click the **AD Triage** button on the desktop 

. The *Triage Admin* window opens.

Chapter 2
Installation

This chapter contains all the information you need to install AD Triage. The Triage Admin console is installed separately.

Prerequisites

Before you install AD Triage, you must have the following items:

- A CodeMeter dongle that is licensed for AD Triage.
  See Appendix A Managing Security Devices and Licenses on page 106.
- CodeMeter Runtime 4.5 installed on your system
- Microsoft .NET 4.0.

Software Requirements

To run AD Triage, in addition to the hardware requirements, you need the following:

- An additional license with separate installation.
- Microsoft Windows OS platform on which AD Triage operates as a standalone product.
- AccessData FTK installed on your machine (if you intend to add the imaged data to a case for further investigation).

Note: Triage 2.x versions do not have backwards compatibility with earlier versions of Triage. However, 2.x versions may be installed in tandem with 1.x versions on the same system, because the 2.x versions use a separate database from 1.x.

Images created by AD Triage are AccessData-proprietary AD1-type images. AD1 images can be imported back into AD Triage, and can be added as evidence to a case in any AD FTK-core product.

Hardware Requirements

AD Triage requires the following additional hardware:

- USB ports on your machine.
- CodeMeter USB or Virtual CmStick (with current licenses installed).
- A USB device for each profile you create in AD Triage.

Installing AD Triage Admin Console

To install AD Triage Admin Console

1. Insert installation disk into the CD/DVD drive.
2. At the **Autorun** screen, click **Install Triage Admin**.
3. In the *ADTriage Setup* window, click **Next**.
4. In the *End-User License Agreement* window, check the **I accept the terms in the License Agreement** and click **Next**.

Select Installation Folder Screen

5. In the *Destination Folder* window, browse to the location where you want to save your program files.
6. Check **Create a shortcut for this program on the desktop** if you want a Triage icon on your desktop, and click **Next**.
7. At the *Ready to Install AccessData Triage* window, click **Install** to begin the installation.
8. Click **Finish** to close the installation wizard.

Language Selector

To change to another supported language other than the default English (United States) that ships with Triage, Language Selector must be installed.

Installing Language Selector

To install Language Selector

1. At the **Autorun** screen, click **Language Selector**.
2. The Language Selector Installer runs. Click **Next** to continue.
3. Read and accept the License Agreement. Click **Next** to continue.
4. Click **Finish.**

Using Language Selector

To run Language Selector

1. Do one of the following:
   - Click **Start > All Programs > AccessData > Language Selector >Language Selector**.
   - Click the Language Selector Icon on your desktop.
2. Click the **Select Languages** drop-down to select the language to use. The languages supported by Triage are English (American) and Chinese (Simplified).
3. Click **Save Settings** to save selections and close the Language Selector.

Chapter 3

Setting up Profiles

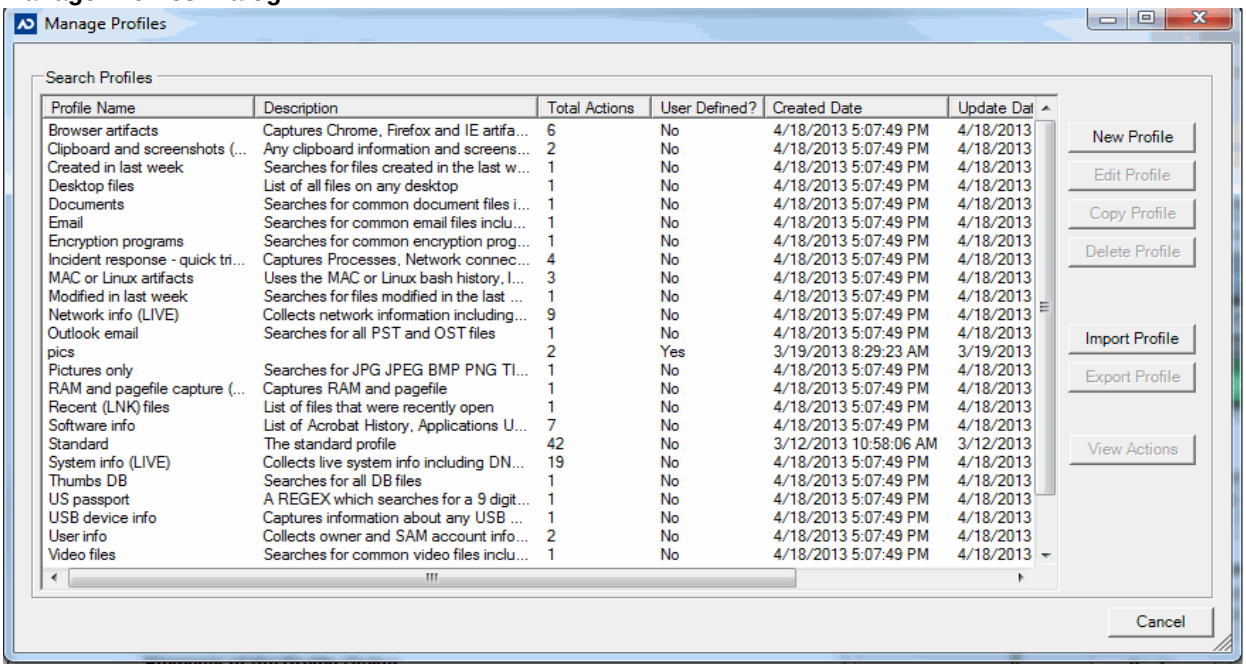
About Triage Profiles

Triage profiles allow you to hold and track all the collections for a single case. You can create a new profile for every case and collect multiple target systems for each profile.

Manage Profiles Dialog

Open the *Profiles* dialog by clicking the **Manage Profiles** button on the *Configure* tab. Use the following figure and table to understand the elements in the *Profiles* dialog.

Manage Profiles Dialog



Elements of the Profile Dialog

Element	Description
Profile Pane	Lists the current profiles. This pane lists the predefined profiles that come with Triage, as well as any custom profiles that have been created. Custom profiles that have been created by the user will be marked as such in the User Defined column.
Copy Profile Button	Click to copy the selected profile.
Edit Profile Button	Click to edit the selected profile.
Delete Profile Button	Click to delete the selected profile.
New Profile Button	Click to create a new profile. See Creating a Profile on page 17.
Import Profile Button	Click to import a profile from file.
Export Profile Button	Click to export the currently selected profile.
View Actions	Click to view the actions assigned to the currently selected profile.
Cancel	Click to close the *Manage Profiles* dialog.

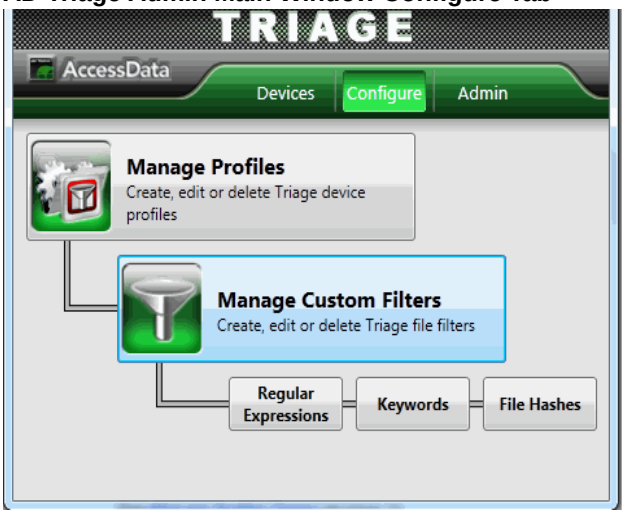
Creating a Profile

Profiles are used to hold collections. Profiles can contain multiple collections. You can create a new profile for each of your cases.

To create a profile

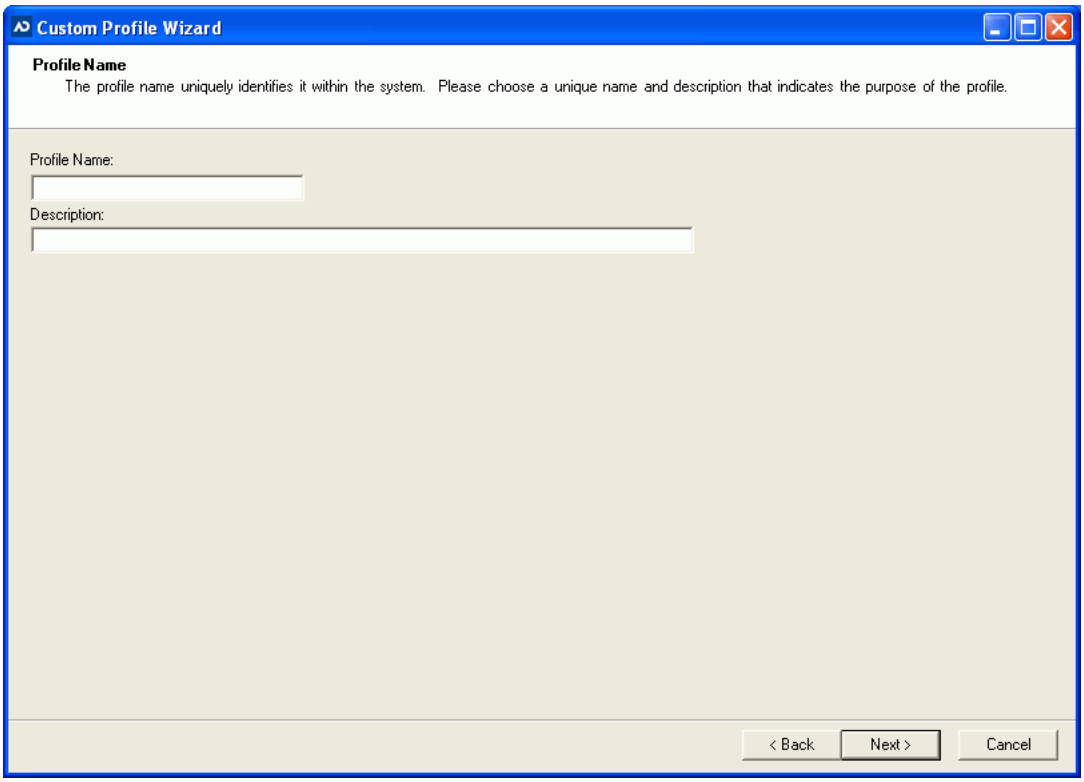
1. Open the *AD Triage Admin* main window.
   See Launching AD Triage Admin on page 11.
2. Select the **Configure** tab.

AD Triage Admin Main Window Configure Tab



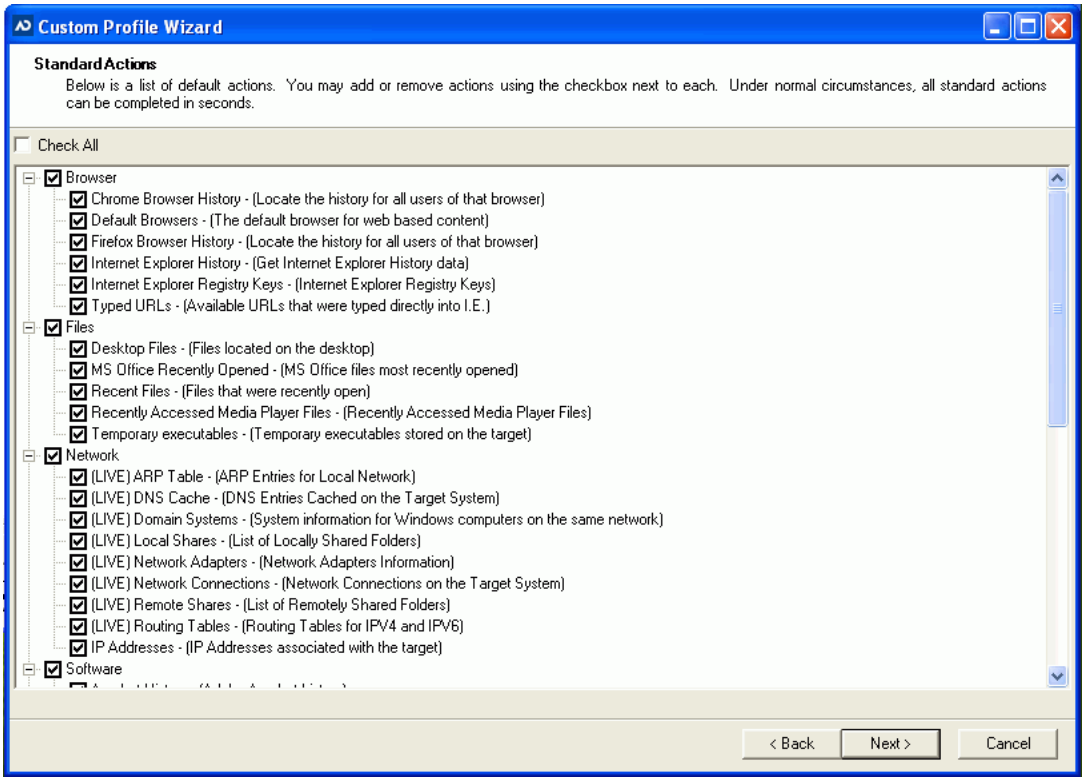
3. Click **Manage Profiles**.
   See Manage Profiles Dialog on page 15.
4. In the *Profiles* dialog, click **New Profile**.
5. In the *Create/Edit Profile* window, click **Next**.

Custom Profile Wizard Profile Name Screen



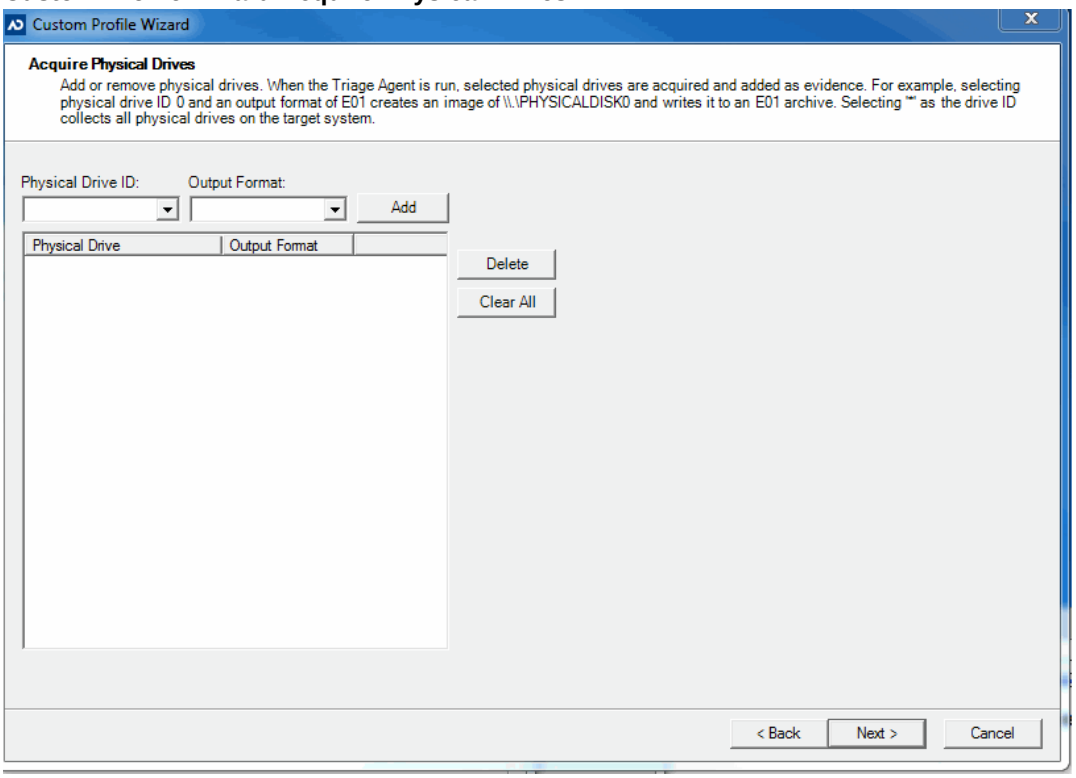
6. In the *Profile Name* screen, enter a name and description for the profile and then click **Next**.

Custom Profile Wizard Standard Actions Screen



7. In the *Standard Actions* screen, check the actions from the default list that you want the profile to perform during collection and click **Next**. (See Selecting Standard Actions For a Profile on page 21.)

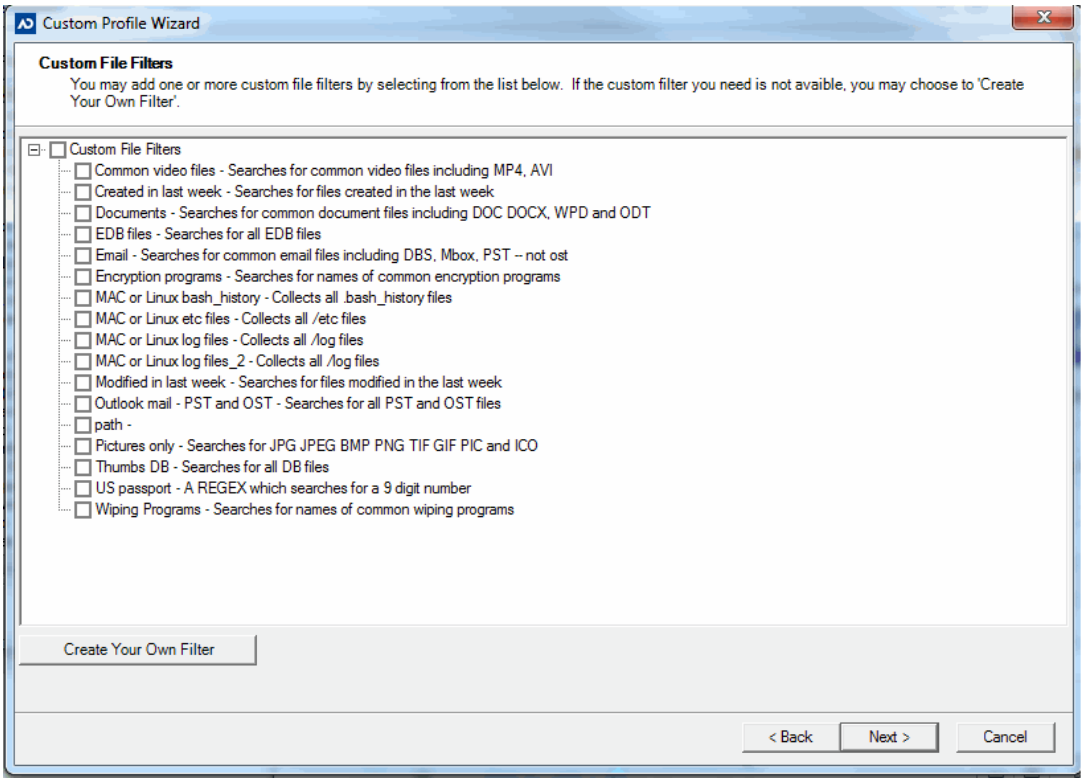
Custom Profile Wizard Acquire Physical Drives



8. In the *Acquire Physical Drives* screen, you can add or remove physical drives by selecting a *Physical Drive ID*, selecting an *Output Format*, and clicking **Add**. When the Triage Agent runs, selected physical drives will be acquired and added as evidence. Click **Next**.

> **Note:** To collect all physical drives, use a wildcard '*'.

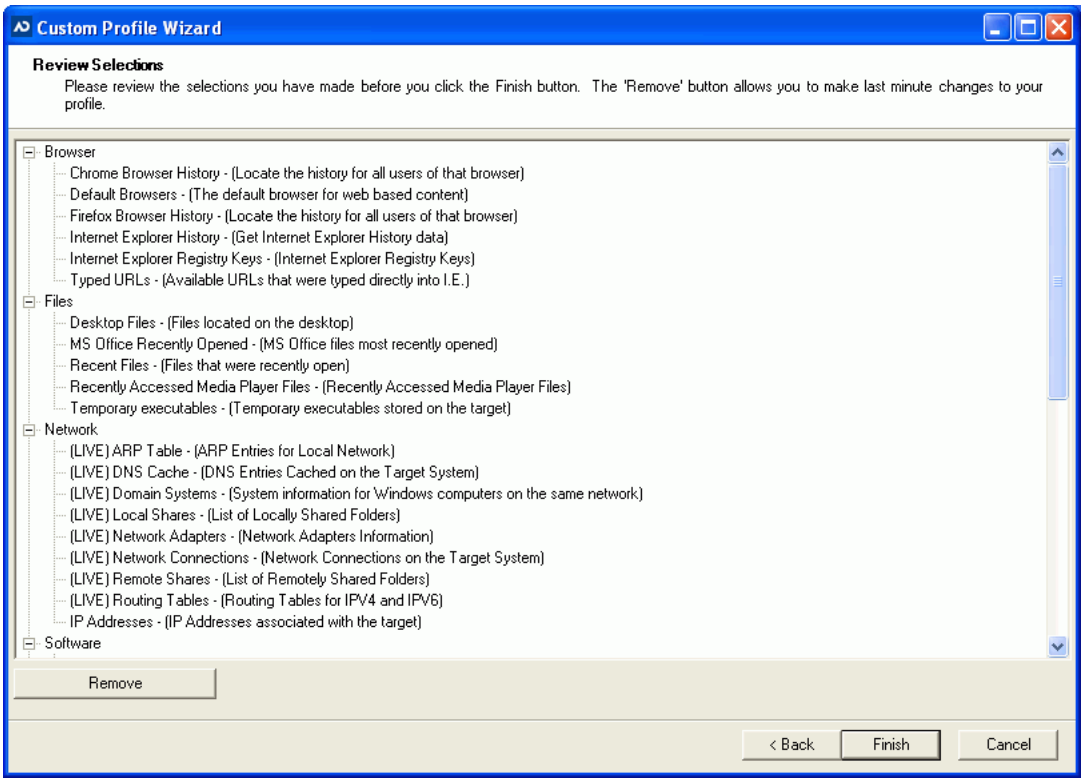
Custom Profile Wizard



9. In the *Custom File Filters* screen, check the custom filters that you want the profile to apply during collection and then click **Next**.

> **Note:** You may, at this time, create a custom filter by clicking the **Create Your Own Filter** button. See Creating a Custom Filter on page 26 for more information on how to do this.

Custom Profile Wizard Review Selections Screen



10. In the *Review Selections* screen, review the actions you have selected to ensure that you want them applied to the profile. If you want to remove any of the actions, highlight the item and click the **Remove** button.
11. Click **Finish**.
12. Click **Yes**.

Selecting Standard Actions For a Profile

Standard actions allow you to collect specific types of information during an investigation. They are divided into subcategories related to their function (for example, collecting an Internet Explorer history or any typed URLs would both be categorized under the *Browser* subgroup). When configuring your Profile, you can select individual actions or entire subcategories. The subcategories are: Browser, Files, Network, Software, System, and Users.

Note: LIVE actions can only be collected from a machine that is on at the time of the collection.

Triage defines each action in parenthesis following the action's name. Most actions are self-explanatory, with a few notable exceptions:

(LIVE) Screenshots Action

The **Screenshots** action captures all active windows at the time of the collection. This includes "hidden" windows that may be running background processes. Because of the screenshot capturing process, transparent

windows can render as empty black or white windows, and overlapped content or transparent borders can also display depending on where and what type of window was captured.

USB Devices Action

The **USB Devices** action captures information about USB devices that have been connected to the machine being investigated. The information collected includes: Manufacturer, Product, Revision, Serial Number, Vendor Id, Product Id, the first time that the device was installed, the last connection, and the last time each user mounted the device.

Copying a Profile

If you want to create a profile that is very similar to an existing profile, but you don't want to have to go through the process of creating a new profile, you can use the copy profile feature.

To copy a profile

1. Open the *AD Triage Admin* main window.
   See Launching AD Triage Admin on page 11.
2. Select the **Configure** tab.
3. Click **Manage Profiles**.
   See Manage Profiles Dialog on page 15.
4. In the *Profile* dialog, select the profile that you want to copy and then click **Copy Profile**.
5. A copy of the profile will appear with the name of the copied filter and the suffix _Copy. For example, Default_Copy.

Editing a Profile

You may want to edit an existing profile to remove or add actions to the profile.

Note: You can edit the actions of the *Default* profile, but you cannot edit the profile name.

To edit an existing profile

1. Open the *AD Triage Admin* main window.
   See Launching AD Triage Admin on page 11.
2. Select the **Configure** tab.
3. Click **Manage Profiles**.
   See Manage Profiles Dialog on page 15.
4. In the *Profile* dialog, select the profile that you want to edit and click **Edit Profile**.
5. Click **Next**.
6. Edit the **Profile Name** or **Description** if desired, and click **Next**.
7. Edit the standard actions that you want included with the profile and click **Next**.
8. Edit the custom file filters that you want included with the profile and click **Next**.
9. Review the actions applied to the profile and click **Finish**.
10. Click **Yes**.

Deleting a Profile

If you want to remove a profile from Triage, you can delete it as long as it is not the default profile.

To delete a profile

1. Open the AD Triage *Admin* main window.
   See Launching AD Triage Admin on page 11.
2. Select the **Configure** tab.
3. Click **Manage Profiles**.
   See Manage Profiles Dialog on page 15.
4. In the *Profile* dialog, select the profile that you want to delete and click **Delete Profile**.
5. Click **Yes**.

Exporting a Profile

You can export a profile to a file that can then be imported to a different computer with Triage Admin on it.

To export a profile

1. Open the AD Triage *Admin* main window.
   See Launching AD Triage Admin on page 11.
2. Select the **Configure** tab.
3. Click **Manage Profiles**.
   See Manage Profiles Dialog on page 15.
4. In the *Profile* dialog, select the profile that you want to export and click **Export Profile**.
5. Click **Yes**.
6. Browse to the location where you want to save the profile and click **Save**.
7. Click **OK**.

Importing a Profile

You can import a profile that has been exported from the Triage Admin console.

To import a profile

1. Open the AD Triage *Admin* main window.
   See Launching AD Triage Admin on page 11.
2. Select the **Configure** tab.
3. Click **Manage Profiles**.
   See Manage Profiles Dialog on page 15.
4. In the *Profile* dialog, click **Import Profile**.
5. Browse to the location of the profile and click **Open**.

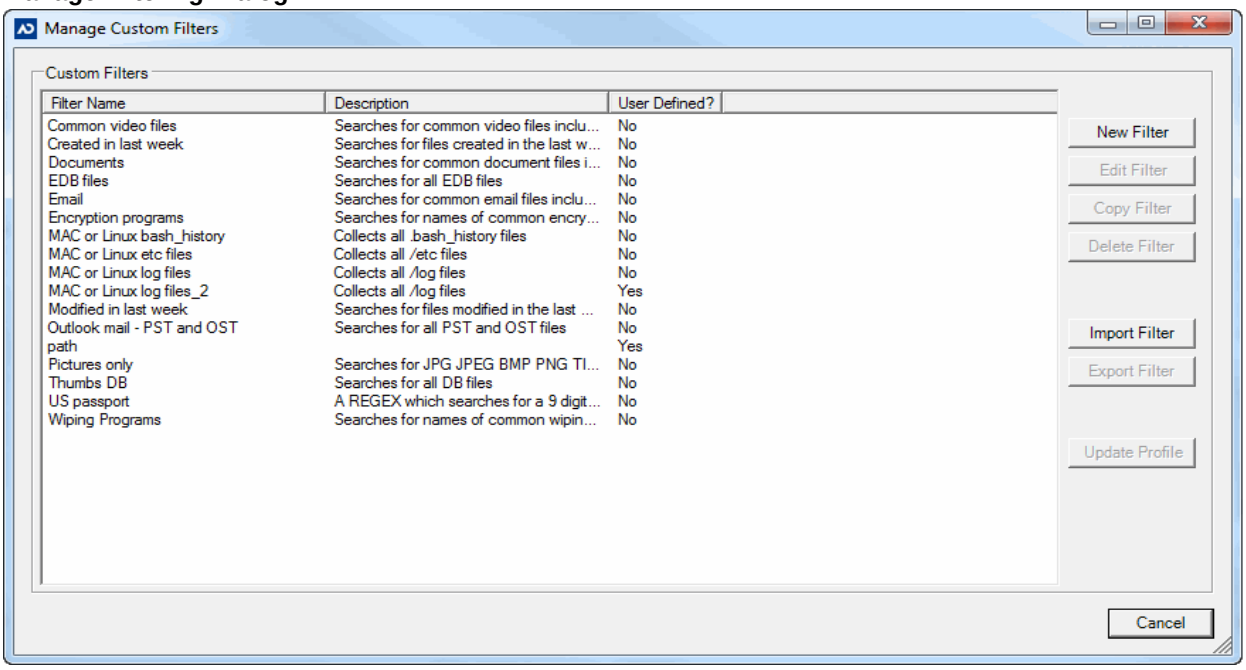
About Custom Filters

In the *AD Triage Admin* console, you can create custom filters, create and add custom conditions to the filters, and add your custom filters to profiles as actions to be performed during collection.

Manage Custom Filters Dialog

Open the *File Filtering* dialog by clicking the **Manage Custom Filters** button on the *Configure* tab. Use the following figure and table to understand the elements in the *File Filtering* dialog.

Manage Filtering Dialog



Elements of the File Filtering Dialog

Element	Description
Existing Filters Pane	Lists the existing filters. This lists the default filters that come standard with Triage, as well as user created filters. Click the column header to sort the list by that column. If a filter has been modified by a user, it will be marked as User Defined in the list.
New Filter Button	Click to create a new custom filter. See Creating a Custom Filter on page 26. See New Filters Wizard on page 29.
Delete Filter Button	Click to delete the selected filter.
Update Profile Button	Click to add the selected filter to a profile.
Copy Filter Button	Click to copy the selected filter.

Elements of the File Filtering Dialog (Continued)

Element	Description
Edit Filter Button	Click to edit the selected filter.
Import Filter Button	Click to import a filter from a file.
Export Filter Button	Click to export the selected filter.

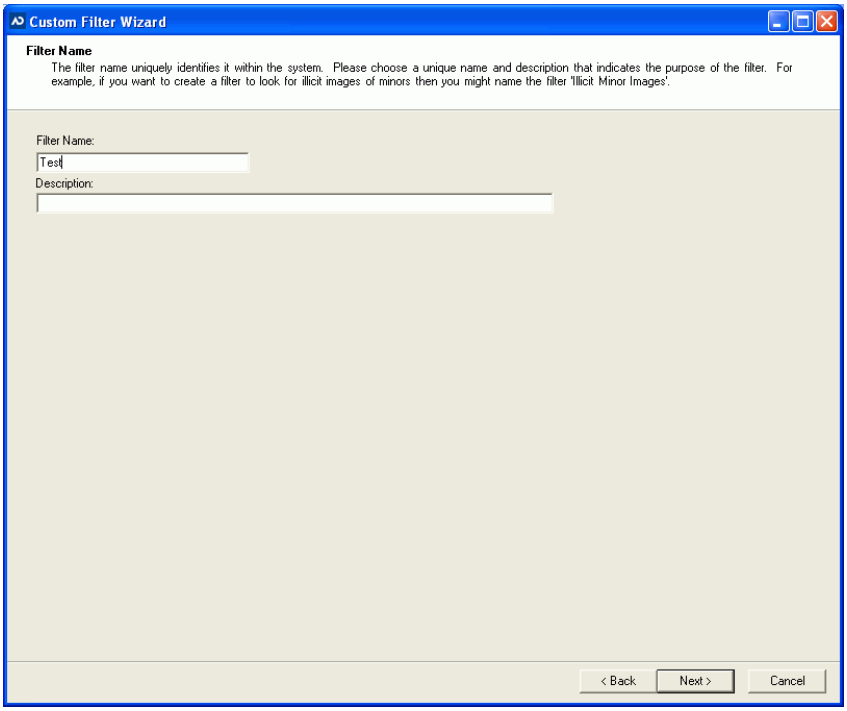
Creating a Custom Filter

Custom filters look for files that contain specified attributes when collecting data. You can apply custom filters to profiles before creating a Triage device.

To create a custom filter

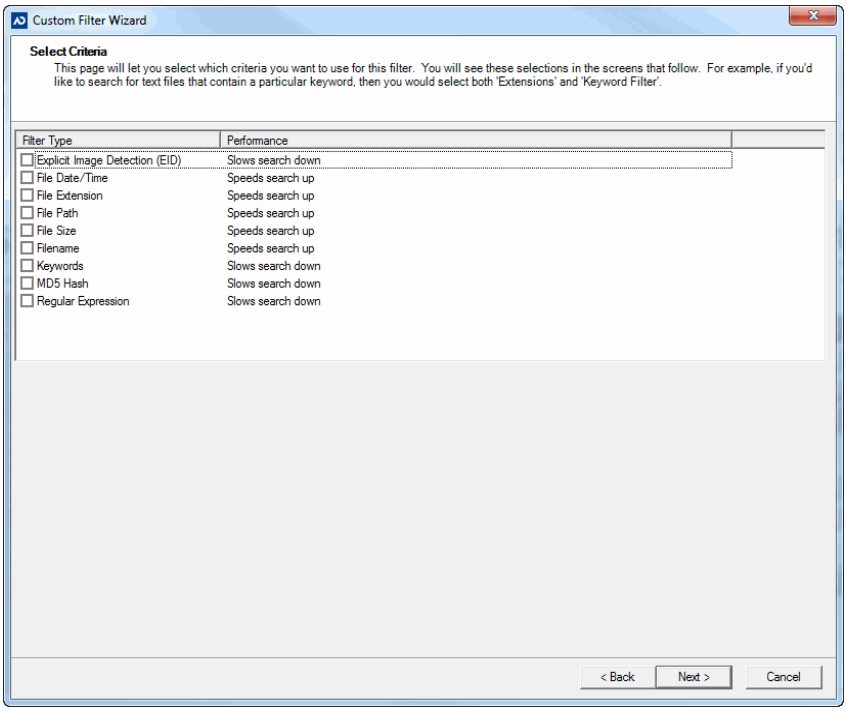
1. Open the *AD Triage Admin* main window.
   See Launching AD Triage Admin on page 11.
2. Select the **Configure** tab.
3. Click **Manage Custom Filters**.
   See Manage Profiles Dialog on page 15.
4. In the *File Filtering* dialog, click **Create New Filter**.
5. In the *Create/Edit Custom File Filter* Wizard, click **Next**.

Custom Filter Wizard Filter Name Screen



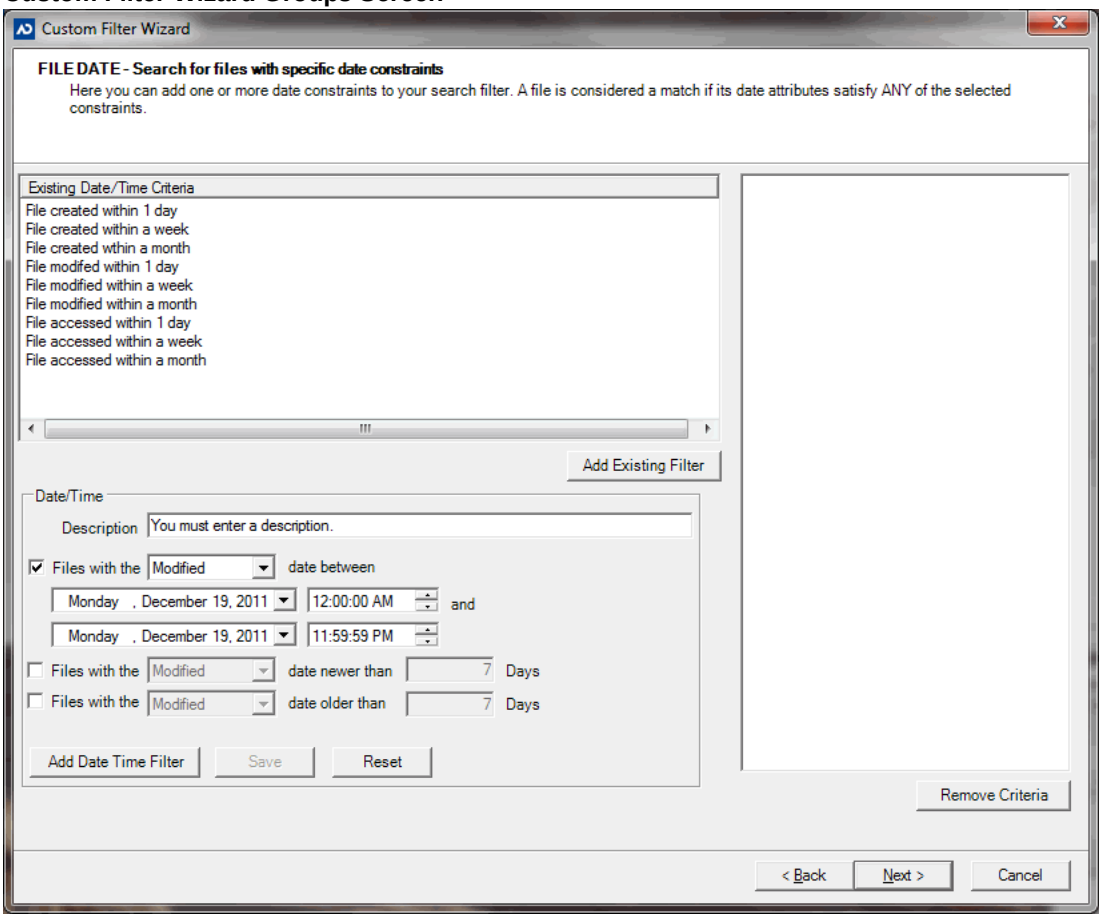
6. In the *Filter Name* screen, enter a name and description for the filter and then click **Next**.

Custom Filter Wizard Select Criteria Screen



7. In the *Select Criteria* screen, check the types of groups you want included in your custom filter and then click **Next**.

Custom Filter Wizard Groups Screen



8. Depending on the groups that you checked, the next screen allows you to add the specific criteria for each group to the custom filter. The following screens may appear:
   - Keyword: See Creating a Keyword Group on page 39.
   - Hash: See Creating a Hash Group on page 41.
   - Regular Expression: See Creating a Regular Expression Group on page 43.
   - File Size: See File Size Filter on page 29.
   - Filename: See Filename Filter on page 35.
   - Date Time: See File Date Filter on page 30.
   - Extensions: See Extensions Filter on page 32.
   - Path: See Path Filter on page 33.
   - Explicit Image Detection: See Explicit Image Detection Filter on page 36.

   Note: Multiple conditions added under a single group name are considered an “OR” condition. Each separate group name added is considered an “AND” condition.

9. Add your criteria for each group and click **Next** until you reach the *Review Custom File Filter Constraints* screen.
10. Click **Finish**.
11. Click **OK**.

Note: To add the filter to a profile, click the **Update Profile** button on the *File Filtering* dialog.

New Filters Wizard

If you click the **New Filter** button in the *Manage Custom Filters* dialog, the *Custom Filter* wizard opens. The screens that appear within the wizard differ depending on the criteria that you select.

See About Custom Filters on page 24.

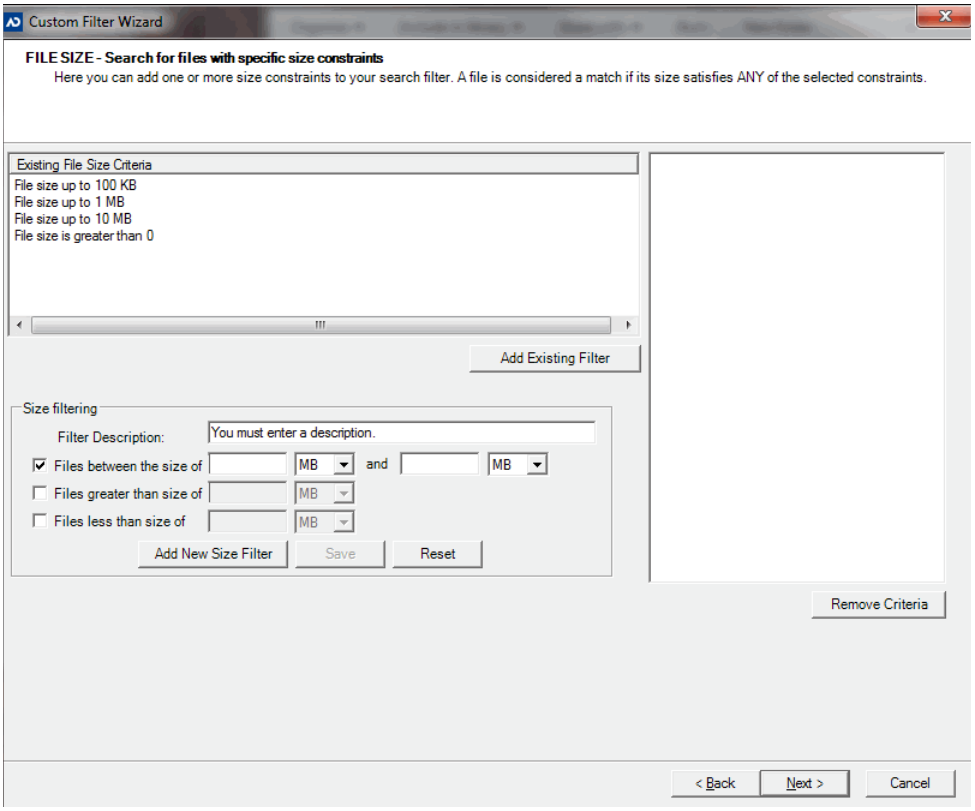
This section covers the following filter screens:

- File Size: See File Size Filter on page 29.
- Date Time: See File Date Filter on page 30.
- Extensions: See Extensions Filter on page 32.
- Path: See Path Filter on page 33.
- Filename: See Filename Filter on page 35.
- Explicit Image Detection: See Explicit Image Detection Filter on page 36.

File Size Filter

The file size filter in the *Custom Filters* wizard can be used to perform actions that have to do with the size of files. Access this screen by checking **File Size** in the *Select Criteria* screen.

File Size Filter Screen



Elements of the File Size Screen

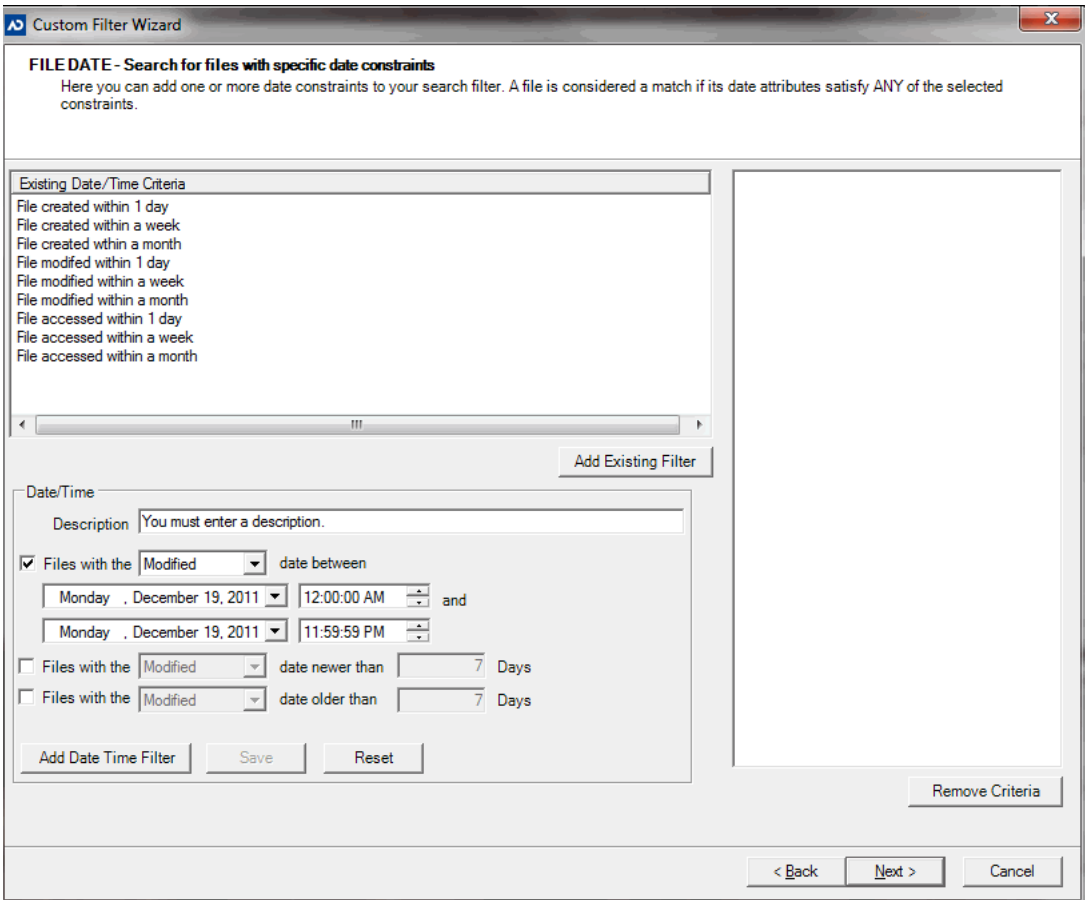
Element	Description
Existing File Size Criteria Pane	Lists the default file size filters.
Add Existing Filter Button	Click to add the selected filter from the Existing File Size Criteria pane to the profile.
Filter Description Field	Enter a description for your custom file size filter.
File Between the Size of	Enter a least and most value to create a filter that searches in a file size range.
File Greater than Size of	Enter a numerical value and select a byte value to create a filter that searches for files bigger than the value you entered.
Files Less than Size of	Enter a numerical value and select a byte value to create a filter that searches for files smaller than the value you entered.
Add New Size Filter Button	Click to add your file size criteria to the profile.
Save Button	Click to save changes to filters already added in the criteria pane. You can change default filters and save them as a new filter, but it does not overwrite the default filter globally.
Reset Button	Click to reset your custom filter changes.
Remove Criteria Button	Click to remove the selected criteria from the profile.
Back Button	Click to go back to the previous screen in the wizard.
Next Button	Click to go to the next screen in the wizard.
Cancel Button	Click to close the wizard.

File Date Filter

The file data filter in the *Custom Filters* wizard can be used to perform actions that have to do with the size of files. Access this screen by checking **Date Time** in the *Select Criteria* screen.

Note: If you are searching, using the *Date Time* filter and have a very small window of time that occurs outside of the DST shift it, your search results will not get things that are within the hour shift.

File Date Filter



Elements of the File Date Screen

Element	Description
Existing Date Time Criteria Pane	Lists the default date time filters.
Add Existing Filter Button	Click to add the selected filter from the *Existing Date Time Criteria* pane to the profile.
Description Field	Enter a description for the custom date time filter.
Files with the (status) between	Check this, select a status from the drop-down, and select a date and time range to create a filter to search for files created/modified/accessed between the dates you selected.
Files with the (status) date newer than (number) days	Check this, select a status, and enter a numerical value to create a filter to search for files created/modified/accessed in the indicated number of days or less.
Files with the (status) date older than (number) days	Check this, select a status, and enter a numerical value to create a filter to search for files created/modified/accessed older than the indicated number of days.
Add Date Time Filter Button	Click to add the date time criteria to the profile.

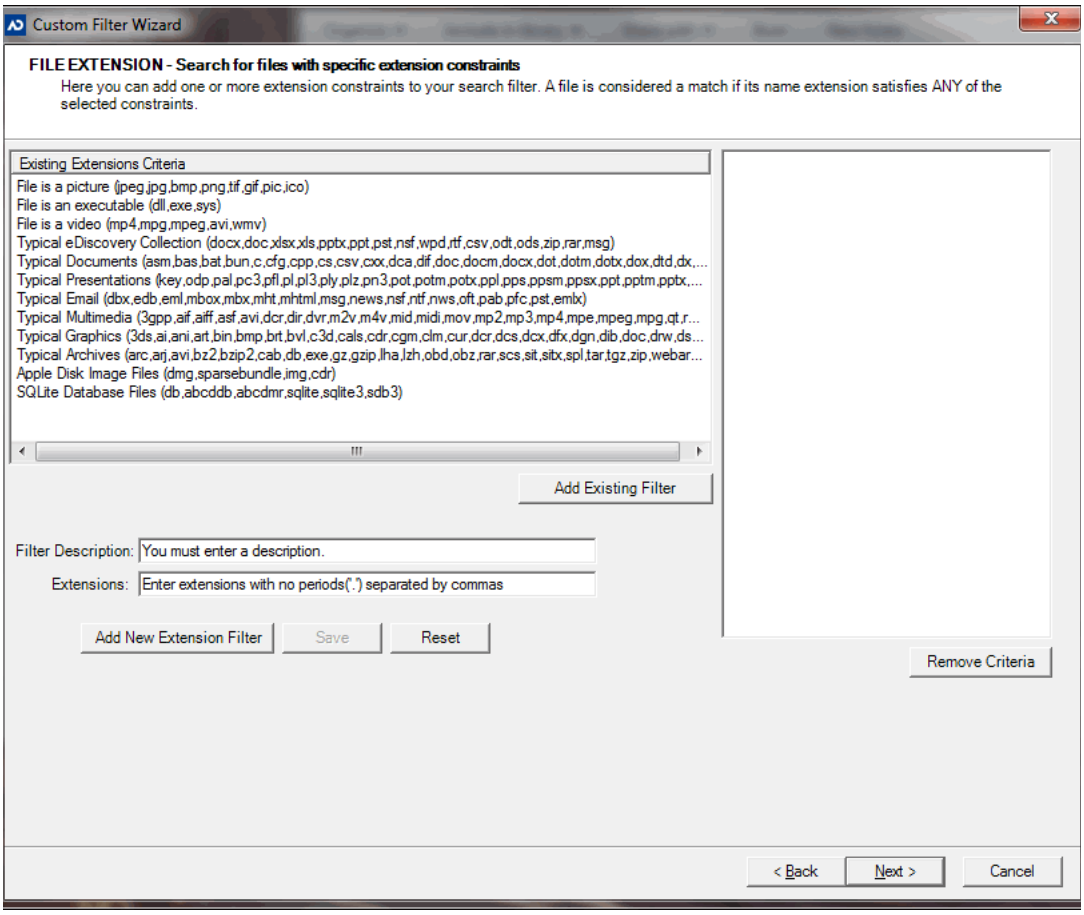
Elements of the File Date Screen (Continued)

Element	Description
Save Button	Click to save changes to filters already added in the criteria pane. You can change default filters and save them as a new filter, but it does not overwrite the default filter globally.
Reset Button	Click to reset your custom filter changes.
Remove Criteria Button	Click to remove the selected criteria from the profile.
Back Button	Click to go back to the previous screen in the wizard.
Next Button	Click to go to the next screen in the wizard.
Cancel Button	Click to close the wizard.

Extensions Filter

The extensions filter in the *Custom Filters* wizard can be used to perform actions that have to do with the size of files. Access this screen by checking **Extensions** in the *Select Criteria* screen.

Extensions Filter



Elements of the Extensions Filter

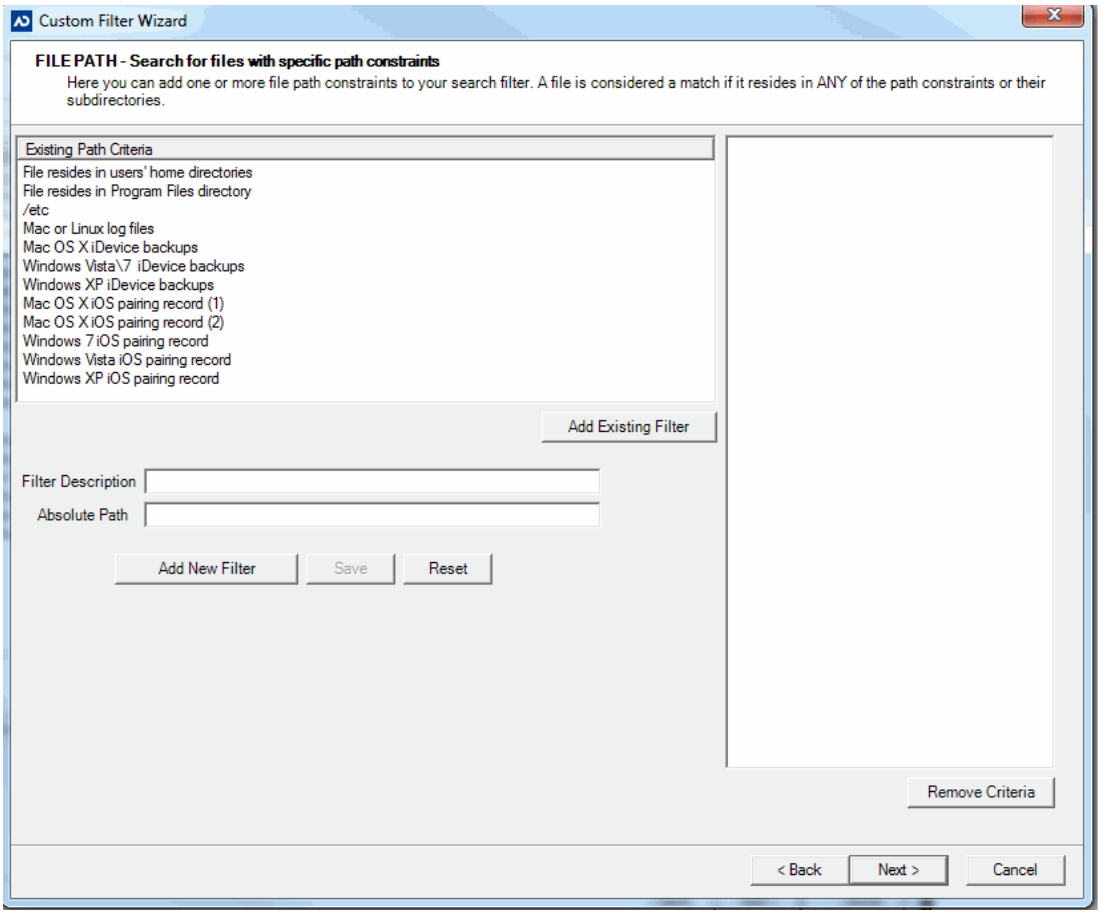
Element	Description
Existing Extensions Criteria Pane	Lists the default extension filters.
Add Existing Filter Button	Click to add the selected filter from the *Existing Extension Criteria* pane to the profile.
Filter Description Field	Enter a description for your custom filter.
Extensions Field	Enter the extensions for which you want to search with no periods and separated by commas.
Add New Size Filter Button	Click to add your file size criteria to the profile.
Save Button	Click to save changes to filters already added in the criteria pane. You can change default filters and save them as a new filter, but it does not overwrite the default filter globally.
Reset Button	Click to reset your custom filter changes.
Remove Criteria Button	Click to remove the selected criteria from the profile.
Back Button	Click to go back to the previous screen in the wizard.
Next Button	Click to go to the next screen in the wizard.
Cancel Button	Click to close the wizard.

Path Filter

The path filter in the *Custom Filters* wizard can be used to perform actions that have to do where the files are located. Access this screen by checking **Paths** in the *Select Criteria* screen.

Note: You can search a specific path for a specific file by combining both the path filter and the filename filter. To search a specific path for a specific file, make sure to select both File path and Filename in the Select Criteria screen. See Filename Filter on page 35.

File Path Filters Screen



Elements of the File Path Screen

Element	Description
Existing Path Criteria Pane	Lists the default path filters.
Add Existing Path	Click to add the selected filter from the *Existing Path Criteria* pane to the profile.
Filter Description	List a description for the filter.
Absolute Path	Allows you to define a path to collect from. You can collect from a specified folder, or target sub folders under a folder. For example, if you were collecting from a system with a folder named photos, with sub folders 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 sub folder. **Note: You do not need to begin or end a path defined in this field with a / (slash) or \ (backslash).**

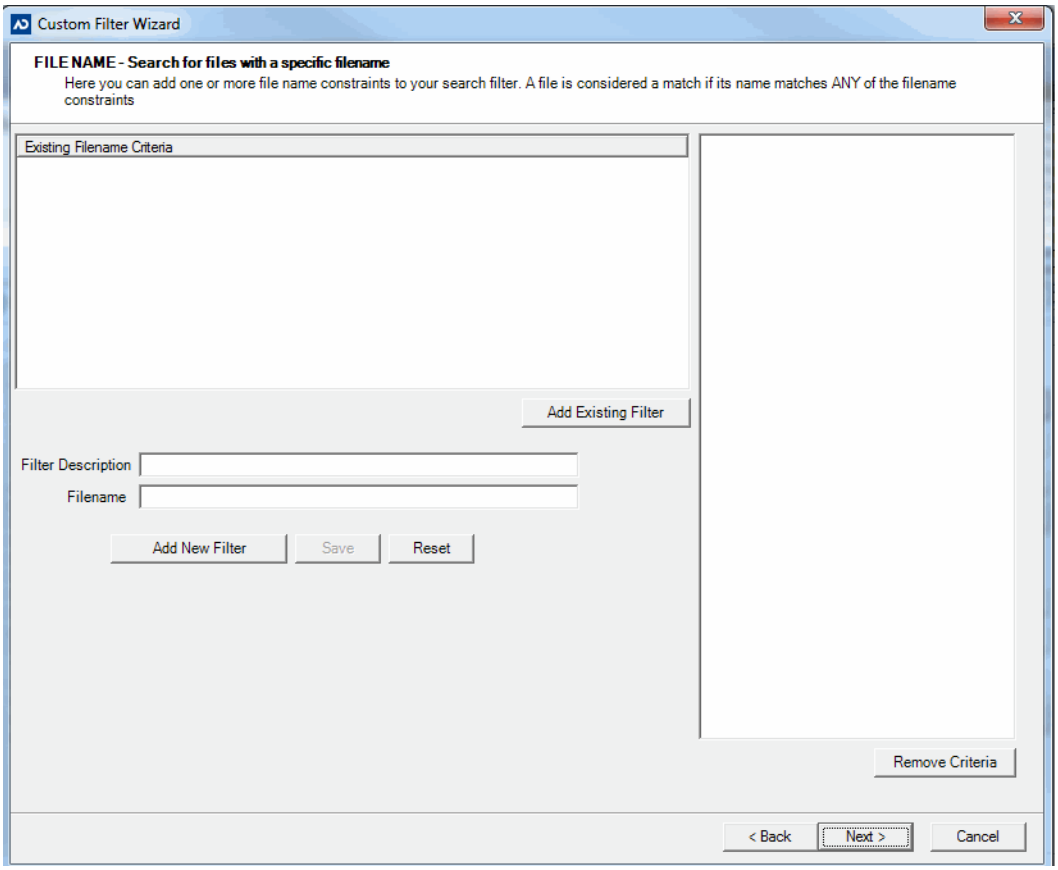
Elements of the File Path Screen (Continued)

Element	Description
Remove Criteria Button	Click to remove the selected criteria from the profile.
Back Button	Click to go back to the previous screen in the wizard.
Next Button	Click to go to the next screen in the wizard.
Cancel Button	Click to close the wizard.

Filename Filter

The Filename filter in the *Custom Filters* wizard can be used to perform actions that have to do with the name of the files. Access this screen by checking **Filename** in the *Select Criteria* screen.

Filename Filters Screen



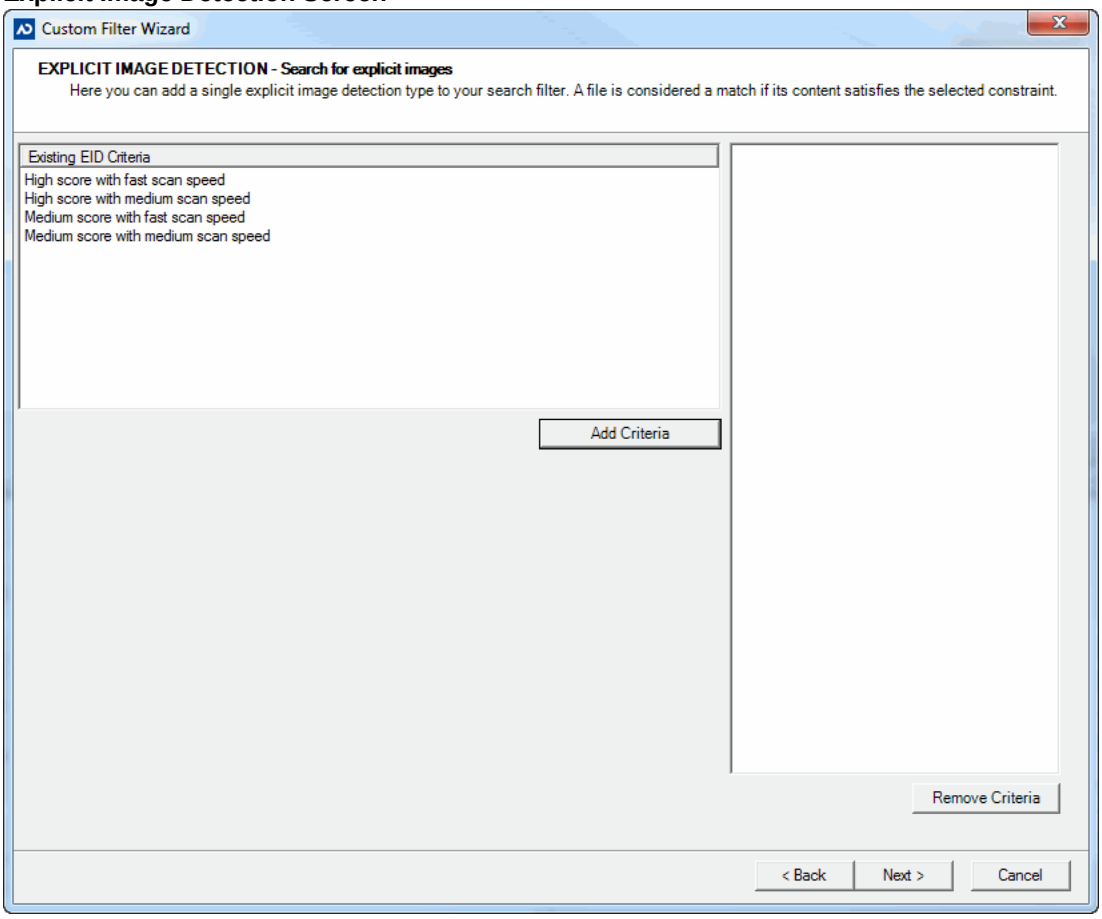
Elements of Filename Screen

Element	Description
Existing Filename Criteria Pane	Lists the default filename filters.
Add Existing Filter	Click to add the selected filter from the *Existing Filename Criteria* pane to the profile.
Filter Description	List a description for the filter.
Filename	Search for a specific named file.
Remove Criteria Button	Click to remove the selected criteria from the profile.
Back Button	Click to go back to the previous screen in the wizard.
Next Button	Click to go to the next screen in the wizard.
Cancel Button	Click to close the wizard.

Explicit Image Detection Filter

The Explicit Image Detection filter in the *Custom Filters* wizard can be used to perform actions that have to do with the size of files. Access this screen by checking **Explicit Image Detection** in the *Select Criteria* screen.

Explicit Image Detection Screen



Elements of the Explicit Image Detection Screen

Element	Description
Existing EID Criteria Pane	Lists the default explicit filters.
Add Criteria Button	Click to add the selected filter from the *Existing EID Criteria* pane to the profile.
Remove Criteria Button	Click to remove the selected criteria from the profile.
Back Button	Click to go back to the previous screen in the wizard.
Next Button	Click to go to the next screen in the wizard.
Cancel Button	Click to close the wizard.

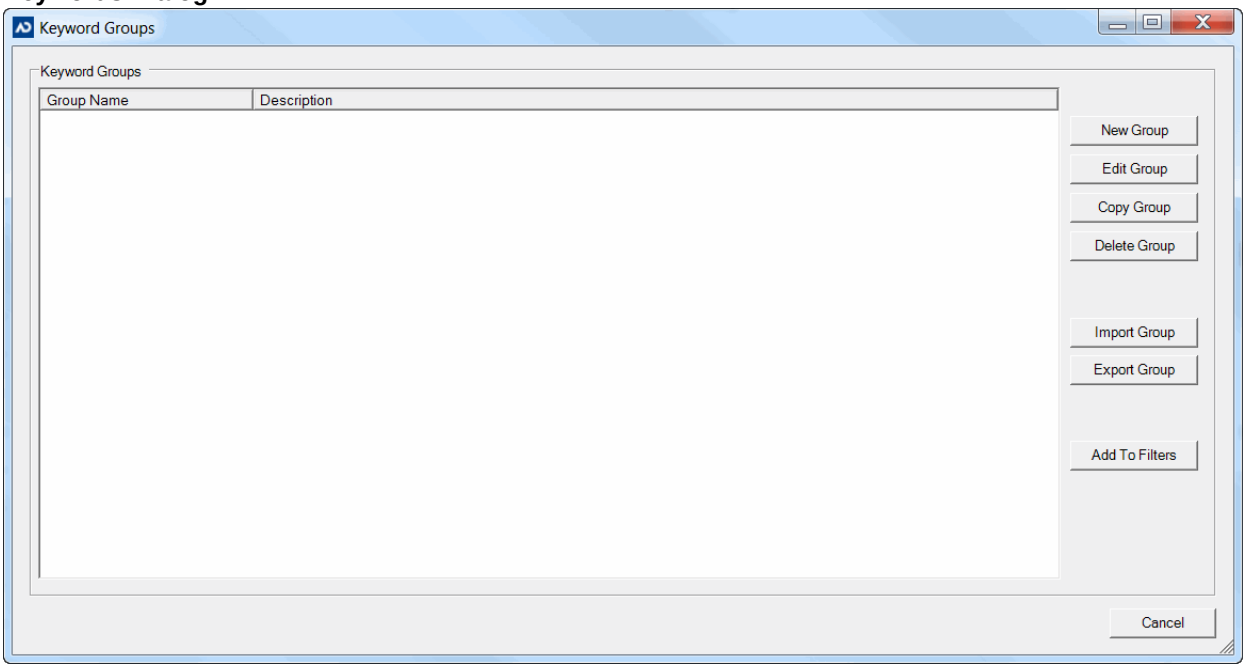
About Keywords

The keyword feature allows you to create a keyword group that can then be added to a custom filter. Keyword conditions search for a specific word or term in the body of files and in the file name. When performing a keyword search, the system will return any file that contains the search term without word boundaries.

Keywords Dialog

Open the *Keywords* dialog by clicking the **Keyword Groups** button on the *Configure* tab. Use the following figure and table to understand the elements in the *Keywords* dialog.

Keywords Dialog



Elements of the Keywords Dialog

Element	Description
Keywords Pane	Lists existing filters.
Copy Group Button	Click to copy the selected group.
Edit Group Button	Click to edit the selected group.
Import Group Button	Click to import a filter from file.
Export Group Button	Click to export a group to a file.
Add to Filter Button	Click to add filters to the selected group.
Delete Group Button	Click to delete the selected group.

Elements of the Keywords Dialog (Continued)

Element	Description
New Group Button	Click to create a new Keyword group. See Creating a Keyword Group on page 39.

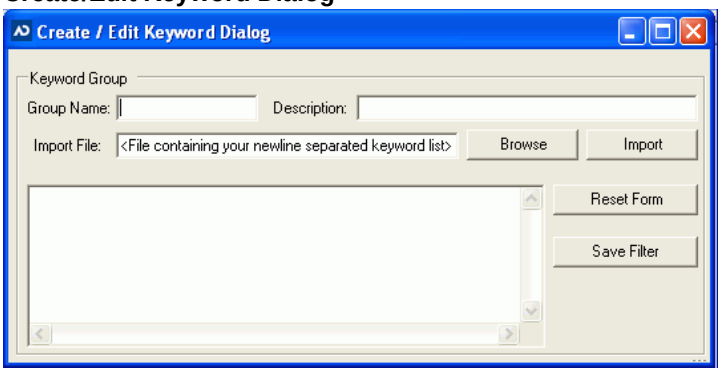
Creating a Keyword Group

You can create a keyword group from the configure tab or while you are creating a custom filter. Keyword groups can be added to custom profiles.

To create a new keyword group

1. In the *Configure* tab, click **Keyword Groups**.
   See Keywords Dialog on page 38.
2. In the *Keywords* dialog, click **Create New Group**.

Create/Edit Keyword Dialog



3. Enter a **Group Name** and **Description**.
4. (Optional) Enter an **Import File** path or browse to a file that contains the keywords you want to add to the group. Once found, click **Import** to add the keywords to the list.
5. Enter the keywords you want added to the condition in the keyword pane.

   Note: Enter each keyword search term on its own line.

6. Click **Save Filter**.
7. Click **OK** to add the keyword to the existing filters list.
8. Click **Yes** to create another keyword group or **No** to close the dialog.
9. Add the group to a filter by following the steps in Creating a Custom Filter on page 26.

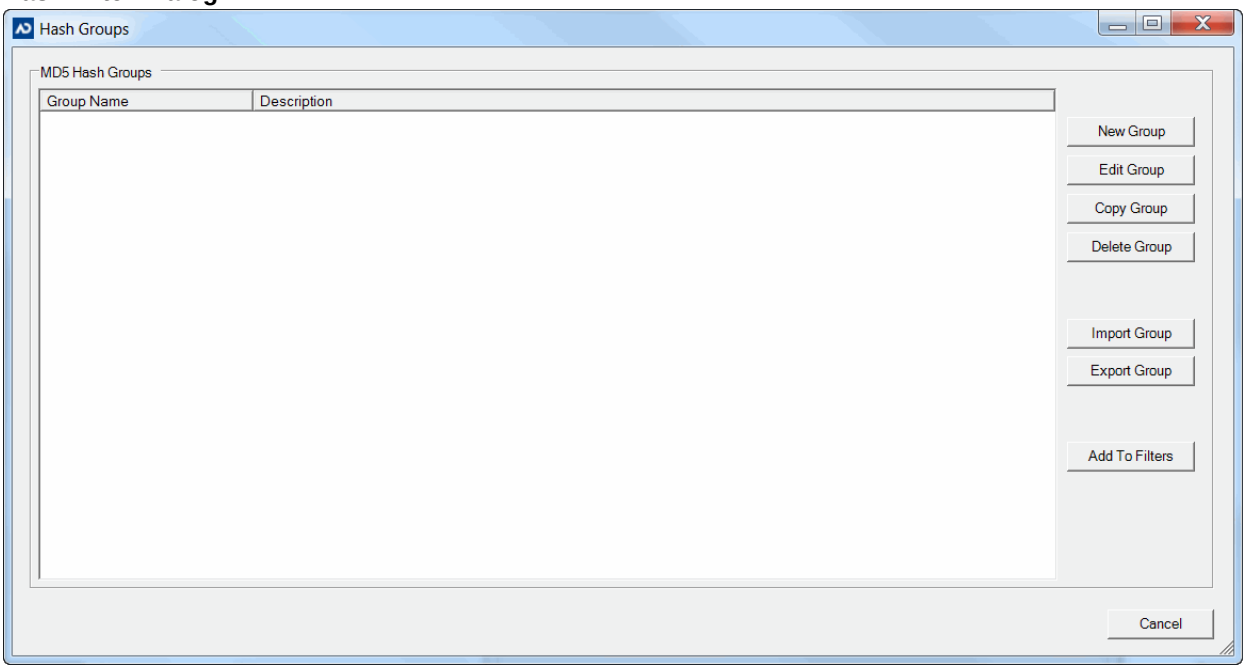
About Hash Groups

The Hash feature allows you to create a hash group that can then be added to a custom filter. Hash conditions search for specified hashes during collection.

Hash Filter Dialog

Open the *Hash Filter* dialog by clicking the **Hash Groups** button on the *Configure* tab. Use the following figure and table to understand the elements in the *Hash Filter* dialog.

Hash Filter Dialog



Elements of the Hash Filter Dialog

Element	Description
Hash Filter Pane	Lists existing groups. Click the column header to sort the list by that column.
Copy Group Button	Click to copy the selected group.
Edit Group Button	Click to edit the selected group.
Import Group Button	Click to import a group from an existing file.
Export Group Button	Click to export the selected group to a file.
Add to Filters Button	Click to add filters to the selected group.
Delete Group Button	Click to delete the selected group.
New Group Button	Click to create a new Hash Filter Group. See Creating a Hash Group on page 41.

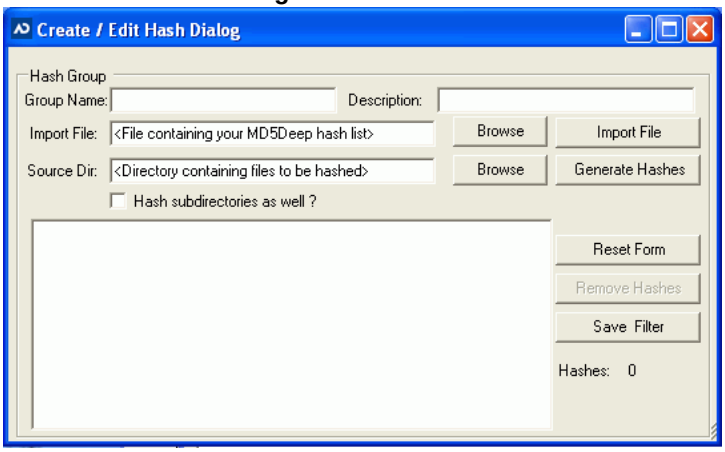
Creating a Hash Group

You can create a hash group from the Configure tab or while creating a custom filter. Hash groups can be added to custom profiles.

To create a hash group

1. In the *Configure* tab, click **Hash Groups**.
   See Hash Filter Dialog on page 40.
2. In the *Hash Filter* dialog, click **Create New Group**.

Create/Edit Hash Dialog



3. In the *Create/Edit Hash* dialog, enter a **Group Name** and **Description** for the group.
4. Click the Import File **Browse** button to browse to the known file on your system. Then, click **Import File** to add the file to the *Hash* pane.
5. Click the *Source Dir* **Browse** button to browse to the directory containing files to be hashed.
6. Check the **Hash Subdirectories as well** check box to include child files for the selected known file.

   Note: Selecting a known file greatly increases the speed of the hashing when collecting data.

7. Click **Generate Hashes** to add the hashes to the *Hash* pane.

   Note: Clicking the **Reset Form** button clears all the fields in the dialog.

8. Click **Save Filter**.
9. Click **Yes**.
10. Click **Yes** again if you want to create a new *Hash* group or **No** to return to the *Hash Filter* dialog.
11. Add the group to a filter by following the steps in Creating a Custom Filter on page 26.

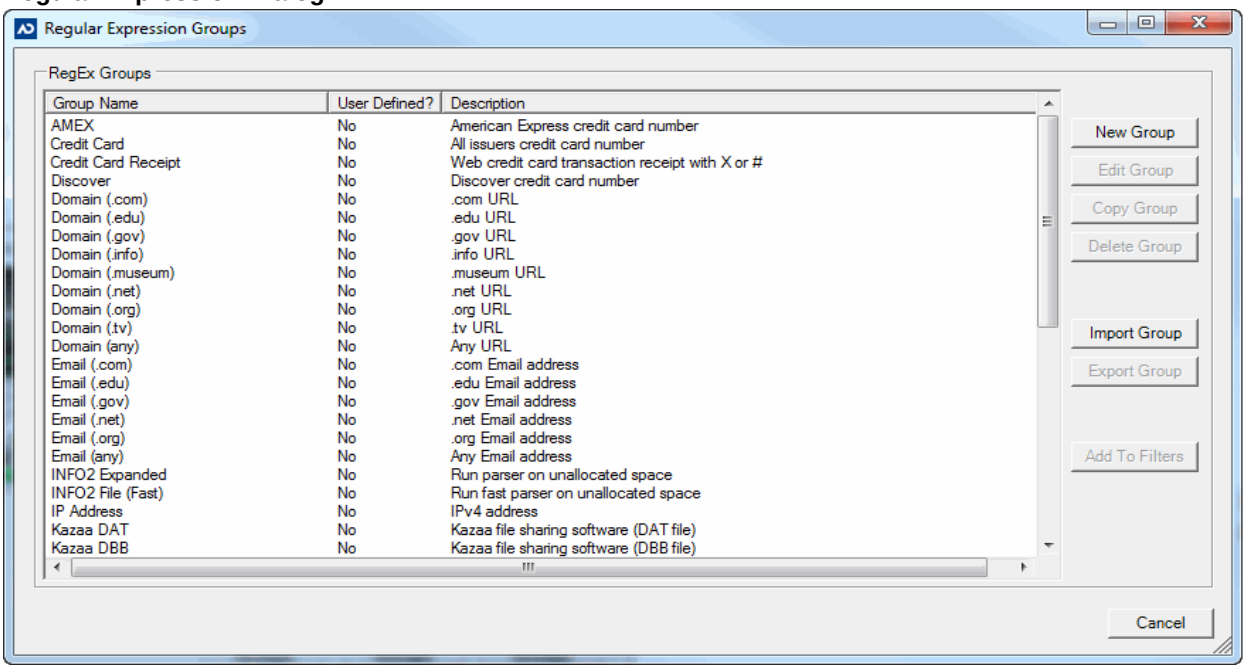
About Regular Expression Groups

The *Regular Expression* feature allows you to create a regular expression condition that can then be added to a custom filter. Regular expression conditions search for a specified expression during collection.

Regular Expression Dialog

Open the *Regular Expression* dialog by clicking the **RegEx Groups** button on the *Configure* tab. Use the following figure and table to understand the elements in the *Regular Expression* dialog.

Regular Expression Dialog



Elements of the Regular Expression Dialog

Element	Description
Regular Expression Pane	Lists existing groups. Triage has predefined RegEx groups that you can choose from. These predefined groups cannot be edited or deleted.
Copy Group Button	Click to copy the selected group.
Edit Group Button	Click to edit the selected group.
Import Group Button	Click to import a group from file.
Export Group Button	Click to export the selected group to a file.
Add to Filters Button	Click to add filters to the selected group.
Delete Group Button	Click to delete the selected group.

Elements of the Regular Expression Dialog (Continued)

Element	Description
New Group Button	Click to create a new Regular Expression group. See Creating a Regular Expression Group on page 43.

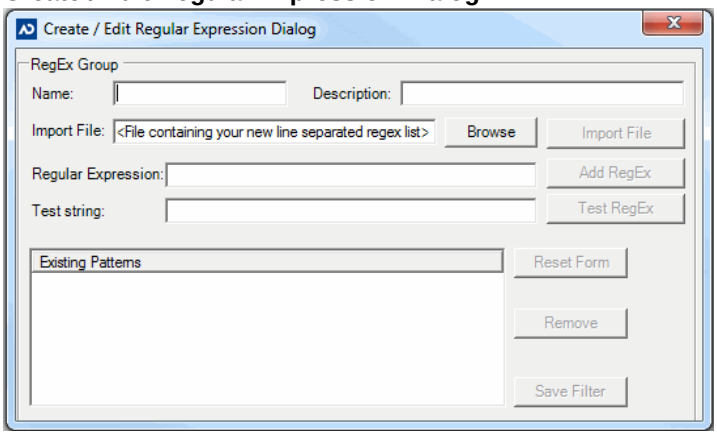
Creating a Regular Expression Group

You can create a regular expression group on the Configure tab and while creating a custom filter. You can add regular expression groups to custom profiles.

To create a regular expression group

1. In the *Configure* tab, click **RegEx Groups**.
   See Explicit Image Detection Filter on page 36.
2. In the *Regular Expression* dialog, click **New Group**.

Create / Edit Regular Expression Dialog



3. In the *Create / Edit Regular Expression* dialog, enter a **Group Name** and **Description** for the group.
4. Click the Import File **Browse** button and select a known file. Then, click **Import File** to add the regular expression to the *Regular Expression* pane.
5. Enter an expression in the **Regular Expression** field.
6. Enter a **Test String** for the regular expression.
7. Click **Test Regular Expression** button to test if the expression matches the string.
8. Click **Add Regular Expression**.

   Note: Clicking the **Reset Form** button clears all the fields in the dialog.

9. Click **Save Filter**.
10. Click **Yes**.
11. Click **Yes** again if you want to create a new *Hash* group or **No** to return to the Hash Filter dialog.
12. Add the group to a filter by following the steps in Creating a Custom Filter on page 26.

Chapter 4

Setting Up Your Triage Device

Managing Licenses

Before you can apply a profile to a device for collection, you must first license the device. You can use one license per device.

See Appendix B Managing Security Devices and Licenses on page 106.

Triage provides a single licensed USB device. There is no limit to number of collections or volume of data per collection.

Note: Multiple licenses can be associated with a single admin console for large organizations

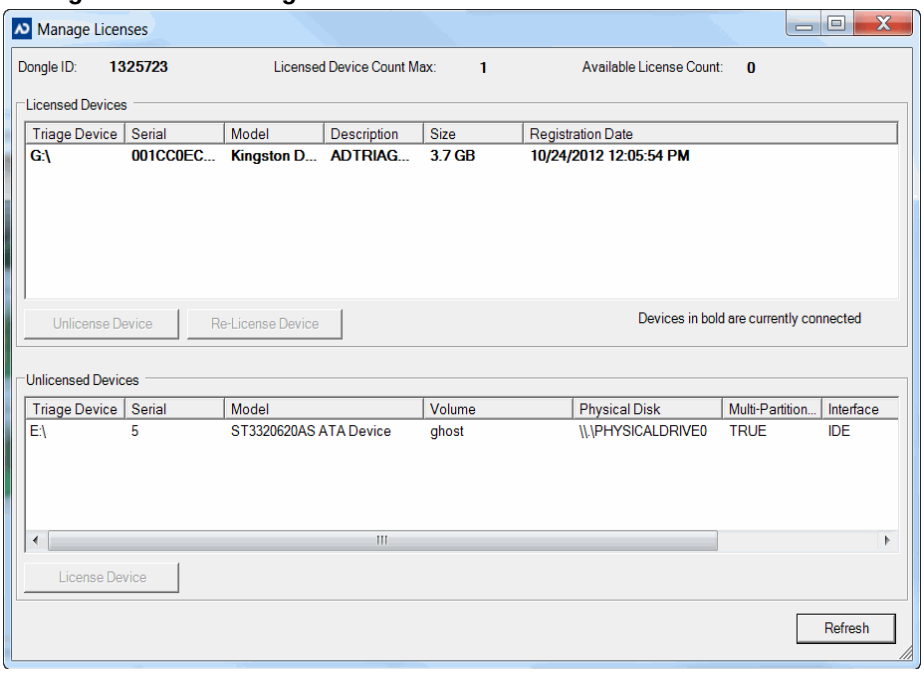
If you have a license that limits the number of USB devices you can license, the available license count appears at the top of the *Manage Licenses* dialog.

Note: If you run out of licenses for USB devices, contact the AccessData sales team for information on how to get more licenses.

Manage Licenses Dialog

Open the *Manage Licenses* dialog by clicking the **Manage Licenses** button on the *Admin* tab. Use the following figure and table to understand the elements in the *Manage Licenses* dialog.

Manage Licenses Dialog



Elements of the Manage Licenses Dialog

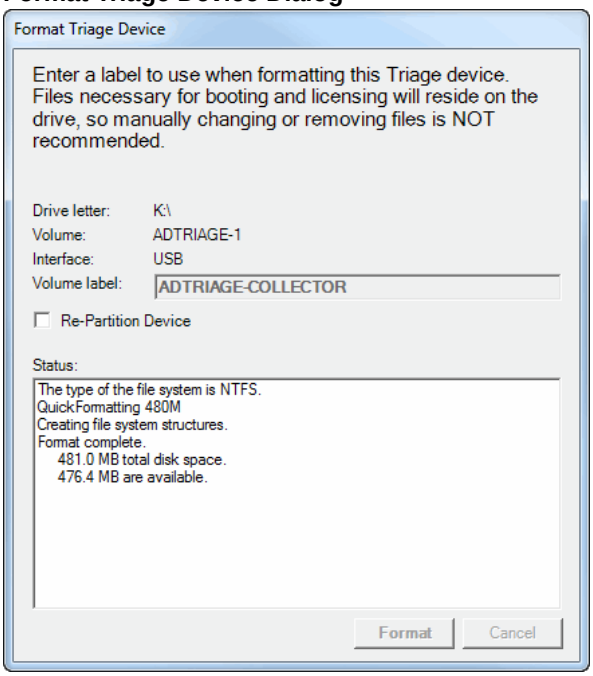
Element	Description
Dongle ID	Lists the number for the codemeter used for AD Triage.
Licensed Device Count Max	Lists the number of licenses for separate devices. Only visible if you signed up for a limited amount of device licenses, but unlimited amount of recoveries.
Available License Count	Lists the number of licenses still available for use. Only visible if you signed up for a limited amount of device licenses, but unlimited amount of recoveries.
Upper Device Pane	Lists the devices currently in use.
Un-License Device Button	Click to remove the license from the selected device.
Re-License Device Button	Click to reattach a license to the selected device.
Lower Device Pane	Lists un-licensed devices that are connected to the computer.
License Device Button	Click to attach a license to the selected device. See Managing Licenses on page 44.
Refresh Button	Click to refresh the lists of devices.

Licensing a Device

To license a device

1. On the *Admin* tab, click **Manage Licenses**.
   See Managing Licenses on page 44.
2. In the *Manage Licenses* dialog, select the device you want to license from the lower pane and click **License Device**.

Format Triage Device Dialog



3. In the *Format Triage Device* dialog, name the USB device in the *Volume Label* field.
4. Click the **Format** button.

   Triage will format the device. You can view the status of the device in the *Status* pane. If an error occurs, follow the steps in the *Status* pane and attempt the format again. Or, check **Also Re-Partition Device** and try to format the device again if formatting fails. Formatting does the following things to the USB device:

   - Formats the device as a single NTFS partition
   - Makes the device bootable
   - Adds a license file

Important: Formatting a USB device will remove all media currently on the device. Make sure that you don't have any wanted data on the USB device. You cannot save more than one profile to a USB device. Each profile must have its own device. However, you can collect multiple target systems to one USB device.

Note: Formatting the device makes the device bootable. So, when booting to a target system, you can boot to the USB device and it will run the Triage collection console. (See Booting AD Triage on a Target System on page 61 for more information on booting to a USB device.)

5. Click **OK**.

   The USB device should now appear in the upper license pane of the *Manage License* dialog.

Unlicensing a Device

Once a device has been licensed, you can unlicense that device and license a different USB device.

Note: The USB device to be unlicensed does not need to be physically attached to the admin system. (For example, when a licensed USB device has been misplaced, and the license needs to be assigned to another USB device.)

To unlicense a device

1. On the Admin tab, click **Manage Licenses**.
   See Managing Licenses on page 44.
2. In the *Manage Licenses* dialog, select the device you want to unlicense from the upper pane and click **Unlicense Device**.

Creating a Triage USB Device

When you create a Triage USB device, you save the profile and all of the actions associated with the profile to the USB device. This allows you to collect data from a target system using the criteria you set up on the selected profile.

Note: You can only create Triage USB devices using devices that you have already licensed. See Managing Licenses on page 44 for information on how to license your device.

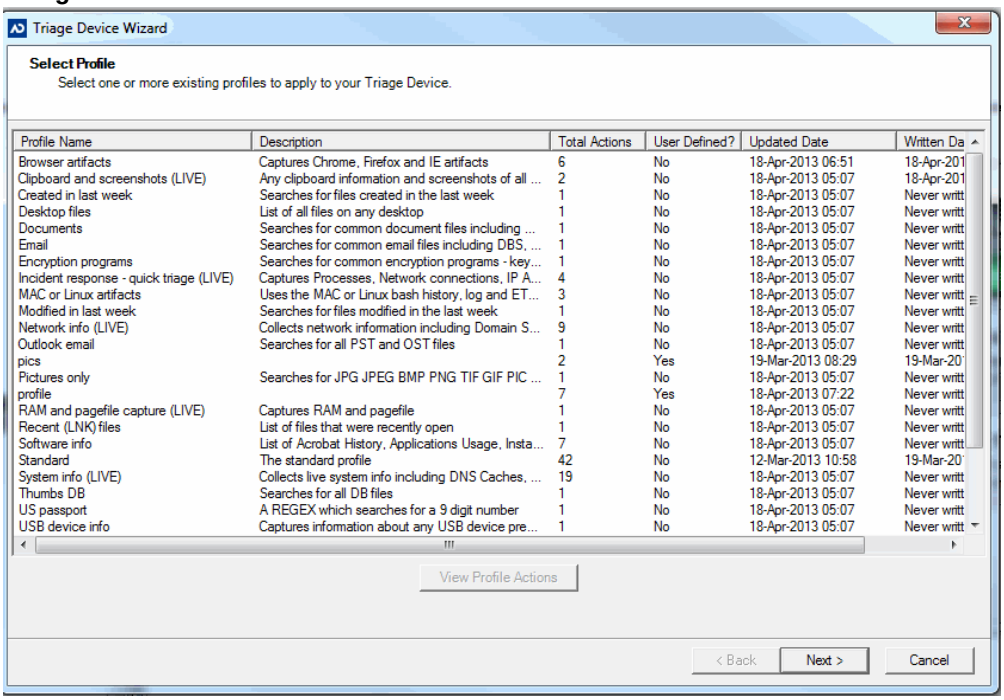
To create a Triage USB device

1. In the *AD Triage* main window, click on the **Device** tab.

Triage Devices Tab

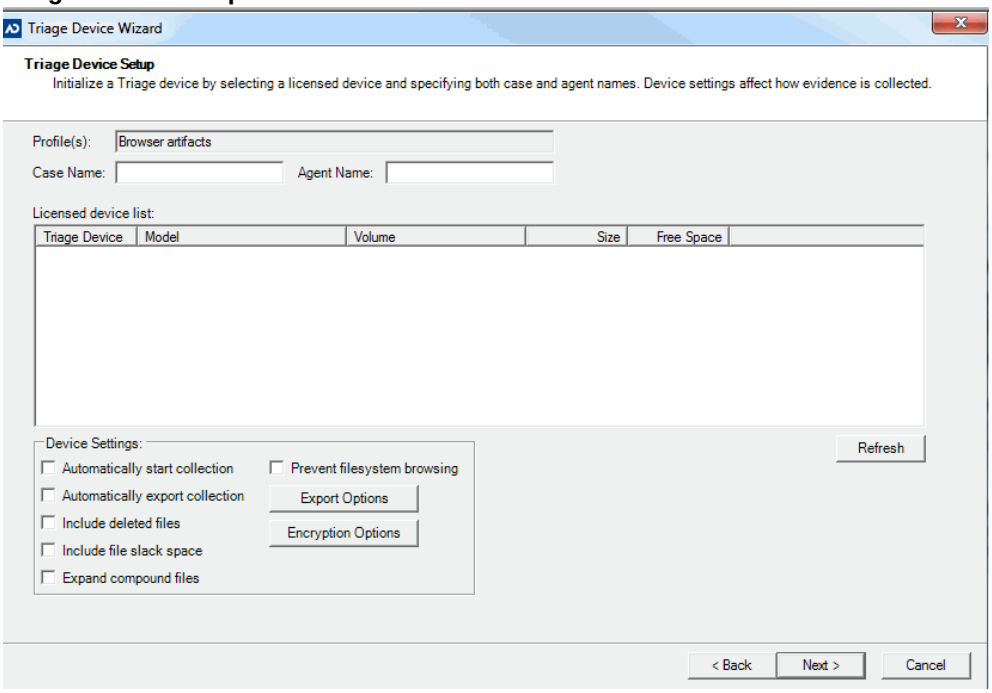
2. Click on the **Create Triage Devices** button.

Triage Device Wizard Profile Screen



3. In the *Select Profile* screen, you can select one or more profiles in the following ways:
   - Drag your mouse to select a group of profiles, or click on a single profile.
   - Hold down CTRL while selecting or deselecting individual profiles.
   - Hold down Shift while selecting the first and the last profiles of a group to select a group of profiles.
4. Click **View Profile Actions** to view the actions that the profile(s) are assigned to perform. These actions are not editable in this screen. See Editing a Profile on page 22 for information on how to edit the actions in the profile.
5. Click **Next**.

Triage Device Setup Wizard Screen



6. In the *Triage Device Setup* screen, enter a *Case Name* and *Agent Name* for the device.
7. Select the USB device that you want to make into a Triage device.

   Note: If you do not see the device that you are looking for, ensure that the device is attached to the computer. Then, ensure that the device is licensed (see Managing Licenses on page 44).

8. Check **Automatically start collection** if you want Triage to automatically collect data on the target system upon start up.

   Note: When a user selects the Automatically start option, and the target has multiple partitions, the Triage Agent will use the Registry from the partition with the most used space and will use all partitions when performing custom file searches.

9. Check **Automatically export collection** if you want Triage to automatically export collected data to the USB device.
10. Check **Prevent filesystem browsing** if you want to prevent the investigator from browsing the file system during the collection process.
11. Check **Expand compound files** if you want to search inside compound files. This should normally be left unchecked, as searching inside compound files takes a considerable amount of time.
12. Check **Include Deleted Files** to include deleted files during collection.
13. Check **Include File Slack Space** to include slack-space during collection.
14. Click **Encryption Options** if you want to specify a password to use when encrypting the collected evidence associated with this profile. Any user will be required to enter the password before they can import collection data back into the Admin console.

    Note: Encrypting a device is not available in the international version of Triage.

Important: If you want to retrieve collections from the device on a different Admin computer, you MUST use a password rather than the default encryption.

15. Click Export Options to configure a network location as a target for collecting data.
See Configuring Export Options on page 51.
16. Click **Next**.

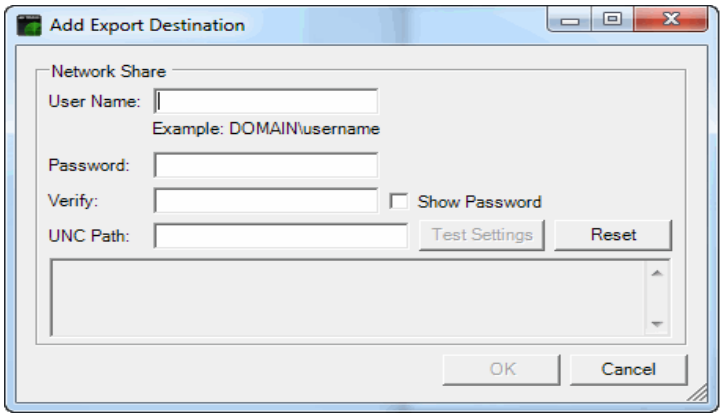
> **Note:** If you have already configured your Triage device, the program will warn you that the program will overwrite the device, and ask you to continue.

17. Click **Finish**.

Configuring Export Options

The Export Options dialog allows you to configure where evidence is saved to a network share. This option makes it easier to save larger collections that may not fit on a USB drive.

Add Export Destination Dialog



Add Export Destination Dialog for the Network Share

Element	Description
User Name	Enter the user name that you will be using to connect to the network share.
Password	Enter the password for the network share. Verify that the password is correct in the field provided.
UNC Path	Enter the UNC path for the network share.
Test Settings	Click **Test Settings** to test the UNC Path connection. The results display in the text window below the UNC Path field.
Reset	Click **Reset** to clear ALL of the fields in the *Add Export Destination* window.

Creating a Bootable Disc

If you are collecting data in the field, it is important to have not only a bootable USB device, but also a bootable copy of the Triage ISO on a disk. It is recommended that you use a disc burning application to burn the Triage ISO to a disc. Use the ADTriageBootable.iso (found on the disc you received with your software) to create a bootable disc.

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

Chapter 5

Collecting Data

About Collecting Data on a Target System

When you collect data on a Target System, you must have a USB device that is formatted as a Triage USB device. You must perform the steps in and Creating a Triage USB Device on page 48 to have a USB device that will collect data on a target system.

Additionally, if you are collecting data in the field, it is recommended that you burn the Triage ISO to a disk, and use the disk in the event that you cannot boot to your USB device.

See Creating a Bootable Disc on page 52.

Once you have completed those tasks, you are ready to collect data on a target system. Triage is designed to collect data from a shut down or live system.

To collect data from a live system, see Collecting Data from a Live System on page 60.

To perform a collection from a shut down system, you must first make the target system boot to the USB device or a bootable CD/DVD. See Booting AD Triage on a Target System on page 61 for information on how to boot to the USB or CD/DVD drive.

After you have set the target system to boot to the USB device or CD/DVD drive, you can then restart the system and collect data. See Automatically Collecting Data on a Shut Down Target System on page 62 for information on what occurs during automatic collection.

Collection Interface Overview

The *Collection* interface is the what you see when you are collecting data on a target system. You can either boot this interface from a shutdown system or launch the interface from a Triage USB device on a live system. Use the following sections as a guide when working with the *Collection* interface.

See About Collecting Data on a Target System on page 54.

See Collecting Data from a Live System on page 60.

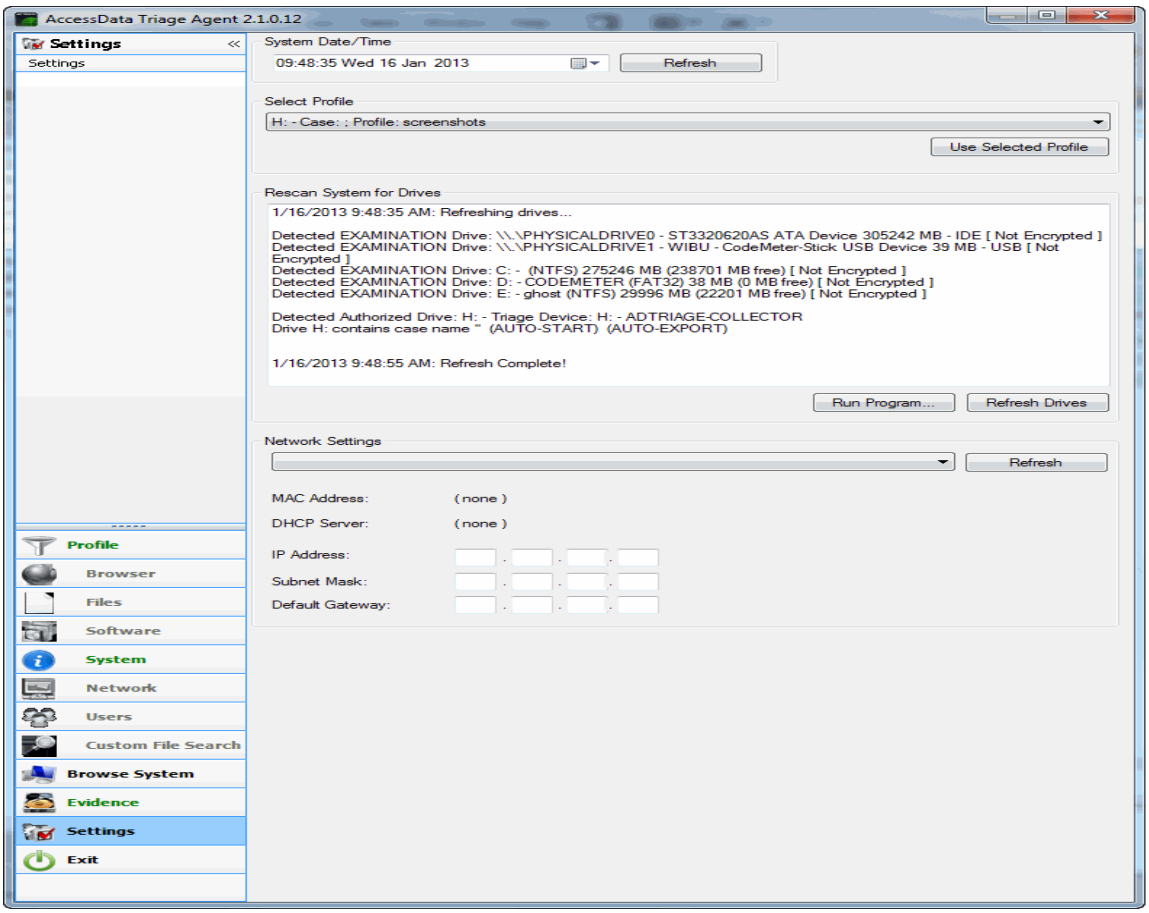
See Booting AD Triage on a Target System on page 61.

See Automatically Collecting Data on a Shut Down Target System on page 62.

See Manually Collecting and Exporting Data on a Target System on page 63.

Use the following figure and table to understand the elements of the Triage *Collection* interface.

Collection Interface Profile Tab



The tabs of the *Collection* interface can appear in the following colors:

- Black: Indicates that collection has not yet begun.
- Orange: Indicates that collection is in process.
- Green: Indicates that collection is complete.
- Red: Indicates that user action is still required.

Elements of the Collection Interface

Element	Description
Case Name	Name saved to the Triage USB device when it was created.
Profile	Name of the profile applied to the Triage USB device.
Primary Collection Partition	Expand drop-down to select a Windows system partition.
Restrict Collection by User	Select a user to filter the collection by user access.
Partitions for Custom File Search	Select a partition(s) from which to collect for custom file searches.
Play Button	Click to start collection.
Action Pane	Lists the actions that will be performed during collection.
Log of Profile Runs Pane	Lists the date and time information for actions performed during collection.
Browser Tab	Displays the status of collection of Browser files.
Files Tab	Displays the status of collection of computer files.
Software Tab	Displays the status of collection of software files.
System Tab	Displays the status of collection of system files.
Network	Displays the status of collection of network files.
Browse System Tab	Click to select specific collected data and create AD1 and RAW files.
Evidence Tab	Click to export collected data, or to view the status of exported collected data.
Settings Tab	Click to view and edit the settings of the *Collection* interface.
Exit	Click to close the *Collection* interface.

Filtering by User Access

Using Triage, you can collect data from a target computer to which one or more users have access. The purpose of this filter is to collect data a user could have created or modified. When user filters are applied, Triage will combine all permissions for the selected users and allow as much access as possible unless it is explicitly denied. Selecting the 'Administrator' user will return data for all users because an administrator has privilege to create/write all files. However, when a single user is selected who belongs to the 'Users' group, typically only data belonging to that user will be collected.

Triage distinguishes between user data and system data for all actions except Custom File Search and Acquire Registry. See Filter by User Access Limitations on page 57.

Actions which collect system data DO NOT apply the user filter when collecting data. If the file containing the desired data is readable, it is extracted and added to the evidence collection (e.g. SAM Users). Actions that collect user data (e.g. Chrome Browser History, Temporary Internet Files, etc.) always check file owner/create/write permissions before extracting data.

Local users and locally cached domain users appear on the profile page of the collection interface when Triage is launched on the target machine. Users are only displayed if the target computer contains SAM and SOFTWARE registry hives. Local group membership for these users is also displayed.

Note: Triage uses NTFS permissions to determine if a user has access to the file. Sometimes investigators will encounter drives formatted with a different file system like FAT32. If the filesystem is something else, Triage will collect the data without regard to permissions.

Filter by User Access Limitations

When performing a Custom File Search, create/write permissions for each file object are matched against the permissions for all selected users. If access is allowed, the file object is added as evidence.

By default, Acquire Registry collects all the known registry hives. Regardless of which users are selected, the SAM, SECURITY, SOFTWARE, and SYSTEM hives will always be included if Triage has read access. User specific hives are included based on create/write permissions of the selected users.

User profile filters don’t apply to non-NTFS file systems. If any of the other filter criteria match the file will be added as evidence.

User Actions

The user data collected on the target computer will depend on the profile that you create and apply to your Triage device. The following actions (selected when creating a profile) will collect user data. All other actions will collect system data.

- Custom File Filters
- Chrome Browser History
- Default Browsers
- Firefox Browser History
- Internet Explorer History

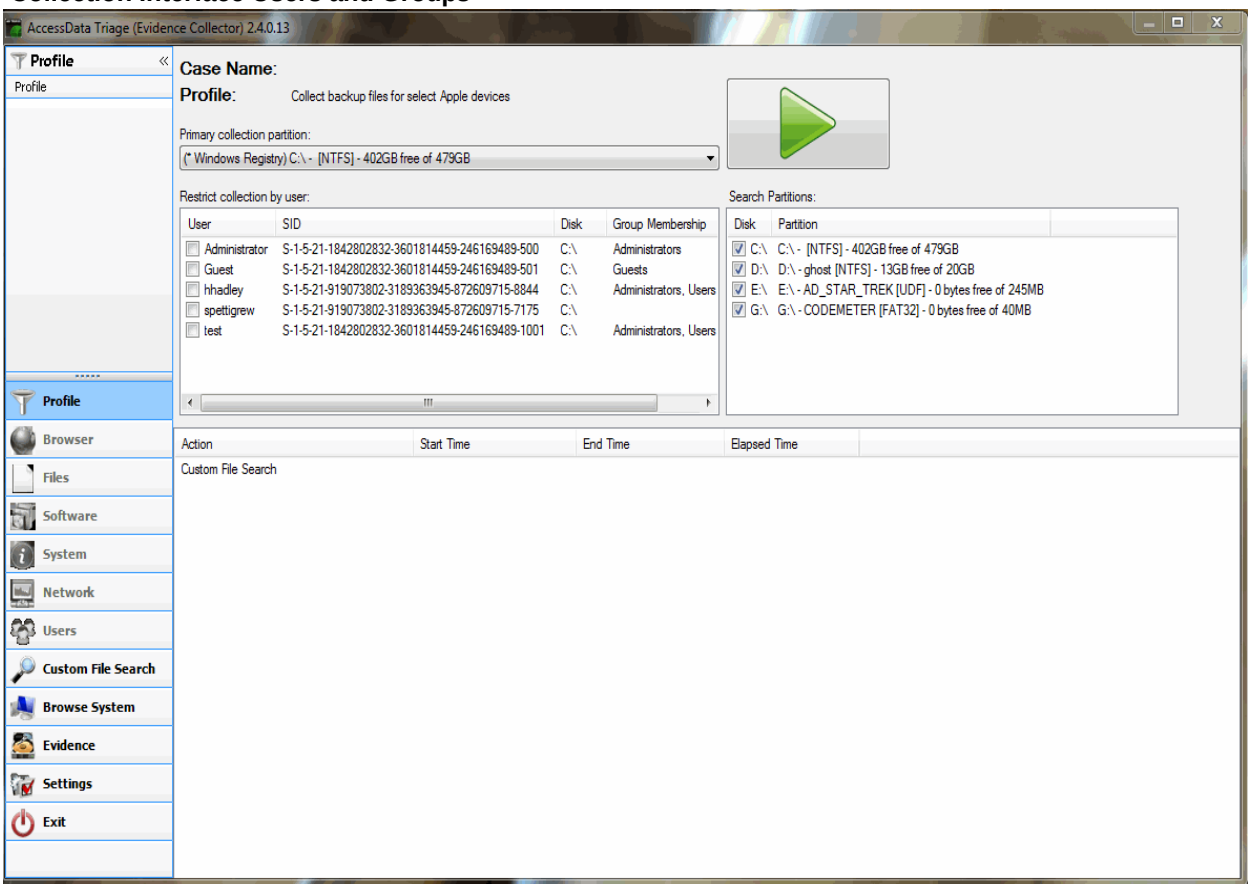
- Internet Explorer Registry Keys
- Typed URLs
- Desktop Files
- MS Office Recently Opened
- Recent Files
- Recently Accessed Media Player Files
- Temporary Files
- Acrobat History
- Application Usage History
- Manually Launched Apps
- Microsoft Management Console
- Acquire Registry
- Typed Paths

Filtering by User Access on a Target Computer

To filter by user access on a target computer

1. Create a Triage profile that includes user actions.
   See User Actions on page 57.
2. Create a Triage device with the previously created profile. Ensure that the device DOES NOT automatically collect data during collection.
3. Run the Triage Agent on the target machine.
   See Collecting Data from a Live System on page 60.
   See Manually Collecting and Exporting Data on a Target System on page 63.

Collection Interface Users and Groups



4. On the *Profile* tab, check a user(s) from the *User Profiles* group box.
5. Click the **Play** button.
   Triage collects the data to which the selected users have access.

> **Note:** If the Profile on the Triage device contains System actions, system data will also be collected. See User Actions on page 57.

Collecting Data from a Live System

You can use Triage to collect data from a live target system. To do this, you must have a bootable USB device or bootable Triage disk. Use the following sections for information on how to obtain these items:

See Managing Licenses on page 44.

See Creating a Triage USB Device on page 48.

See Creating a Bootable Disc on page 52.

Note: In order to use Triage on a live system, it requires that the USB port is not blocked or write protected.

To collect data on a live system

1. Insert the Triage USB device into target system.
2. Do one of the following:
   - In the Windows prompt, select to run **AD Triage**.
   - Open the folder for the device, open the *Agent* folder, and run the **TriageAgent.**
3. In the *AccessData Triage Language Selector* dialog, select your language from the pull down menu. Click **OK**.
4. In the Collection window, perform one of the following tasks:
   - Data will automatically be collected and exported if you selected Auto-Start Collection and Auto-Export Collection. See Automatically Collecting Data on a Shut Down Target System on page 62.
   - Manually collect the data from the target system. See Manually Collecting and Exporting Data on a Target System on page 63.

Booting AD Triage on a Target System

You can use Triage to collect data from a shut down system, but to do this, you will need to boot the system to a Triage USB device, or a Triage disk. Use the following sections for information on how to obtain these items:

See Managing Licenses on page 44.

See Creating a Triage USB Device on page 48.

See Creating a Bootable Disc on page 52.

This section describes how to set up the target system to boot to the USB device or disk.

To boot AD Triage on a target system

1. Insert the bootable disk or bootable USB device. (See Creating a Bootable Disc on page 52 for more information on how to make a bootable disk.)
2. Start the target system and enter the BIOS.

   Note: On Intel system boards, press **F2** or **F12** during start up to enter the BIOS. On non-Intel systems, press **Delete** or **Esc** during start up to enter the BIOS.

3. Edit the BIOS boot sequence to one of the following:
   - Make the CD/DVD drive boot before the hard drive if you are booting using a disk.
   - Make the USB boot before the hard drive if you are booting using the USB device (see Managing Licenses on page 44 for making a bootable USB device).
4. Save and exit the BIOS.

   Note: Press **CTRL > ALT > Delete** if the system has trouble booting. If this does not work, hold down the power button for 4 to 5 seconds.

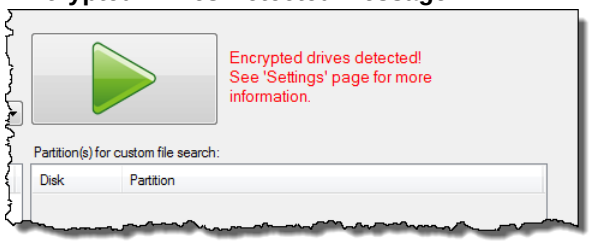
Automatically Collecting Data on a Shut Down Target System

The following steps occur after you have set the target system to boot to the USB device or CD/DVD drive, and you have restarted the target system:

1. The target system boots into Windows.
2. The AD Triage collection application launches.
3. AD Triage detects drives.
4. If there are encrypted drives, Triage will notify you as to which drives are encrypted. Data will not be collected from encrypted drives. The following types of encryption are detected by Triage:
   - PGP
   - Safeguard (Utimaco)
   - Safeguard Enterprise (Utimaco)
   - McAfee Safeboot
   - Guardian Edge
   - Point Sec
   - Bitlocker (Vista only)

Note: If encryption prevents Triage from locating a drive with the installed operating system, the investigator will not be able to execute the profile. However, if the investigator has browsing rights, it's possible to manually select the evidence and export it.

Encrypted Drives Detected Message



5. AD Triage collects the data for the profile on the USB device (if **Automatically Start Collection** was selected when creating a Triage USB).
6. AD Triage exports the data to the USB device (if **Automatically Export Collection** was selected when creating a Triage USB).
7. Close the *Collection* window and shut down the system.

Manually Collecting and Exporting Data on a Target System

If you did not check to Auto-start collection when you created your Triage USB device, you will need to manually start collection when on the target system.

To manually collect data from a target system

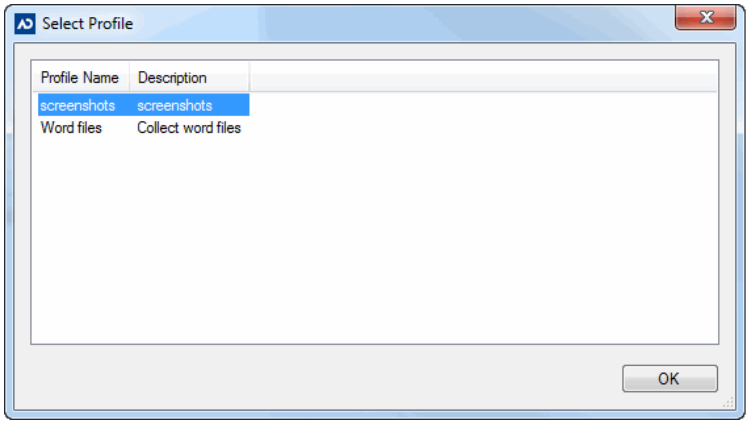
1. After setting up the target system to boot to the USB device or CD/DVD drive, restart the computer. The *AD Agent* window opens.

   Note: If the screen says that *No Profiles Were Found*, ensure that the licensed USB (with a profile on it) is connected and click the **Refresh Drives** button on the **Settings** tab.

2. If your Triage device has multiple profiles, the program prompts you to select the profile to run. Highlight the profile and click **OK**.

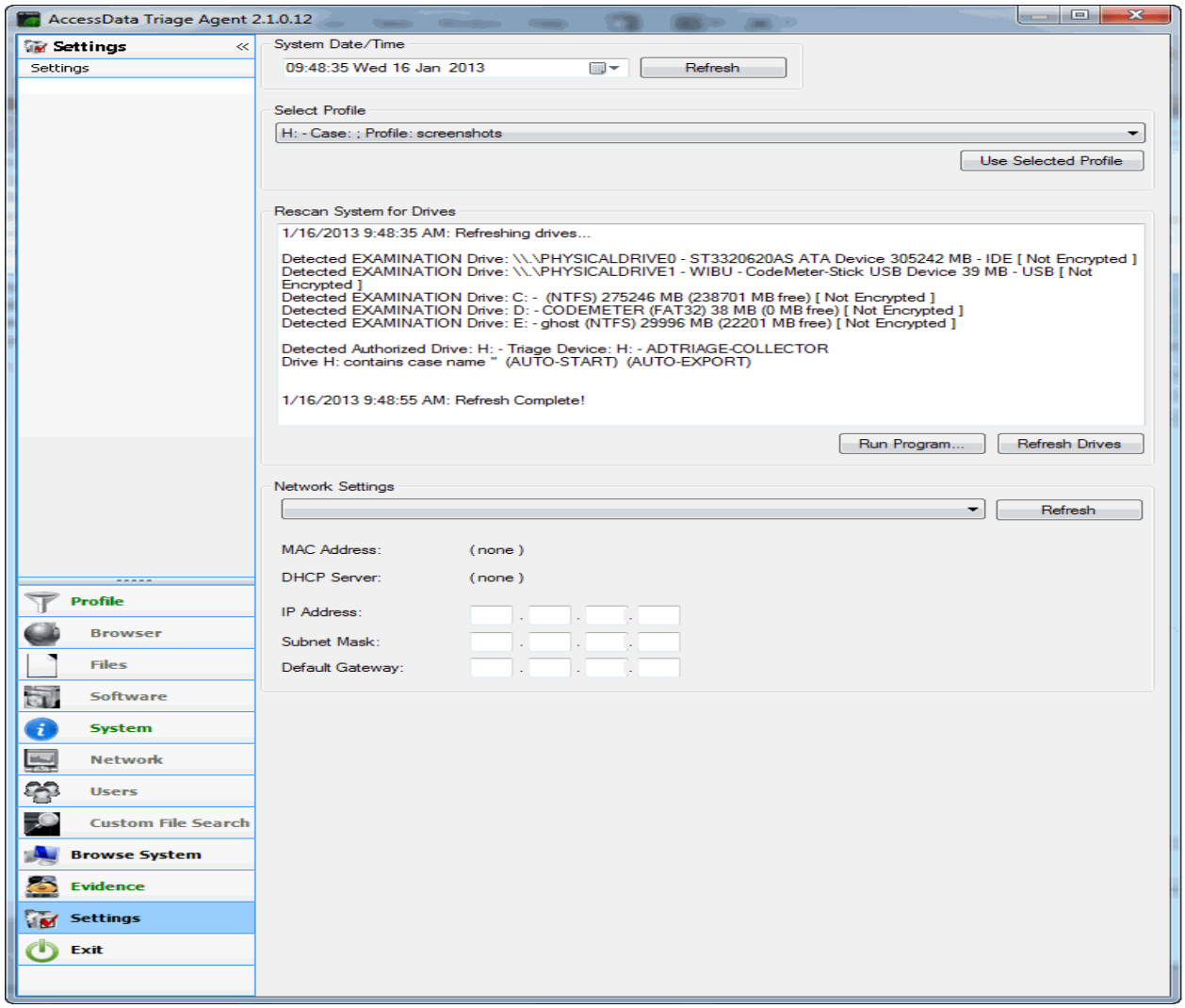
   Note: If you have two different Triage devices attached to the system at the same time, switching between profiles will properly refresh the user interface.

Select Profile Dialog



Note: After entering the Collection Interface, you can change the profile by selecting a different profile from the **Select Profile** menu and clicking **Use Selected Profile**.

Collection Interface



3. If there are encrypted drives, Triage will notify you as to which drives are encrypted. Data will not be collected from encrypted drives. The following types of encryption can be detected by Triage:
   - PGP
   - Safeguard (Utimaco)
   - Safeguard Enterprise (Utimaco)
   - McAfee Safeboot
   - Guardian Edge
   - Point Sec
   - Bitlocker (Vista only)

   Note: If encryption prevents Triage from locating a drive with the installed operating system, you will not be able to execute the profile. However, if you have browsing rights, it's possible to manually select the evidence and export it.

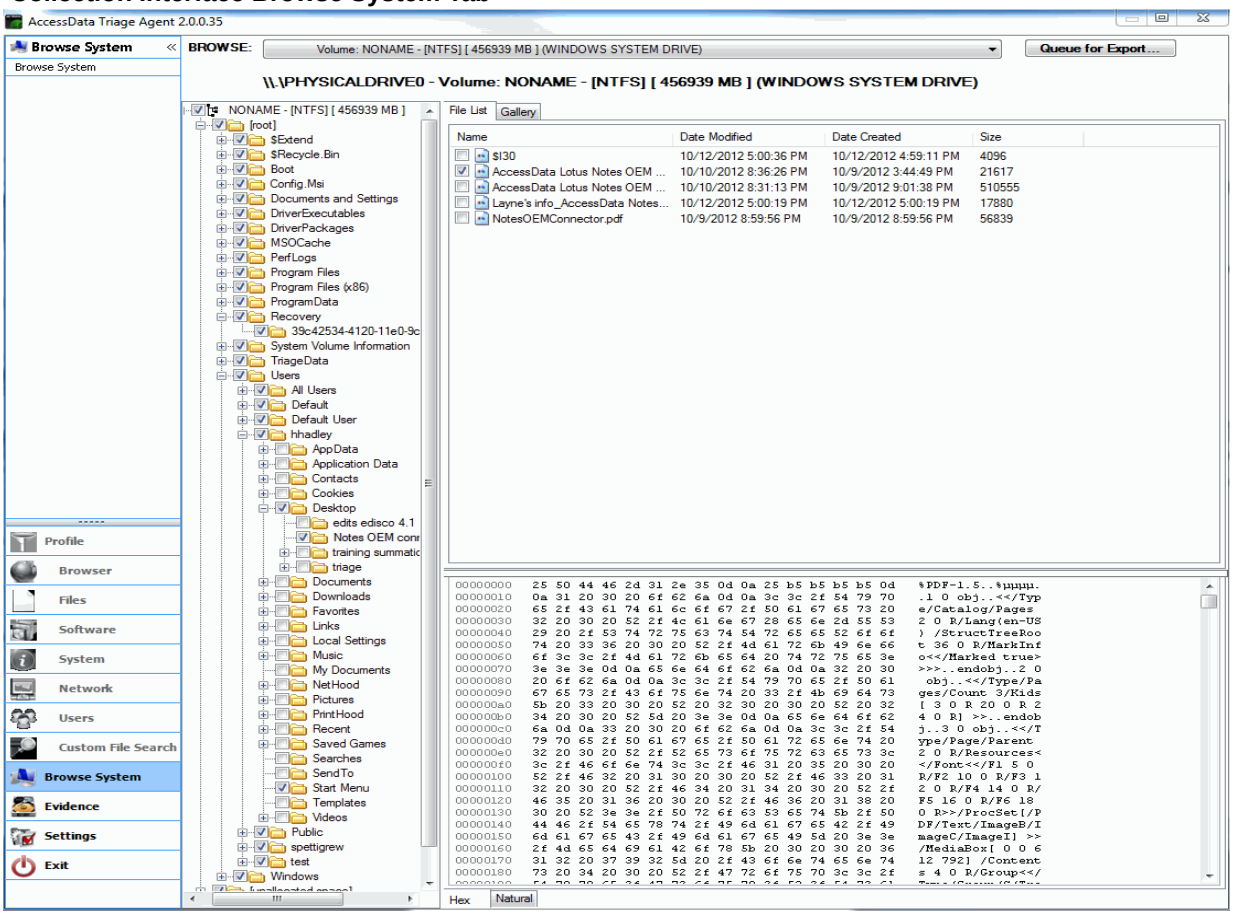
4. Click the **play** button on the *Profiles* tab.

   Collection begins. You can identify the progress of the collection by the colors of the words on the tabs. Green indicates that the action has been completed.

Note: If you click the play button twice in one session, the subsequent collection will overwrite the previous collection.

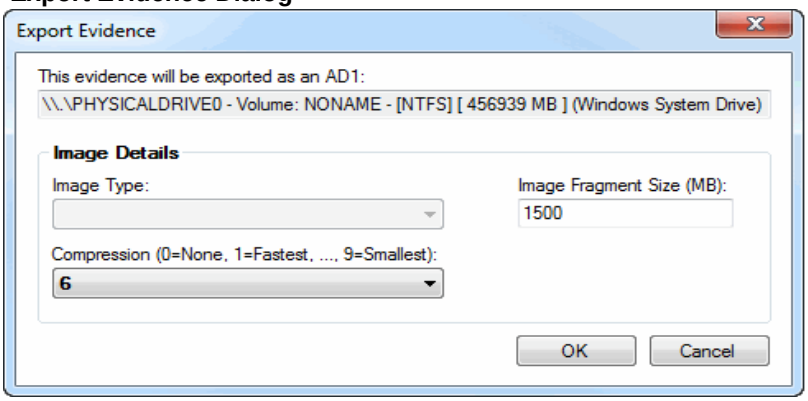
Note: If you checked **Automatically start collection** when creating a Triage USB device, AD Triage will automatically collect data on the target system upon boot up. And the play button will not be available.

Collection Interface Browse System Tab



5. After collection is complete, you can select the *Browse System* tab and check the specific system drives that you want to acquire. See Browse System Tab on page 68.
   You can view files in the following views:
   - **File List**: Displays files in a list.
   - **Gallery**: Displays thumbnails of files.
6. Click **Queue for Export** (optional).

Export Evidence Dialog

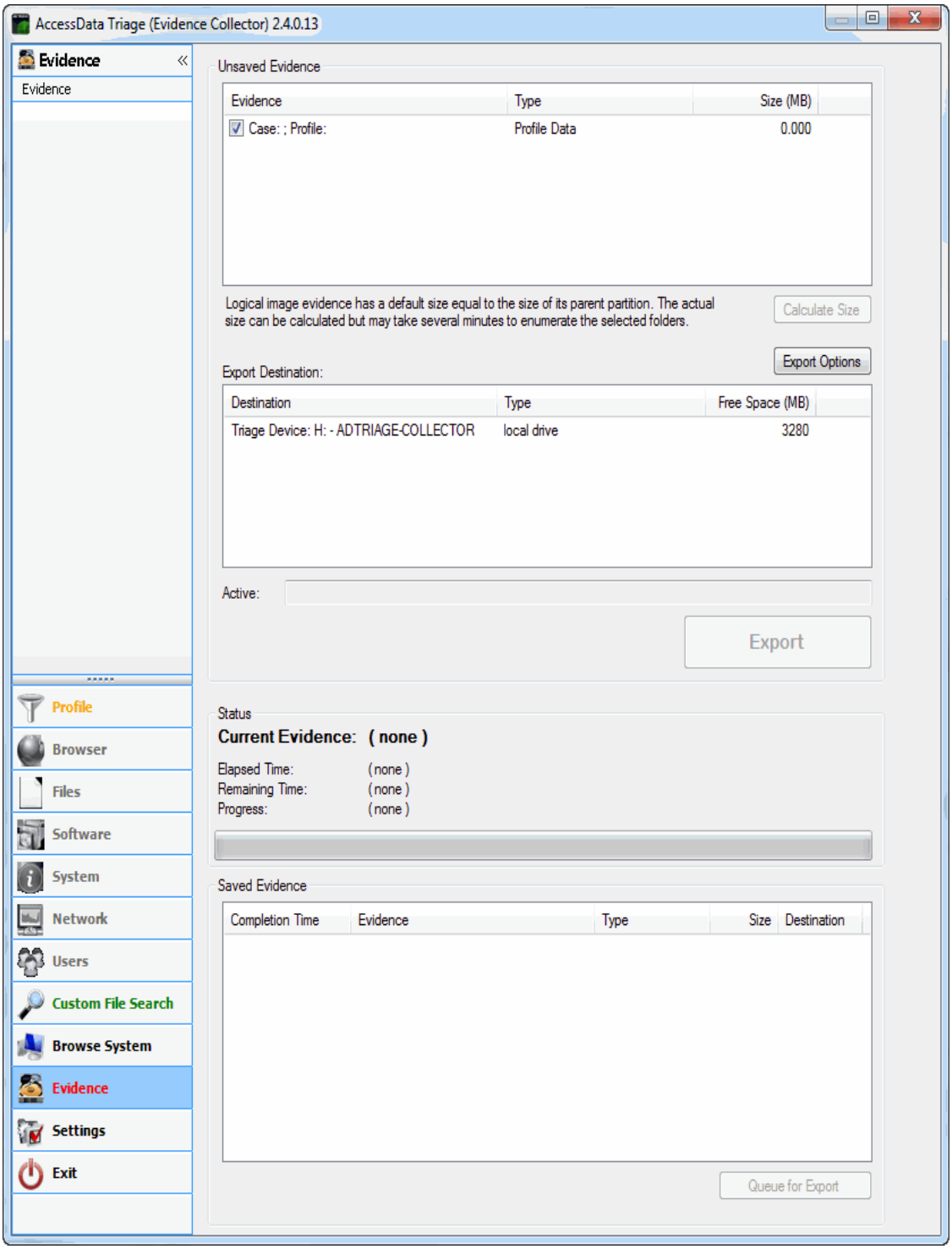


6a. In the *Export Evidence* dialog, you can see the following fields:

- The UNC path that the evidence will be exported to appears in the field.
- If the evidence is an image, you can select the type of image.
- You can select the value for compression in the **Compression** menu.
- You can change the **Image Fragment Size** or leave the default value.

7. If there is data that has not been exported, the *Evidence* tab appears in red. Click on the **Evidence** tab.

Collection Interface Evidence Tab



8. All data that still needs to be exported appears in the *Pending Export* pane. Select the items you want to export, select the location where you want to export the data, and click **Export**.
   Collected data and AD1 files are exported to the selected device/location. Data that was successfully exported appears in the *Successfully Exported* pane. When all the evidence has been exported, the *Evidence* tab appears in green.

Note: If you click the export button twice in one session, the second export will overwrite the previous export on the Triage device.

9. After you have exported your data, you can calculate the estimated size of the export to determine the actual required destination storage size. But, calculation can take a long time, so it should only be used when necessary. Click **Calculate Size** to perform this task.
10. Click **Re-pend Selected Item for Export** if you want exported items to reappear in the *Pending Export* pane.
11. Click **Exit** to close the *Collection* window. If you have not exported all your evidence, you will be alerted that you have pending evidence.
12. Shut down the system.

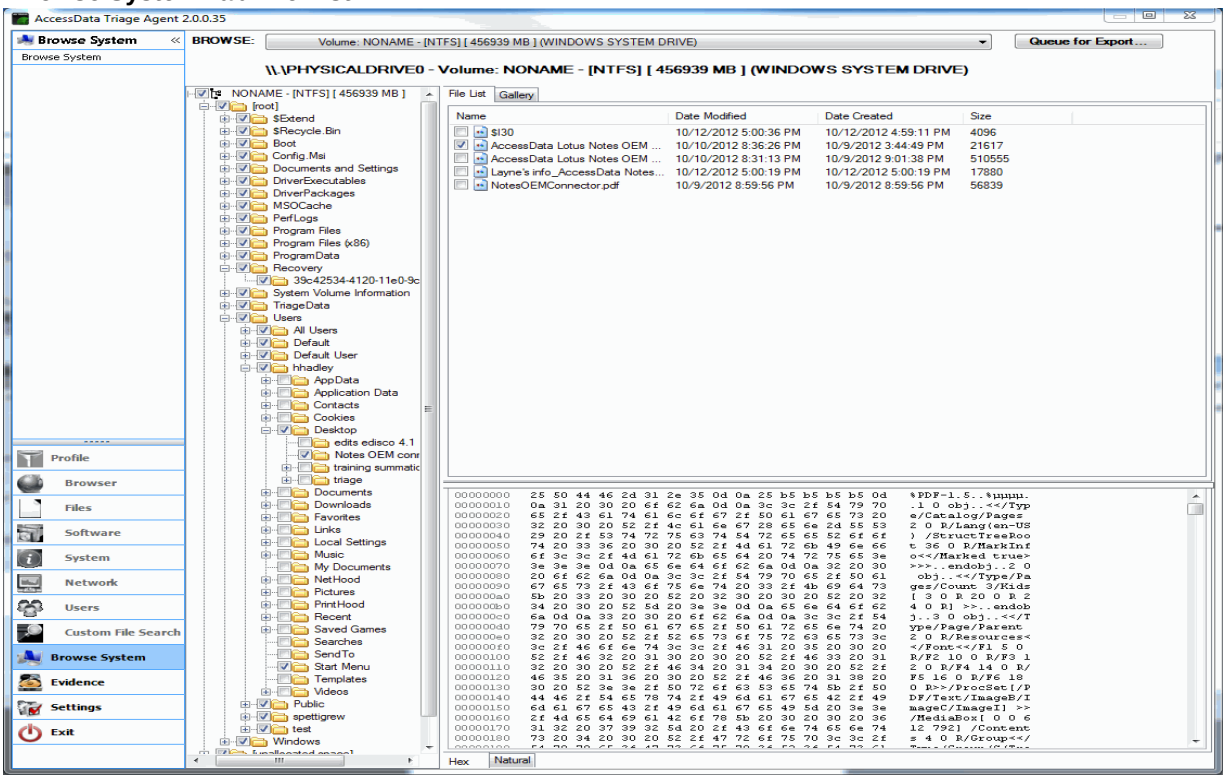
Note: Remember to reset the BIOS on the target system to boot from the hard drive first after you are done collecting data.

Browse System Tab

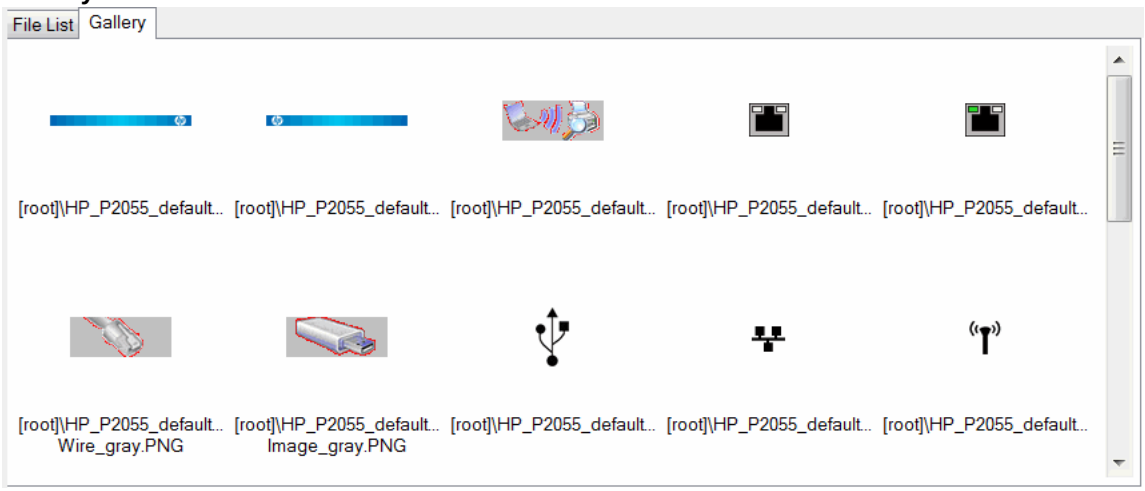
After you run a collection, you can select the Browse System tab in the Collection interface to browse the files of collected data and create AD1 and RAW files.

Note: The Browse tab will be deactivated if Prevent FileSystem Browsing is checked when the device was initially created.

Browse System Tab File List



Gallery View



Elements of the Browse System Tab

Element	Description
File Tree	Expand and collapse files to navigate through the collected files. Select a file to view the contents in the *File List* or *Gallery* tabs. Check a file to include it in your AD1 or RAW file for export.
File List Tab	Lists the items in the selected folder in the *File Tree*. **Note:** The Agent review mode can only display up to 1000 results in List mode at a time. The Admin review mode does not have this limitation and will show all results.
Gallery Tab	Displays thumbnails of the items in the selected folder in the *File Tree*. Right-click the thumbnail to change the size.
Hex Tab	Displays the hex for the selected file.
Natural Tab	Displays the natural view for the selected file.
Browse Drop-down	Expand to select the partition in which you want to browse.
Queue for Export	Click to create an AD1 or RAW file containing the checked items from the File Tree. You can export these files from the *Evidence* tab.

There are many columns that may display in the file list tab. The columns displayed depend upon the files collected, the filter criteria that is selected, and the order in which the criteria was evaluated for a given file.

Depending upon those criteria, any of the following columns could be viewed:

Columns Displayed in File List Tab

Columns	Description
Name	Lists the name of the files.

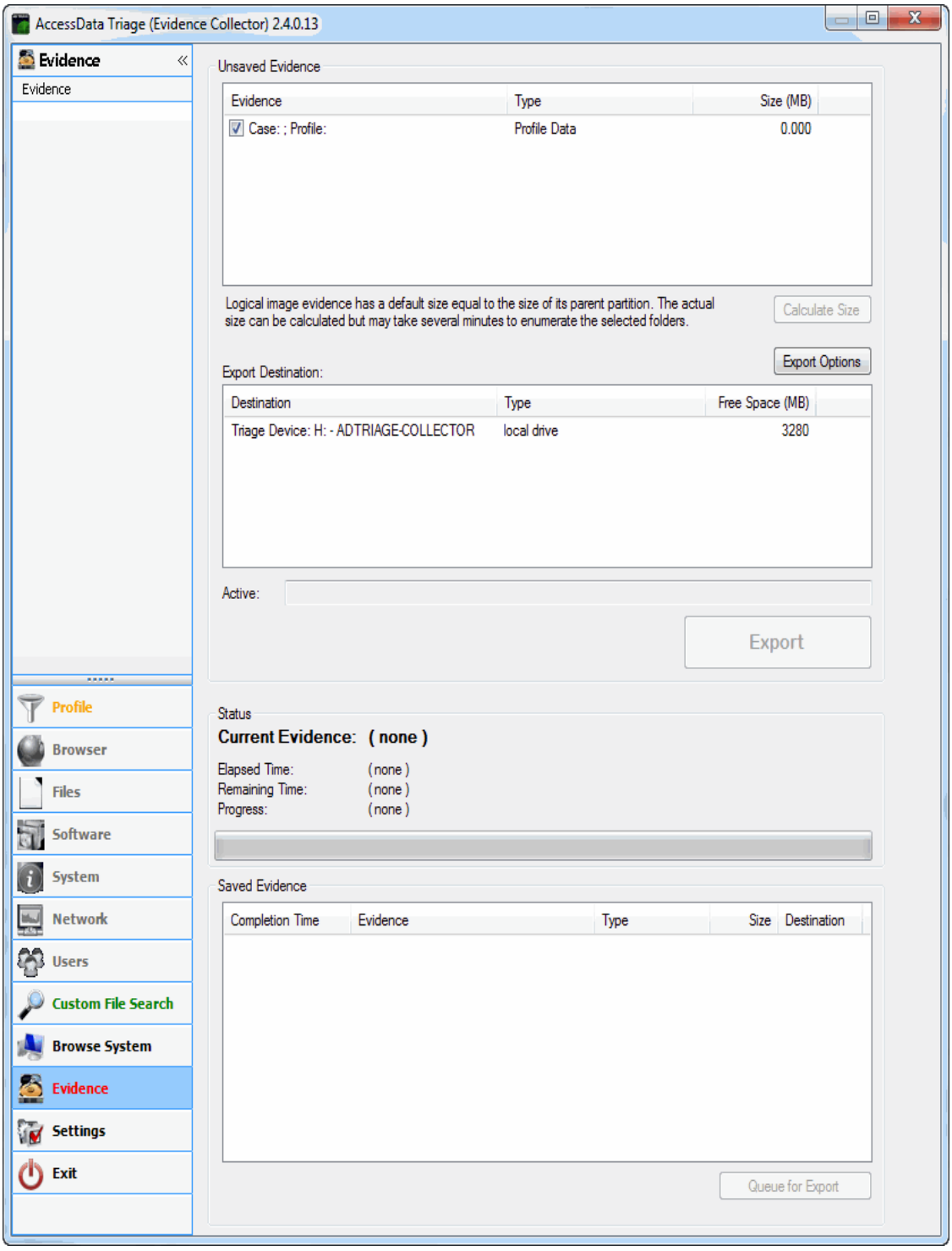
Columns Displayed in File List Tab

Columns	Description
Date Modified	Lists the date the file was modified.
Date Created	Lists the date the file was created.
Size	Lists the size of the file in MB.
Keyword List	Displays the name of the keyword list that was a match for the file.
Data	Data varies depending upon the file examined. Data could be hex values, binary, IP addresses, or paths.
EID Score	Displays the Explicit Image Detection (EID) score of matching files. The column will only show a value if the EID Score is above a preset limit.

Evidence Tab

After you have run the collection, you can click the **Evidence** tab to export collected data, or to view the status of exported collected data.

Evidence Tab



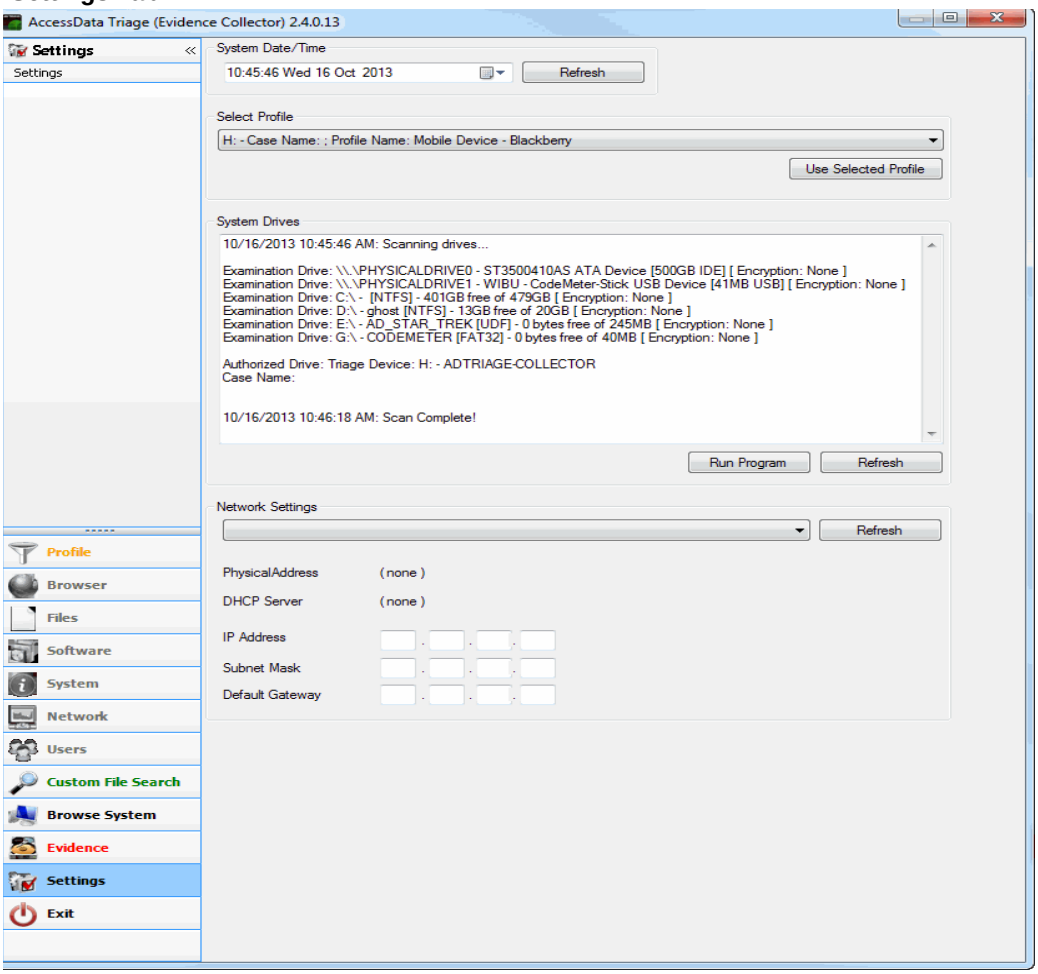
Elements of the Evidence Tab

Element	Description
Pending Export Pane	Displays the items queued for export. Check the items that you want to export.
Export Destination Pane	Displays the possible destinations for export. The Triage USB device that you booted from is the default location for export.
Export Options	Click to add an export destination. If you are exporting to a network share, enter the network **User Name** and **Password** in the appropriate fields. You can select **Show Password** if you are not sure you entered the password correctly. Enter a valid UNC Path and click **Add**.
Calculate Size	Click to calculate the size of the export before exporting. Data exported may be larger than the device that you are saving to.
Export	Click to export the checked items in the *Pending Export* pane.
Status Group Box	Displays the status of the export.
Successful Export Pane	Displays the successfully exported items.
Re-Pend Selected Item for Export	Click if you want exported items to reappear in the *Pending Export* pane.

Settings Tab

Click the Settings tab to view and edit the settings of the *Collection* interface.

Settings Tab



Elements of the Settings Tab

Element	Description
Date/Time Drop-down	Expand and select a date and time.
Set Date/Time Button	Click to set the date and time to what you selected in the Date/Time drop-down.
Refresh Drives Button	Click if the agent didn't recognize your Triage USB device. This refreshes the agent and searches for the drive again.
Network Settings Group Box	Use the items in this group box to set up the network for export.

Using Kanguru and IronKey Encrypted Devices

If you are using a Kanguru and IronKey encrypted device when collecting data, the process differs slightly from non-encrypted keys. To use an encrypted key on a shutdown system, you must boot from a burned CD.

Chapter 6

Reviewing Collected Data

Managing Collected Data

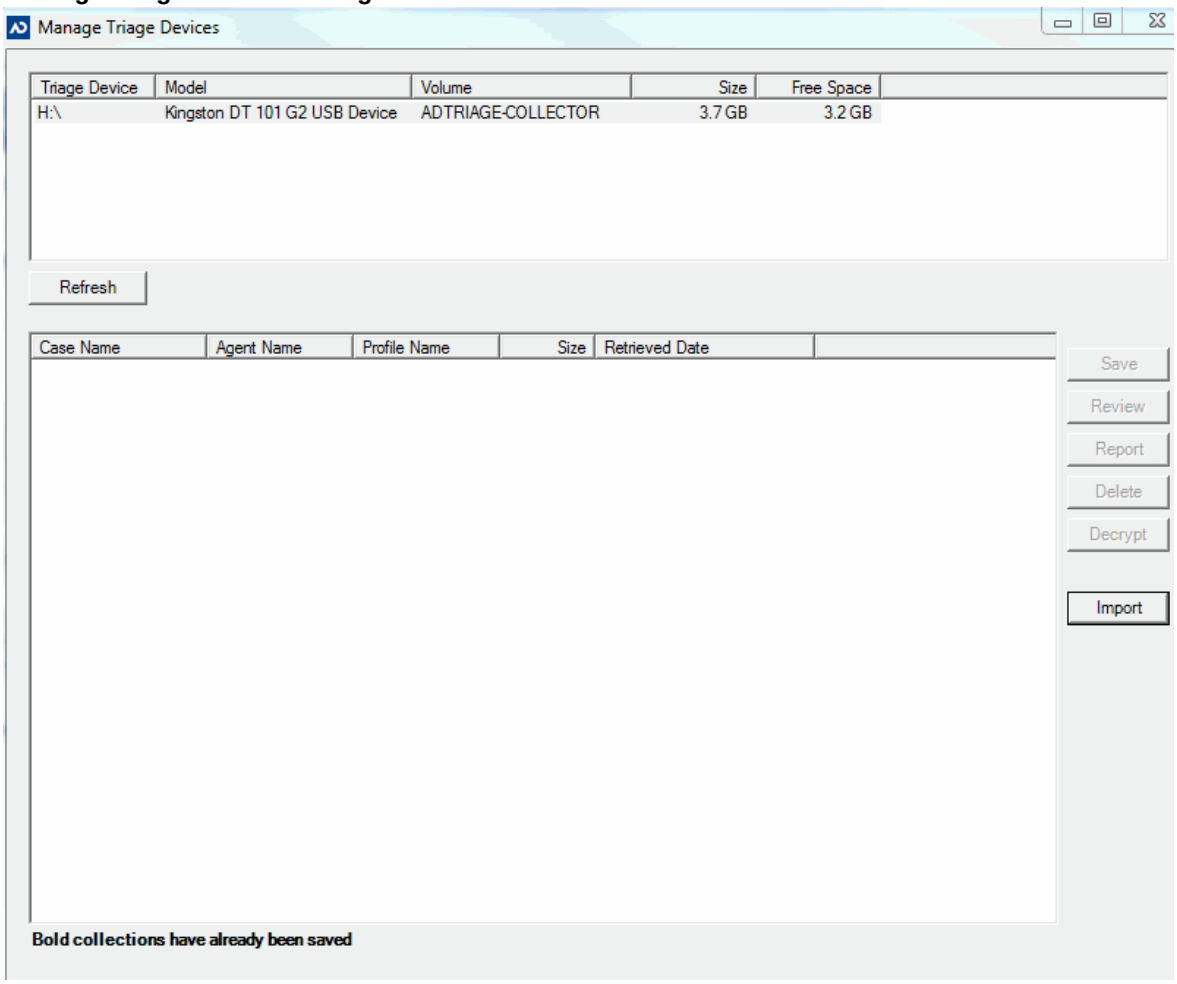
If you exported your collected data from a target system to your Triage USB device, you can save the data in Triage Admin, review the data, and generate reports.

Before saving a collection, ensure that you have enough available disk space on your Admin computer. If you do not have sufficient disk space, collections will not import completely.

Manage Triage Devices Dialog

Open the *Manage Triage Device*s dialog by clicking the **Manage Triage Devices** button on the *Devices* tab of the *Admin* window. Use this window to save collected evidence, review collected evidence, generate reports, and delete collected evidence (see Saving Collected Data on page 78). Use the following figure and table to understand the elements in the *Manage Triage Devices* dialog.

Manage Triage Devices Dialog



Elements of the Manage Triage Devices Dialog

Element	Description
Devices Pane	Lists the connected Triage USB Devices.
Refresh Triage Devices Button	Click to refresh the Devices pane.
Profile on Triage Device	Lists the name of the profile on the selected Triage device.
Collection Pane	Lists the Case Name, Agent Name, Profile Name, Collection Size, and Collection Retrieved Date for each collection on the selected Triage device.
Save Collection Button	Click to save the selected collection in the Triage files.
Review Collection Button	Click to review the selected collection.
Generate Report Button	Click to generate a report of the selected collection.
Delete Collection Button	Click to delete the selected collection from the USB device.
Decrypt Button	If you have encrypted the Triage device, you can click to decrypt the device.

Elements of the Manage Triage Devices Dialog (Continued)

Element	Description
Import Collection Button	Click to import a collection to the Triage device. When you click the **Import Collection** button, a dialog appears and you can browse to the folder that contains the collection that you want to import.
Evidence Pane	Lists file sizes for the selected USB device.
Format Drive Button	Click to reformat the selected USB device. This will delete all existing data on the device.
License Count	This will appear at the bottom of the dialog if you signed up for an unlimited amount of devices license, but a limited amount of recoveries. The count of total and available licenses are listed here.

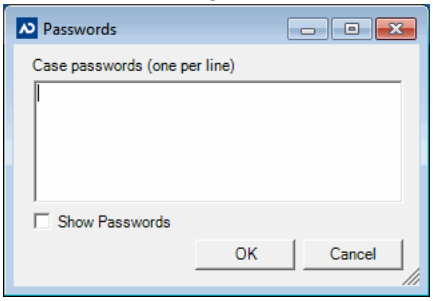
Saving Collected Data

To save collected data

1. Ensure that the USB device is connected to the computer.
2. In the *Triage Admin* console, click the **Devices** tab.
3. Click **Manage Triage Devices**.

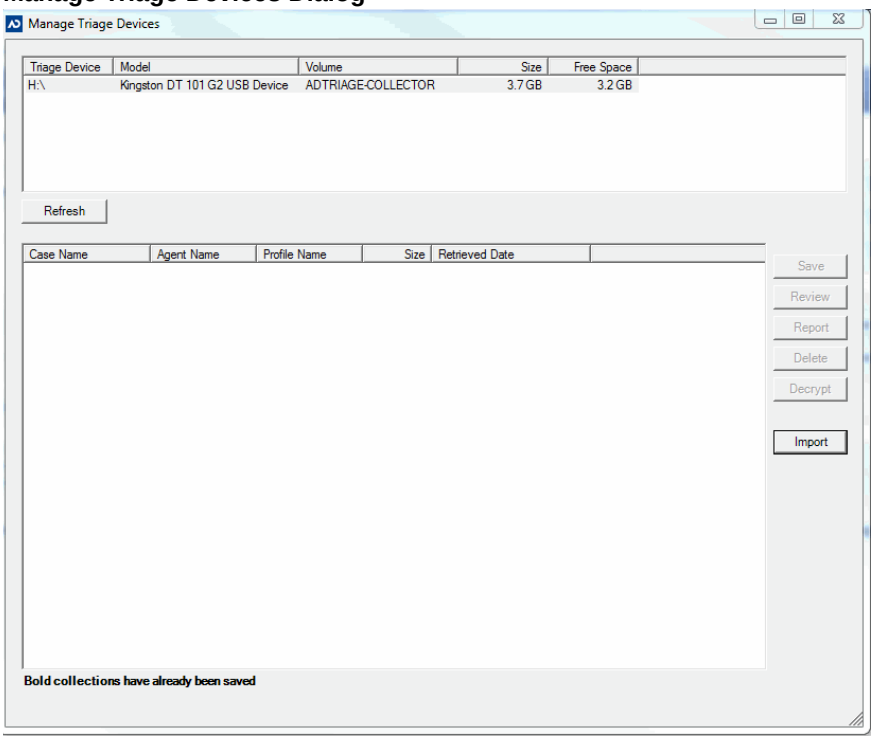
   The Passwords dialog appears if any of the collected evidence files are encrypted with a user password.

Passwords Dialog



4. If the *Passwords* dialog appears, enter the passwords for all of the collected evidence files. You can enter one password per line. Click **OK**.

Manage Triage Devices Dialog



5. Select the USB device that contains the collections that you want to save from the upper pane.
6. Collections appear in the lower pane, select the collection that you want to save.

Note: You can review collections, generate reports and delete collections from this dialog. More information on performing these tasks are covered in Managing Saved Collections on page 80.

7. If the collection is encrypted, you will need to click the **Decrypt** button before you can save the collection.
8. Click **Save**.
9. In the *Save Collectio*n dialog, browse to the location where you want the case data to save.

   The collection is saved in the designated location.
10. Close the dialog.

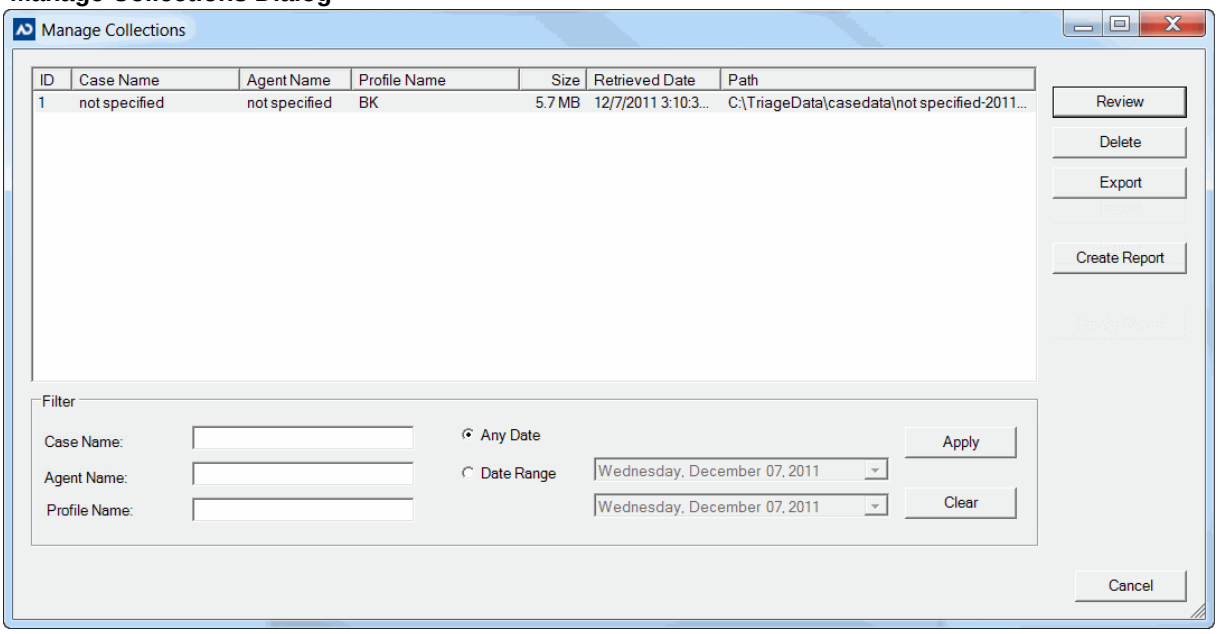
Managing Saved Collections

Once you have saved your collected data, you can then review it, generate reports, and export the collection from the *Manage Collections* dialog. You can view a list of all the saved collections in the *Manage Collections* dialog. This section will help you filter and manage all your saved collections.

Manage Collections Dialog

Open the *Manage Collections* dialog by clicking the **Manage Saved Collections** button on the *Admin* tab. Use the following figure and table to understand the elements in the *Manage Collections* dialog.

Manage Collections Dialog



Elements of the Manage Collections Dialog

Element	Description
Manage Collections Pane	Lists recent actions performed in the *Triage Admin* main window. Click the column headings to sort by column. Double-click the ID number to open the evidence file.
Review Button	Click to open the *Recover Evidence* dialog. See Reviewing Saved Collections on page 82.
Generate Report Button	Click to open the *Generate Reports* dialog. See Generating Reports for Saved Collections on page 83.
Export Button	Click to create an AD1 image of the evidence. See Exporting Saved Collections on page 84.

Elements of the Manage Collections Dialog (Continued)

Element	Description
Delete Button	Click to delete the selected evidence from the profile. See Deleting a Saved Collection on page 85.
Profile Name Field	Enter text to filter the *Manage Collections* pane by the *Profile Name* column.
Case Name Field	Enter text to filter the *Manage Collections* pane by the *Case Name* column.
Agent Name Field	Enter text to filter the *Manage Collections* pane by the *Agent Name* column.
Clear Button	Click to remove filters and return to the default collection view.
Any Date Radio Button	Select to filter without a date range selected.
Date Range Radio Button	Select to filter the *Manage Collections* pane by selected date range.
Apply Button	Click to filter the *Manage Collections* pane by the criteria you entered.
Cancel Button	Click to close the Manage Collections dialog.

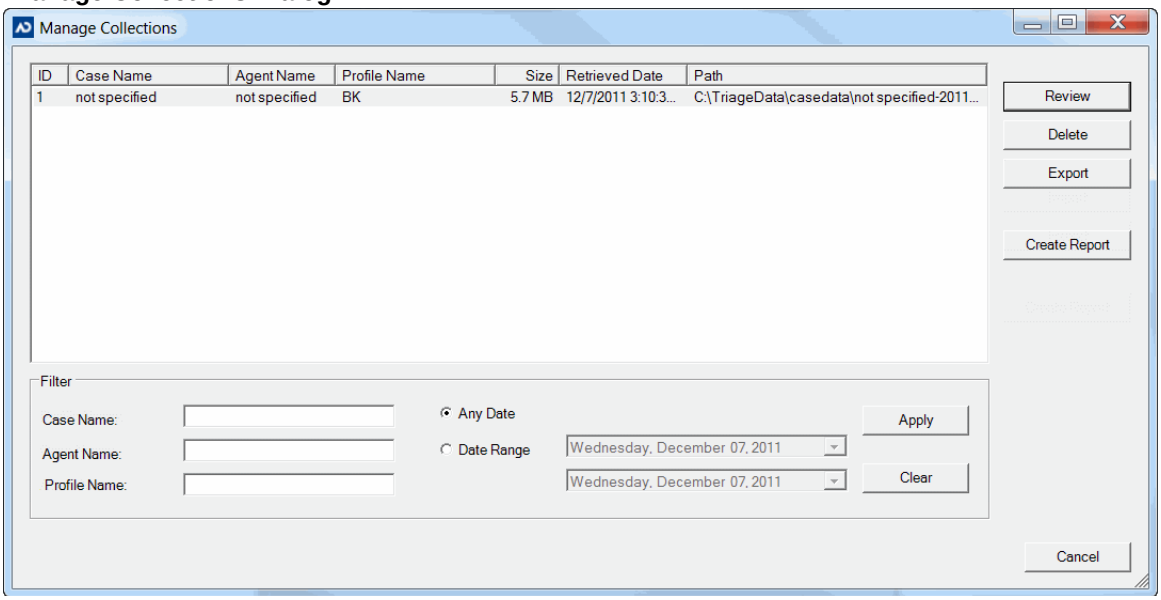
Filtering Saved Collections

The list of collections in the *Manage Collections* dialog is a list of ALL the collections saved to AD Triage. If you are looking for a specific collection, you may need to filter the list to find the collection you are looking for.

To filter saved collections

1. In the *Admin* console, click the **Admin** tab.
2. Click the **Manage Saved Collections** button.

Manage Collections Dialog



3. In the *Manage Collections* dialog, you can filter the list of collections by specifying the name of the profile, the name of the case, the name of the agent, and/or a specified date range. Enter your filtering criteria and click **Search**.

4. Once you have found the collection(s) you are looking for, you can perform the following actions:
   - Review the collection: See Reviewing Saved Collections on page 82.
   - Generate a report: See Generating Reports for Saved Collections on page 83.
   - Export the collection: See Exporting Saved Collections on page 84.
   - Delete the collection: See Deleting a Saved Collection on page 85.
   - Import a collection: See Importing a Saved Collection on page 85.

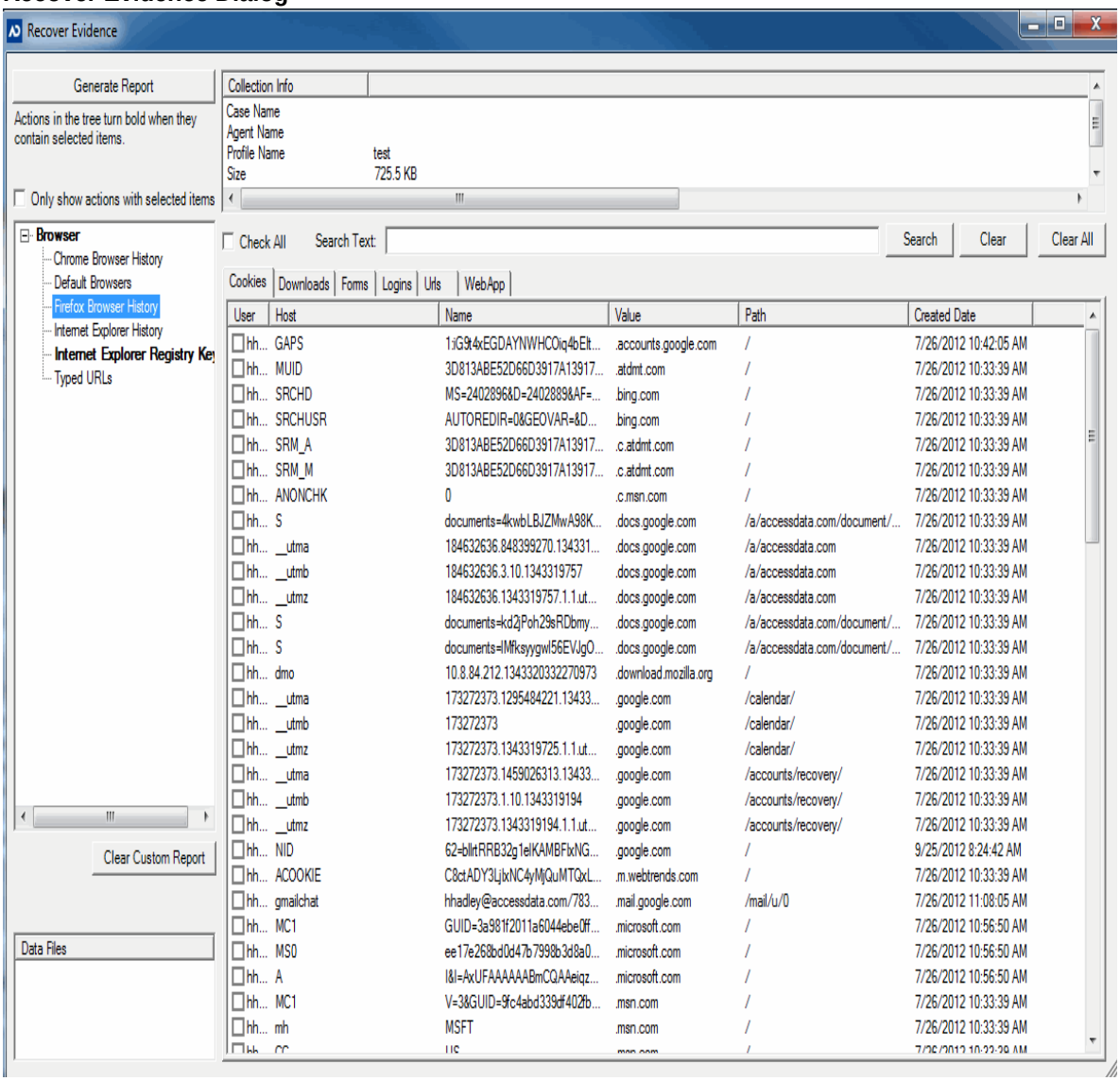
Reviewing Saved Collections

Once you have found the collection/s you are looking for in the *Manage Collections* dialog using the filters (see Filtering Saved Collections on page 81), you can then review the collected data.

To review saved collections

1. In the *Manage Collections* dialog, select the collection that you want to review.
   See Filtering Saved Collections on page 81.
2. Click **Review**.

Recover Evidence Dialog



3. In the *Recover Evidence* dialog, use the left panes to navigate the collected data and the AD files created during collection. Check the files that you would like to include in a custom report.

   Note: If using Gallery View, you can right-click the thumbnail and change the size if desired.

4. Click **Generate Report** to create a report of the collection, then follow the steps found in Generating Reports for Saved Collections on page 83.
5. Close the *Recover Evidence* dialog.

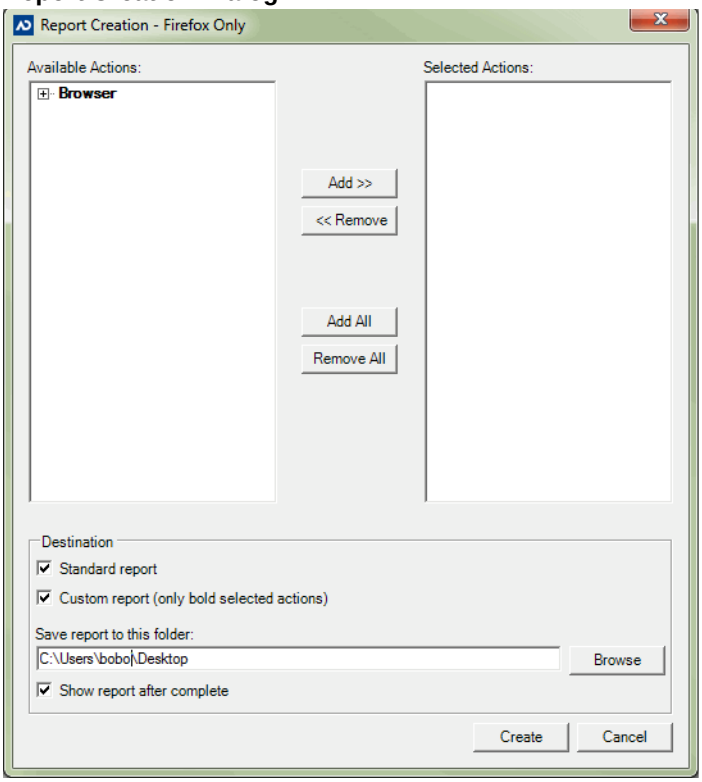
Generating Reports for Saved Collections

Once you have found the collection/s you are looking for in the *Manage Collections* dialog using the filters (see Filtering Saved Collections on page 81), you can then generate a report of the collected data.

To generate a report for a saved collection

1. In the *Manage Collections* dialog, select the collection for which you want to generate a report. See Filtering Saved Collections on page 81.
2. Click **Generate Report**.

Report Creation Dialog



3. Check whether you want to generate a *Standard* or *Custom Report*.
4. Highlight the collected data that you want to include in your report and click **Add**.

   Note: Items in bold are those items that you selected when you reviewed your data.

5. **Browse** to the location where you would like to save the generated report.
6. Check **Show report after complete** to open the report after it has been generated.
7. Click **Create**.
   If you checked to view the report, it opens in an internet browser.

Exporting Saved Collections

Once you have found the collection/s you are looking for in the *Manage Collections* dialog using the filters (see Filtering Saved Collections on page 81), you can then export the collection to a designated location. This makes a copy of the collection and saves it in the location you select. You can then use the exported file and import it into another *AD Triage Admin* system for others to review.

To export a saved collection

1. On the *Admin* tab of the *Admin* console, click **Manage Saved Collections**.
   See Manage Collections Dialog on page 80.
2. In the *Manage Collections* dialog, select the collection that you want to export.
   See Filtering Saved Collections on page 81.
3. Click **Export Collection.**
4. Browse to the location where you want to save the exported file.
5. Click **OK**.

Deleting a Saved Collection

Once you have found the collection/s you are looking for in the *Manage Collections* dialog using the filters (see Filtering Saved Collections on page 81), you can then delete the collected data from your saved collection file. This will not remove the collected data from the USB device that it originated from.

To delete a saved collection

1. On the *Admin* tab of the *Admin* console, click **Manage Saved Collections**.
   See Manage Collections Dialog on page 80.
2. In the *Manage Collections* dialog, select the collection that you want to delete.
   See Filtering Saved Collections on page 81.
3. Click **Delete Collection**.
4. Click **OK**.

Importing a Saved Collection

If you want to import a collection that is saved from another *Triage Admin* console or if you want to recover a collection that is saved on a remote share, you can use the *Import Collection* feature. Import Collection auto detects whether the case data is encrypted

To import a saved collection

1. On the *Admin* tab of the *Admin* console, click **Manage Saved Collections**.
   See Manage Collections Dialog on page 80.
2. In the *Manage Collections* dialog, click **Import Collection**.
3. Browse to the location of the file or remote directory that you want to import and click **OK**.
4. In the *Import Collection* dialog, select the collection(s) that you want to import and click **Import Collections**.
5. In the message box that appears, click **Yes**.

   Note: If the collection was encrypted with a password on the device that collected the data, you will be prompted to enter the password for the collection. This enables you to import data that was collected on a different Admin machine.

   The collection is added to your saved collections.

Chapter A

Appendix A Troubleshooting

This section deals with common problems that may occur with AD Triage.

Updating Triage's Database

After launching Triage, you may see the following dialog:

The database file (v{0}) has been previously upgraded and is now newer than the expected files (v{1}). The current database is only compatible with a more recent release of Triage

If you receive this message, you need to either re-install the version that is compatible with the database or delete the Triage database.

Note: If you delete the Triage database, you will lose all of the data in the database.

To re-install Triage

- ❖ See Installing AD Triage Admin Console on page 14.

To delete Triage's database

1. In the Windows search field, enter **C:\ProgramData\AccessData\Products\ADTriage2**
2. Open the *ADTriage2* folder and delete the **TriageAdmin.s3db** file.
3. Close the folder and return to Triage. Triage will write a new database file to the ADTriage2 folder, correcting the error.

Exporting to a Network Location

You may be unable to export to a network location (i.e. \\servername\directory) which is already mapped to a local drive. If you have this issue, disconnect the mapped local drive before configuring the Triage Export option.

To export to a network location that is already mapped to a local drive

1. In Windows, disconnect the mapped drive. For information on disconnecting network drives, consult your Windows documentation.
2. Configure the Triage Export option. See Manually Collecting and Exporting Data on a Target System on page 63.
3. Execute the collection.

4. When the collection is complete, re-map your network drive.

Licensing Issues

Each license of Triage comes with a maximum number of client counts, or licenses to create devices. These client counts are found in **Admin>Manage Licenses**. There is an issue that refreshing your licensing dongle more than once will drop the licensing client count to zero, and you will be unable to create Triage devices. To avoid this problem, do not refresh the dongle more than once. However, if the licensing client counts drop to zero, contact support to add the correct client counts back to the dongle.

Domestic and International Versions

Domestic and international versions of Triage cannot run on the same network.