

Searching in Summation



AccessData Legal and Contact Information

Document date: December 15, 2014

Legal Information

©2014 AccessData Group, Inc. All rights reserved. No part of this publication may be reproduced, photocopied, stored on a retrieval system, or transmitted without the express written consent of the publisher.

AccessData Group, Inc. 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, Inc. 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, Inc. 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, Inc. 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, Inc.
1100 Alma Street
Menlo Park, California 94025
USA

www.accessdata.com

AccessData Trademarks and Copyright Information

AccessData®	MPE+ Velocitor™
AccessData Certified Examiner® (ACE®)	Password Recovery Toolkit®
AD Summation®	PRTK®
Discovery Cracker®	Registry Viewer®
Distributed Network Attack®	ResolutionOne™
DNA®	SilentRunner®
Forensic Toolkit® (FTK®)	Summation®
Mobile Phone Examiner Plus®	ThreatBridge™

A trademark symbol (®, ™, etc.) denotes an AccessData Group, Inc. trademark. With few exceptions, and unless otherwise notated, all third-party product names are spelled and capitalized the same way the owner spells and 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

BSD License: Copyright (c) 2009-2011, Andriy Syrov. All rights reserved. Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met: Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer; Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution; Neither the name of Andriy Syrov nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission. THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

WordNet License

This license is available as the file LICENSE in any downloaded version of WordNet.

WordNet 3.0 license: (Download)

WordNet Release 3.0 This software and database is being provided to you, the LICENSEE, by Princeton University under the following license. By obtaining, using and/or copying this software and database, you agree that you have read, understood, and will comply with these terms and conditions.: Permission to use, copy, modify and distribute this software and database and its documentation for any purpose and without fee or royalty is hereby granted, provided that you agree to comply with the following copyright notice and statements, including the disclaimer, and that the same appear on ALL copies of the software, database and documentation, including modifications that you make for internal use or for distribution. WordNet 3.0 Copyright 2006 by Princeton University. All rights reserved. THIS SOFTWARE AND DATABASE IS PROVIDED "AS IS" AND PRINCETON UNIVERSITY MAKES NO REPRESENTATIONS OR WARRANTIES, EXPRESS OR IMPLIED. BY WAY OF EXAMPLE, BUT NOT LIMITATION, PRINCETON UNIVERSITY MAKES NO REPRESENTATIONS OR WARRANTIES OF MERCHANT- ABILITY OR FITNESS FOR ANY PARTICULAR PURPOSE OR THAT THE USE OF THE LICENSED SOFTWARE, DATABASE OR DOCUMENTATION WILL NOT INFRINGE ANY THIRD PARTY PATENTS, COPYRIGHTS, TRADEMARKS OR OTHER RIGHTS. The name of Princeton University or

Princeton may not be used in advertising or publicity pertaining to distribution of the software and/or database. Title to copyright in this software, database and any associated documentation shall at all times remain with Princeton University and LICENSEE agrees to preserve same.

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 require 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, Inc. 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 License Manager 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 website.

AccessData Contact Information

Your AccessData Sales Representative is your main contact with AccessData. 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:

AccessData Mailing Address, Hours, and Department Phone Numbers

Corporate Headquarters:	AccessData Group, Inc. 1100 Alma Street Menlo Park, California 94025 USAU.S.A. <i>Voice: 801.377.5410; Fax: 801.377.5426</i>
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:	<i>Voice: 800.574.5199, option 1; Fax: 801.765.4370</i> <i>Email: Sales@AccessData.com</i>
Federal Sales:	<i>Voice: 800.574.5199, option 2; Fax: 801.765.4370</i> <i>Email: Sales@AccessData.com</i>
Corporate Sales:	<i>Voice: 801.377.5410, option 3; Fax: 801.765.4370</i> <i>Email: Sales@AccessData.com</i>
Training:	<i>Voice: 801.377.5410, option 6; Fax: 801.765.4370</i> <i>Email: Training@AccessData.com</i>
Accounting:	<i>Voice: 801.377.5410, option 4</i>

Technical Support

Free technical support is available on all currently licensed AccessData solutions.

You can contact AccessData Customer and Technical Support in the following ways:

AD Customer & Technical Support Contact Information

AD SUMMATIONand AD EDISCOVERY	Americas/Asia-Pacific: 800.786.8369 (North America) 801.377.5410, option 5 Email: legalsupport@accessdata.com
AD IBLAZE and ENTERPRISE:	Americas/Asia-Pacific: 800.786.2778 (North America) 801.377.5410, option 5 Email: support@summation.com
All other AD SOLUTIONS	Americas/Asia-Pacific: 800.658.5199 (North America) 801.377.5410, option 5 Email: support@accessdata.com
AD INTERNATIONAL SUPPORT	Europe/Middle East/Africa: +44 (0) 207 010 7817 (United Kingdom) Email: emeasupport@accessdata.com

AD Customer & Technical Support Contact Information (Continued)

<i>Hours of Support:</i>	Americas/Asia-Pacific: Monday through Friday, 6:00 AM– 6:00 PM (PST), except corporate holidays. Europe/Middle East/Africa: Monday through Friday, 8:00 AM– 5:00 PM (UK-London) except corporate holidays.
<i>Web Site:</i>	http://www.accessdata.com/support/technical-customer-support
	The Support website allows access to Discussion Forums, Downloads, Previous Releases, our Knowledge base, a way to submit and track your “trouble tickets”, and in-depth contact information.

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, Lab and the entire Resolution One platform. They can help you resolve any questions or problems you may have regarding these solutions.

Contact Information for Professional Services

Contact AccessData Professional Services in the following ways:

AccessData Professional Services Contact Information

Contact Method	Number or Address
<i>Phone</i>	North America Toll Free: 800-489-5199, option 7
	International: +1.801.377.5410, option 7
<i>Email</i>	services@accessdata.com

Contents

- AccessData Legal and Contact Information 3**
- Contents 8**
- Chapter 1: Introduction to Searching Data 11**
 - About Searching Data 11
 - Search Limitations 12
- Chapter 2: Running Searches 13**
 - Running a Quick Search 13
 - Building Search Phrases 15
 - Using Search Operators 15
 - Using Boolean Logic Options 17
 - Using ? and * Wildcards 18
 - Searching Numbers 19
 - Searching for Virtual Columns 19
 - Running a Subset Search 20
 - Returning to a Previous Search 20
 - Searching in the Natural Panel 21
 - Using Global Replace 21
 - Committing a Global Replace Job 22
 - Using Dates and Times in Search 23
 - Using Dates and Times in Searches 23
 - How Time Zone Settings Affect Searches 23
 - Viewing the Display Time Zone 23
 - Using the Search Excerpt View 24
 - Using Search Reports 26
 - About Search Reports 26
 - Generating and Downloading a Search Report 26
 - About the Search Report Details 27
- Chapter 3: Running Advanced Searches 28**
 - Running an Advanced Search 28
 - Advanced Search Operators 31
 - Advanced Search Operators Exceptions 31

Understanding Advanced Variations	33
Using the Term Browser to Create Search Strings	34
Importing Index Search Terms	35
Chapter 4: Re-running Searches	36
The Search Tab	36
Running Recent Searches	37
Clearing Search Results	37
Saving a Search	38
Sharing a Search	39
Chapter 5: Using Filters to Cull Data	40
Filtering Data in Case Review	40
About Filtering Data with Facets.	40
The Facets Tab	43
Available Facet Categories	45
Examples of How Facets Work	48
Using Facets	53
Caching Filter Data	54
Filtering by Column in the Item List Panel	55
Clearing Column Filters	55
Object Types	56
Chapter 6: Using Visualization	58
Culling Data with Visualization.	58
Files Visualization	59
Emails Visualization	62
Chapter 7: Using Visualization Social Analyzer	65
About Social Analyzer	65
Accessing Social Analyzer	67
Social Analyzer Options	68
Analyzing Email Domains in Visualization	69
Analyzing Individual Emails in Visualization	69
Chapter 8: Using Visualization Heatmap	70
Chapter 9: Using Visualization Geolocation	72
About Geolocation Visualization	72
Geolocation Components	72
Geolocation Workflow	73
General Geolocation Requirements.	73

Viewing Geolocation EXIF Data	73
Using Geolocation Tools	75
The Geolocation Map Panel	75
Using the Geolocation Grid	78
Filtering Items in the Geolocation Grid	78
Using Geolocation Columns in the Item List	79
Using Geolocation Column Templates	80
Using Geolocation Facets	80
Using Geolocation Visualization to View Security Data	81
Prerequisites for Using Geolocation Visualization to View Security Data	81
Viewing Geolocation IP Locations Data	83
Using the Geolocation Network Information Grid	83
Geolocation Filter	84

Chapter 1

Introduction to Searching Data

This document will help you filter and search through data in the Project Review.

About Searching Data

You can use searching to help you find files of interest that are relevant to your project. After you perform a search, you can save your search or share your search with groups. Then, you can filter your result set to further cull down evidence. As you find relevant files, you can tag the files with Labels, Issues, or Categories for further review or for export.

When you search data, you use search phrases to find relevant evidence. A search phrase is any item that you would receive a search hit on, such as a word, a number, or a grouping of words or numbers.

See [Building Search Phrases](#) on page 15.

You can search for text that is either in the file name or in the body of a file. You can narrow the scope of the search to only checked items in the list, or search through the entire list. And you can select a column in the *Item List* panel and filter on that specific column.

When you start a search, be mindful of the items in the list that you are starting with. For example, if you have applied a facet filter to show only DOC files, and you search for a text string that you think is in a PDF file, it will not find it. However, the same is not true for column filters. If you have applied a column filter to show only DOC files and you search for a text string that you think is in a PDF file, it will locate the file, regardless of the previous column filter application.

Searching Results

When you run a search, any items in your data that contain the search phrase are displayed in the *Item List*. When you view an item in the *INSO view*, the terms in the search phrase are highlighted.

You need to be aware of the following when viewing highlighted terms:

- After the first page of search results are available, the application retrieves the excerpts for the word/phrase hits on the document through a separate workflow. Depending upon the load on the system, highlights might take longer to appear.
- Search results are not highlighted in the view if the word phrases is split on separate lines, especially in documents created in ASCII, such as text files.

- If you have a document where the text is arranged in columns, search results that appear in the same column or span across multiple columns do not highlight in the *INSO* view. The *Text* view should highlight the results accurately.

To search data, see information about the following:

- [Running Searches](#) (page 13)
- [Running an Advanced Search](#) (page 28)
- [Running Recent Searches](#) (page 37)
- [Saving a Search](#) (page 38)

Search Limitations

When performing a Quick Search or Advanced Search, if you have over 10,000 total characters of search text, the search may fail and the application may become non-responsive.

Chapter 2

Running Searches

You can perform the following search tasks:

- [Running a Quick Search](#) (page 13)
- [Searching for Virtual Columns](#) (page 19)
- [Running a Subset Search](#) (page 20)
- [Searching in the Natural Panel](#) (page 21)
- [Using Global Replace](#) (page 21)
- [Using Dates and Times in Search](#) (page 23)
- [Using the Search Excerpt View](#) (page 24)
- [Using Search Reports](#) (page 26)
- [Running an Advanced Search](#) (page 28)

When running a search, you build and use search phrases.

See [Building Search Phrases](#) on page 15.

Running a Quick Search


In most projects, relevant data and privileged information in a data set is found using quick searches. You can use the basic search field in the *Item List* panel to help you perform fast filtering on selected evidence.

When you start a search, be mindful of the items in the list that you are starting with.

See [About Searching Data](#) on page 11.

Important: A processing option, *Disable Tab Indexing*, disables the reindexing of labels, categories, and issues. With this option, the application prevents reindexing from occurring as frequently while you are reviewing data, and search counts appear correctly. This option is enabled by default. If this option is enabled, in Review, the following text is displayed: *Tag indexing is disabled*. However, you can still search for specific tags using a field search, such as “Label contains xxx”.

To run a quick search

1. Log in as a user with Run Search privileges.
2. Click the *Project Review* button  in the *Project List* panel next to the project.
3. In *Project Review*, ensure that the *Project Explorer*, the *Item List*, and *Natural* panel are showing.
4. Select the data that you want to search in by doing the following:

- 4a. In the *Project Explorer*, the default scope selection includes all evidence items in the project. Using the check boxes, uncheck items to exclude items from the scope of the search. These scope items include:
 - Document Groups
 - Production Sets
 - Transcripts
 - Notes
 - Exhibits
 - Labels
 - Issues
 - Categories
- 4b. In the *Facets* tab of the *Project Explorer*, you may select any combination of facets to apply to the current search scope.
- 4c. Click the **Apply** check mark button in the top of the *Project Explorer*. This will apply the currently selected scope and any selected facets to the *Item List*, allowing you to search and review on the resulting subset. The facets will persist through searches until you clear them. Scopes may be changed and searches re-run by use of the *Apply* button as well. After updating a facet or scope item, you may click the *Apply* button, which will update the scope and re-run any search that has not been cleared out by use of the *Clear Search* button in the *Search Options* menu of the *Item List* panel.
5. In the search bar of the *Item List* panel, enter a search phrase.

A search phrase can be either one word or or number or multiple words. You may also use operators or boolean search phrases.

See [Building Search Phrases](#) on page 15.
6. Click **Go** to execute the search.

The search is performed within the specified scope and searches the body content of the documents within the scope. Also depending upon the type of search query, the query will also search the documents' metadata. Search results appear in the *Item List* panel.

If you are searching by keyword, you can select a document from your search results, and see highlighted instances of the word in the *INSO view*. The instances will also be highlighted in the text view and in the *Item List* if there are results in the metadata.

Quick searches will also appear in the *Recent Searches* on the *Searches* tab of the *Project Explorer*.

Note: You are unable to perform a quick search for values in the *ProductionDocID* column. To search for values in the *ProductionDocID* column, use *Advanced Search*. See [Running an Advanced Search](#) on page 28.

Building Search Phrases

When you search data, you use search phrases to find relevant evidence. A search phrase is any item that you would receive a search hit on, such as a word, a number, or a grouping of words or numbers.

A search phrase can be any of the following:

- A single term, such as a word or number
For example, **patent**. Any document with the term “patent” will be found.
- A string of terms (within parentheses)
For example, **2010 patent application**. Any document with the string “2010 patent application” will be found.
- Multiple terms with boolean operators, such as AND or OR
For example, **patent AND 2010**. Any document with both “patent” and “2010” will be found.

See the following about building search phrases:

- See [Using Search Operators](#) on page 15.
- See [Using Boolean Logic Options](#) on page 17.
- See [Using ? and * Wildcards](#) on page 18.
- See [Searching Numbers](#) on page 19.
- See [Search Limitations](#) on page 12.

Using Search Operators

You can use a Boolean search to find the logical relationships among the search terms and phrases that you enter. A Boolean search consists of the following three full logical operators:

- OR
- AND
- NOT

Note: The NOT operator by itself is not an option in Advanced Search. The Not Contains and Not Equals operators are available in Advanced Search. However, you can use the NOT operator in Quick Search.

If you use more than one logical operator, you should use parentheses to indicate precisely what you want to search for. For example, the phrase **apple and pear or orange** could mean either **(apple and pear) or orange**, or it could mean **apple and (pear or orange)**. Use parentheses to clarify which of the two searches that you want.

However, if you want to execute searches that contain parentheses as part of the search term, you should enclose the search term with double quotes. For example, if you want to search the To field of emails for the phrase, **Carton, Sydney (TTC-San Antonio)**, you need to write the search query as **To Contains “Carton, Sydney (TTC-San Antonio).”** This will allow you to get the expected search results and those search results will be highlighted in the *Text* view. However, the search results will not be highlighted in the *INSO views*.

Only alphanumeric characters are recognized in search terms. Also, certain non-alphanumeric characters are recognized by the search, such as @ and \$. To search for text with non-alphanumeric characters, include the whole string in quotes. For example, if you searched for **mckay@accessdata**, you would find **mckay@accessdata**. But if you searched for **mckay#accessdata**, it would not return results.

Noise Words

Noise words, such as **if**, or **the** are ignored in searches. For example, if you were to search on the term **MD&A**, the search would treat the **&** as an AND operator and return documents with both the terms “MD” and “A” in them. However, because **A** is a noise word, the search only highlights “MD” in the document.

When a term contains a noise word with another term, the search results will return results with the noise word, as well as other words that are in the same place as the noise word. For example, by searching for the term **MD** and **A**, not only are results returned that locate the terms “MD” and “A,” but also “MD” and “<any word that is adjacent to ‘MD’>.” For example, by searching for the term **MD** and **A**, you might also get the result of “MD” and “Surgeon.”

However, if you were to search on **MD&Surgeon**, you will not get “MD” and “A” or any other variation. The results are only “MD” and “Surgeon.”

Words that are used as logical operators, such as **and** or **or** will be treated as operators and not as part of the search term. If you want to include words such as **and** or **or** as part of the search term, you need to enclose the entire search term in double quotes. For example, enclosing in double quotes the search term “**this or that**” will return only those occurrences where all three search words appear together, and not all of the terms where **this** appears separately from **that**.

The following words are ignored in searches:

a, about, after, all, also, an, and, any, are, as, at, be, been, but, by, can, come, could, did, do, even, for, from, get, got, he, her, him, his, how, i, if, in, into, it, its, just, like, me, my, not, now, of, on, only, or, other, our, out, over, see, she, some, take, than, that, the, their, them, then, there, these, they, this, those, to, too, under, up, very, was, way, we, well, were, what, when, where, which, while, who, will, with, would, you, your

Also, there are exceptions for certain characters:

- The characters **0-9**, **a-z**, **A-Z**, **@**, and the **_** (underscore) are searchable.
- Other characters, such as **-**, **+**, and **;** are not searchable. With a few exceptions, they are treated as spaces.
- The characters **?** and ***** are wildcards. See [Using ? and * Wildcards](#) on page 18.
- The **%**, **~**, **#**, **&**, **:**, **=** characters are used in advanced variations of the search, such as synonym or fuzzy searches. See [Understanding Advanced Variations](#) on page 33.

Note: The & symbol is interpreted as an AND operator. If you searched for Steinway & Sons, it would search for Steinway AND Sons. To use the & symbol in a search, include it in quotes. For example, "Steinway & Sons".

Using Boolean Logic Options

The following table describes the boolean options that you can use in searches. Some boolean options are combined in the table to serve as examples of what is possible.

Boolean Logic Options

Option	Description
AND	Returns as search results those evidence files that contain all of the search words that you specified. For example: marijuana AND cocaine Matches all evidence files that contain both the words "marijuana" and "cocaine." However, if you search for the example: marijuana + cocaine You will only get search results highlighted if "marijuana" and "cocaine" are adjacent.
OR	Returns as search results those evidence files that contain any of the search words that you specified or at least one of the search words that you specified. For example: marijuana OR cocaine Matches all evidence files that contain either the word "marijuana" or "cocaine."
NOT	Returns as search results those evidence files that do not contain the search words that you specified. This expression is an efficient way to eliminate potential privileged data from production sets. Used the expression at the beginning of your search word or phrase. For example: NOT licensed Matches all evidence files except those with the word "licensed" in them. Note: Do not use implied boolean search with this operator (Example: -license). It will return incorrect results.
W/N	Returns as search results those evidence files that include the specified word or phrase that is found within so many number of words (for example, W/2) of another. For example: (rock AND stump) W/2 (fence AND gate) Matches all evidence files that contain both the words "rock" and "stump" that occur within two words of both the words "fence" and "gate." or (pear w/10 peach) W/7 (apple OR plum) Matches all evidence files that contain the word "pear" that occurs within ten words of the word "peach" and that also occurs within seven words of either "apple" or "plum." You can also use this option to search for evidence files with known words in certain locations or instant messaging chats. Note: For eDocs, all occurrences of the words on either side of the W/N operator are highlighted. For Cool HTML email files, there is no highlighting on the <i>Natural</i> and <i>Text</i> views.

Boolean Logic Options (Continued)

Option	Description
AND NOT	Returns as search results those evidence files that contain the expression on the left when the expression on the right is not found. For example: peach AND NOT pineapple Matches all evidence files that contain the word “peach,” but do not also contain the word “pineapple.”
OR NOT	Returns as search results those evidence files that contain either the left expression or specifically not containing the right expression. For example: peach OR NOT pineapple Matches all evidence files that contain the word “peach,” and any other file that does not contain the word “pineapple.” Note: The search phrase before the OR operator is highlighted.

Using ? and * Wildcards

A search word can contain the wildcard characters * and ?. A ? in a word matches any single alphanumeric character, and a * matches any number of alphanumeric characters. The wildcard characters can be in any position in a word.

Wildcard	Description
?	Matches any single alphanumeric character. The following are examples: <ul style="list-style-type: none">• appl? matches <i>apply</i> or <i>apple</i>, but not <i>apples</i>• a?l matches <i>all</i> or <i>aol</i>
*	Matches any number of characters within a single word. The following are examples: <ul style="list-style-type: none">• appl* matches <i>apply</i>, <i>apple</i>, <i>apples</i>, <i>application</i>• ap*ed matches <i>applied</i>, <i>approved</i>• appl*ion matches <i>application</i>• a*l matches <i>all</i>, <i>aol</i>, <i>april</i>, <i>actual</i>, <i>additional</i>• *cipl* matches <i>principle</i>, <i>participle</i> Note: Use of the * wildcard character near the beginning of a word will slow searches somewhat.

You can use wildcards with search phrases that use operators.

For example, 20* OR pat* OR appl* would match any document that had *2010*, *2011*, *patent*, *patents*, *application*, or *applications*.

You can use wildcards within terms that are within text strings.

For example, “20* p*t a*n” would match *2010 patent application*.

? and * Wildcard Limitations and Tips

- The ? and * wildcards can be used for alphanumeric characters only.
For example, a search of PSE?G or PSE*G will not find *PSE&G*.

- The ? and * wildcards only work within single words not separated by spaces, periods, commas, and so on.
For example, a search of “n*w” will find “New” but a search of “n*k” will not find “New York” or New.York”.

Searching Numbers

When searching for numbers, be aware the commas, dashes, and spaces are word separators. A word separator will find docs where terms are separated by that separator or space.

For example:

- A search of 123,?56 will find
 - 123,456, 123,556, 123,656, etc.
 - 123-456
 - 123 456
- A search of 123-456 will also find 123,456
- A search of *123, 456* will find
 - xxx123
 - 456xxx

To find numbers containing a comma, dash, or space, use a string in parentheses.

Searching for Virtual Columns

You can search for virtual columns in the quick search field. Virtual columns are fields of data that are included in the records, but there is not a physical column in the database that correlates with that data. Searching for virtual columns will result in records that contain the virtual data, but the column will not actually appear in the *Item List* panel.

Running a Subset Search

After running a quick search, you can run another search that is a subset of your search. Subset searches appear in your recent searches. Subset searches connect your first search with your second search using an AND connector. Subset searches will appear in the recent searches of the *Searches* tab of the *Project Explorer*.

To run a subset search

1. Run a quick search.
See [Running a Quick Search](#) on page 13.
2. Enter new search criteria in the quick search field in the *Item List* panel.

Subset Search Button



3. Click the **Subset Search** button.
Your search results appear in the *Item List* panel.

Returning to a Previous Search

After you run a subset search, you can return to a previous search using the subset drop-down.

To return to a previous search

- ❖ After you run a quick search and a subset search, expand the **Subset Search** drop-down and select **Previous Search**.

Searching in the Natural Panel

In the Natural panel, you can search by keyword in the *Search* tab for the selected document.

To search in the Natural panel

1. In *Project Review*, ensure the *Natural* and *Item List* panel are showing.
2. Select a document in the *Item List* that has a native application.
3. In the *Natural* panel, click the **Search** tab.
4. In the *Search* field, enter a keyword for which you want to search.
5. The first instance of the word is highlighted in the INSO view.
6. Click the next and previous buttons to see the other instances of the keyword.

Note: You will not be able to search for numerals in spreadsheets.

Using Global Replace

In the *Item List*, you can use Global Replace to globally search the documents and replace a keyword or phrase. Only one Global Replace job can be submitted at a time per project. Once the job is submitted, you will have thirty minutes to either manually commit the job or allow it to commit automatically. After a Global Replace job has been committed, you can choose to create a new Global Replace job for that project.

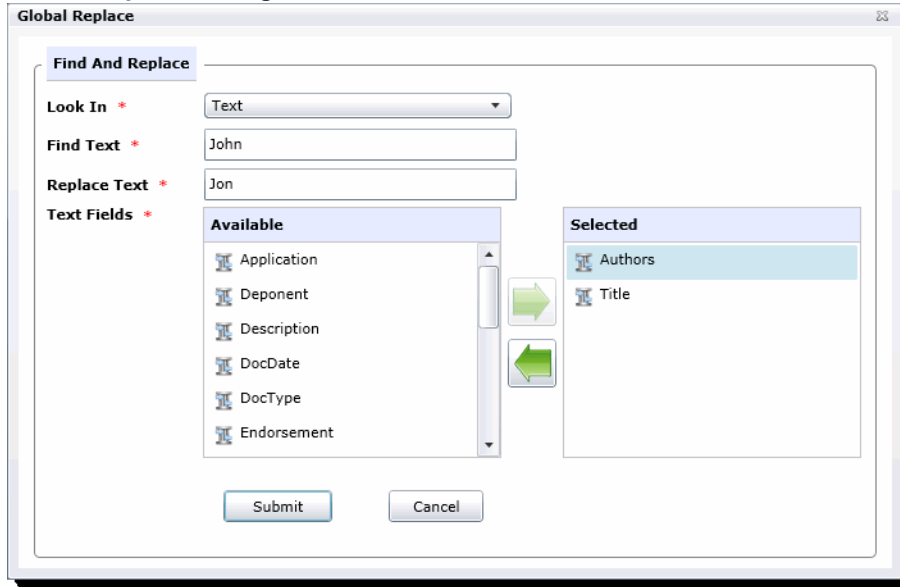
Note: If Global Replace jobs are submitted by two different users on the same project at the same time, both Global Replace jobs will fail. However, if two different users submit Global Replace jobs on two separate projects at the same time, both Global Replace jobs should complete successfully.

See [Committing a Global Replace Job](#) on page 22.

To use Global Replace

1. In *Project Review*, either select a document in the *Item List* or select **All** from the actions.
2. Select **Global Replace** from the pull-down menu. The **Global Replace** dialog appears.

Global Replace Dialog





3. Choose which field that Global Replace will search and replace:
 - Text
 - Number
 - Date Time - You cannot search for a specific data and replace it with a fuzzy date.
4. Add text fields that you want to change to the selected box. The options available will change depending on what is chosen in the **Look In** field.
5. Click **Submit**.

Once you have completed the Global Replace action, return to the *Work List* on the *Home* page. If there were any Document IDs that failed to code, they will be listed by their number under the *Work List*. You can then resubmit Global Replace for those failed IDs.

Committing a Global Replace Job

You must manually commit a Global Replace job if you want to run another Global Replace job on the same project before thirty minutes has elapsed. You can also undo a Global Replace job within that thirty minute window.

To manually commit a Global Replace job

1. In the *Work List* on the *Home* page, select the Global Replace job.
2. Click **Commit** .
3. A Commit job will appear in the *Work List*.
4. (optional) Click **Undo**  to cancel a Global Replace job. You cannot cancel a Global Replace job once thirty minutes has elapsed from the job's creation.

Using Dates and Times in Search

Using Dates and Times in Searches

You can perform searches based on dates and times. For example, you can perform searches based on the date a file was created or when an email was sent or received. The following are examples of date or time searches:

- 2/2/2008 - this will find any item with text or a database date of 2/2/2008
- anydate = 2/5/2011 - this will find any item with an event occurring on 2/5/2011
- anytext = 2/5/2011 - this will find any item with a date of 2/5/2011 in the text
- receiveddate = 12/18/2011 - this will find emails that were received on 12/18/2011
- receiveddate between 12/17/2011 and 12/19/2011 - this will find emails that were received between those dates
- receiveddate > 12/17/2011 - this will find emails that were received after 12/17/2011
- receiveddate < = 12/17/2011 - this will find emails that were received on or before 12/17/2011

How Time Zone Settings Affect Searches

By default, date and times from meta data that you see in Review are in UTC format. These dates and times are converted to UTC when data is entered in a project. As a result, by default, email dates and times, and file stamp date and times are displayed in the UTC time zone.


However, an administrator can configure a Display Time Zone for a project. If this was done, then all dates and times are offset to be shown in the specified time zone. For example, suppose an email was sent on 1/1/ 2010 at 1:15 am based on UTC time. If the project was set to display the Pacific Time Zone, the email sent data would have an -8:00 offset. As a result, it would have a sent date and time of 5:15 pm on December 31, 2009.

The offset does not apply to dates or times that are in the text body of a document, only dates in the meta data. For example, file creation dates, email sent dates. As another example, if an email is a reply, the date and time of the original email is in the email but simply as text, not meta data.

If you perform a search based on a meta data date or time, be aware the Display Time Zone will be used, not the UTC date and time.

Viewing the Display Time Zone

To the Display Time Zone settings for a project

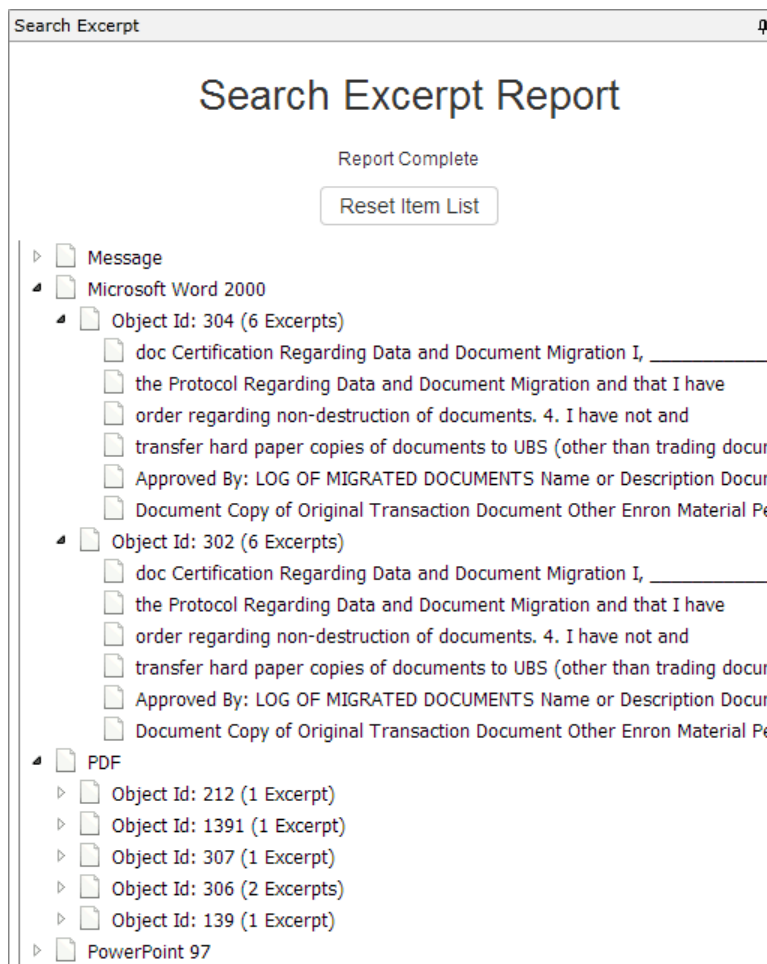
1. On the *Home* page in *Review*, select the case.
2. On the  (*Info*) page, view the *Display Time Zone* value.
The time zone and the offset from UTC is displayed.

Using the Search Excerpt View

After performing a search, you can generate a Search Excerpt view. You generate and see this view in the *Search Excerpt* panel. This panel is now included by default in the *Search* layout.

You can generate the Search Excerpt view after you have completed a search. When you generate the Search Excerpt view, a DTSearch job is run in the background on the text of the documents.

The Search Excerpt view contains a list of all of the items, by Object ID, that have search hits. The items are clustered by document type, such as email Message, Microsoft Word, PowerPoint, PDF, and so on. Under each ObjectID item, there is a list of excerpts of the text that contains the search hits.




You can click either the item or the excerpt and the document is shown in the Natural Viewer and the search results and the excerpts are highlighted.

The Search Excerpt uses dtSearch to search for text strings. dtSearch will find exact terms unless you use wildcards. For example, if your initial search is for the word *document*, other forms of the word, like *documents* or *documented* will be highlighted as a partial hit, but will not be shown as excerpts --it will not show excerpts of text containing *documents* or *documented*. However, if your search includes a wildcard, like *document**, then it will display excerpts for all forms of the word.

Also, the dtSearch will not return excerpts for search results that do not contain text strings. For example, you can search on a database property such as ObjectID > 50. Because there are no text hits, no excerpt can be generated.

You can also save and download a Search Excerpt report.

To access the Search Excerpt panel

1. Open a project in *Review*.
2. Click the  *Layouts* drop-down.
3. Click **Panels**.
4. Make sure that the **Search Excerpt** panel is checked.
5. If it is already checked, click the **Search Excerpt** panel in *Review*.

To generate the Search Excerpt view

1. Run a report and let it complete.
2. In the *Search Excerpt* panel, click **Create Search Excerpt Report**.
A DTSearch job is run in the background to generate the list.
The resulting view lists all items that contain the search results.
The items are clustered by document type, such as email Message, Microsoft Word, PowerPoint, PDF, and so on.
3. Expand a document category.
All of the items are listed by their ObjectID.
It also shows how many excerpts within that item have the search results.
4. Expand an item.
One or more excerpts are displayed.
5. You can do one of the following.
In either case, the *Item List* only displays that one item and the document is shown in the *Viewer*.
 - Click an ObjectID item.
If you click an item, the document is opened in the *Viewer* and the search results are highlighted in the document.
 - Click an excerpt.
If you click an excerpt, and if the document has been converted to SWF, the document is displayed in the *Stand Viewer*, and the whole excerpt is highlighted along with the search results. If the document has not been converted to SWF, the document is displayed in the *Alternate File Viewer* and only the search results are highlighted.
See [Using the Standard Viewer and the Alternate File Viewer](#) on page 73.
6. To restore the *Item List* to include all of the documents from the search, click **Return Item List to Search Results**.
7. To save and download a report, click **Save**.

Using Search Reports

About Search Reports

You can generate, download, and view search reports. The search reports provide a history of a search and information about the results.

The reports are saved in XLSX format. The report has the following XLSX sheets:

Search Report Sheets

Sheet	Description
<i>Details</i>	Includes the following: <ul style="list-style-type: none">• The date and time of the search• Who performed the search• Which phrase was searched for• Which search options were used• Information about the files that were in the search results
<i>Filters</i>	Which facets were included and excluded and which Quick Filters were applied.
<i>Documents Group</i>	Any related Document Groups
<i>Hits by Type</i>	Details which file types hits were found in
<i>Keywords</i>	Details hit counts for each keyword used
<i>Files</i>	Details of the files for the search hits

Generating and Downloading a Search Report

After you have generated a search report you can download it in one of two ways:

- In *Review*, from the *Search Options*.
- On the *Home* page, on the *Reports* tab, under *Search Reports*.

To generate and download a search report

1. In *Review*, after performing a search, click **Search Options**.
2. Click **Search Report Options > Generate Search Report**.
After several seconds, the report is generated.
To download the report, click **Download Search Report**.
3. Select to **Open** or **Save** the report.
By default, the report is saved in the browser's *Downloads* folder as **Search History Report - n**.
You can use **Save As** to specify a filename and path.

About the Search Report Details

The following table describes some of the information provided in the report details.

Search Report Details

Field	Description
Total Files	Includes all emails and eDocs that match the search criteria.
Unique Family Items	This count is the number of files where any single family member had a keyword hit. If any one file within a document family had a keyword hit, the individual files that make up this family are counted and added to this total. For example, one email had 3 attachments and the email hit on a keyword, a count of 4 files would be added to this count as a result.
Unique Family Emails	This count is the number of emails that have attachments where either the email itself or any of the attachments had a search hit. This count is for top level emails only. Emails as attachments are counted as attachments.
Unique Emails with no Attachments	This count is the number of the emails that have no attachments where a search hit was found.
Unique Loose eDocs	This count is the number of loose edocuments where a search hit was found. This does not include attachments to emails, but does count the individual documents where a hit was found from within a zip file.
Total Hit Count	This count is the total number of hits that were found within all of the documents.
Max Relevancy	This is the maximum relevancy score achieved with the search criteria. *
Min Relevancy	This is the minimum relevancy score achieved with the search criteria. *
	Note: * Max and Min relevancy scores are calculated based on the total number of hits in the document as a percentage of the maximum number of hits found in a during the search when performing an index search. For example, if one document contains 50 hits but another document in the results has 100 hits (and that's the max) then the first document will be scored as 50% relevant and the second document will be scored as 100% relevant. These relevancy scores are only relative within a single search set. They may vary when the search set is increased or decreased. Additionally, some searches are run against the database instead of the index and these searches will always get a 100% relevancy score. A database search would be one that requests information within a specific field or non-indexed field such as "ObjectID = xxx".

Chapter 3

Running Advanced Searches

Running an Advanced Search

If using a simple search does not return the results you expected, you can use advanced searching techniques to pinpoint relevant data and privileged information.

AccessData software uses the utility dtSearch to index project data. In Advanced Searching, you can query the index using a specialized query language. In addition to extended searching capabilities, the index allows searches to be returned in seconds instead of the minutes or hours that are required for a standard linear search.


Note: In order for a document to be indexed for search, it must contain at least six characters in the file. Documents with less than six characters will not be indexed. However the metadata in those documents will be indexed normally.

Note: When searching using the *DocDate* or *NoteDate* fields, you must search using a YYYYMMDD format regardless of how your date fields are formatted for display.

For more information on using dtSearch syntax, you can view technical papers on the AccessData web site:

<http://www.accessdata.com/technical>

To run an advanced search

1. Log in as a user with Run Search privileges.
2. Click the *Project Review* button  in the *Project List* panel next to the project.
3. In *Project Review*, ensure that the *Project Explorer*, the *Item List*, and *Natural* panel are showing.
4. In the *Project Explorer*, default scope selection includes all evidence items in the project. Using the check boxes, uncheck items to exclude them from the scope of the search. These scope items include:
 - Document Groups
 - Production Sets
 - Transcripts
 - Notes
 - Exhibits
 - Labels
 - Issues
 - Categories

5. In the *Facets* tab of the *Project Explorer*, you can select any combination of Facets to apply to the current search scope.
6. Click the **Apply** check mark button in the top of the *Project Explorer*. This applies the currently selected scope and any selected Facets to the *Item List*, allowing search and review on the resulting subset. The scope of a search is saved along with the query. This Facet will persist through searches until you clear it. Scopes may be changed and searches re-run by use of the *Apply* button. After updating a Facet or scope item, you may click the **Apply** button to update the scope and re-run any search that has not been cleared out by use of the **Clear Search** button in the *Search Options* menu.
7. Click the **Search Options** button in the *Item List* panel and select **Advanced Search**.

Advanced Search Dialog

The screenshot shows the 'Advanced Search Builder' dialog box. It features a title bar with the text 'Advanced Search Builder' and a close button. Below the title bar, there are four main sections, each with a collapse/expand arrow on the left:

- Information:** Contains a 'Search Name' text field, a 'Variations' dropdown menu (currently set to 'None'), a large text area for entering search criteria, and two buttons: 'Expand All' and 'Import Terms'.
- Conditions:** Currently collapsed.
- Columns:** Currently collapsed.
- Result Sorting:** Currently collapsed.

At the bottom of the dialog, there are four buttons: 'Save', 'Search', 'Clear', and 'Cancel'.

8. In the Information section, do the following:
 - 8a. Enter a Name for the search if you want to save the search. Otherwise, the search will appear in the Recent Searches list and will not be able to be saved.
 - 8b. (Optional) Select the type of Variation you want to include in your search.
See [Understanding Advanced Variations](#) on page 33.
 - 8c. In the text field, enter the free form text you want to include in the search. Freeform searching lets you combine keyword, boolean, and regular expression criteria to perform a search on evidence files.
See [Using the Term Browser to Create Search Strings](#) on page 34.
 - 8d. To add related terms for the words you entered, click **Expand All**.
See [Using the Term Browser to Create Search Strings](#) on page 34.
 - 8e. To import a list of terms from a TXT file, click **Import Terms**.
See [Importing Index Search Terms](#) on page 35.
9. Expand the **Conditions** section to search within the fields/columns of the documents.

Conditions

(Field	Operator	Value)	Connector
(To	Equal	Kate Symes)	And
(Subject	Contains	Re: 3/13 Checkout)	Or
(Subject	Contains	Re: Constellation C)	And
(CreationDate	Between	12/7/2011 AND 12/12/2011)	And

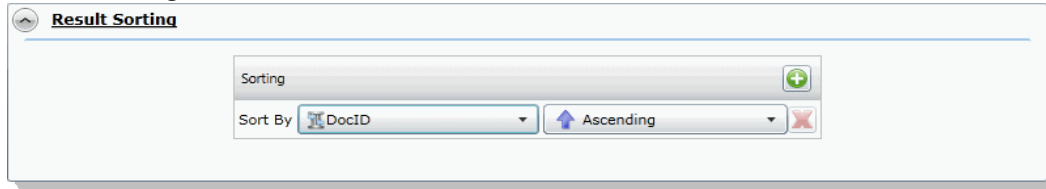
10. In the *Conditions* section, do the following:
 - 10a. Select a field that you want to search within.
See the Project Manager Guide for more information on creating custom fields.
 - 10b. Select an Operator from the drop-down.
See [Using Search Operators](#) on page 15.
See [Using Boolean Logic Options](#) on page 17.
 - 10c. Select or enter a value using the following:
 - Field: Enter text or symbols.
 - Date: Enter a date or click the calendar to select a date.
 - Look up button: Click the blank button to look up available search criteria for the selected field.
 - 10d. Select either “And” or “Or” as the connector.
See [Using Boolean Logic Options](#) on page 17.
 - 10e. Click **Add Row** to add additional conditions.
 - 10f. Set parenthetical criteria. Then, click **Validate Grouping** to validate your parenthesis.
11. Expand the **Columns** section to add visible columns to your search results.

Columns

Available	Selected
AttachDocIDs	Authors
AttachmentCount	Category1
BCC	
BegDocID	
Category Radio Field	
CategoryCheckBoxField	

- 11a. Click the right arrow to add columns and the left arrow to remove columns.
- 11b. Click the up and down arrows to adjust the order of the columns.
12. Expand **Result Sorting** to select the column by which you want the search results to be sorted. The column does not need to be visible to sort by it.

Result Sorting



- 12a. In the *Sort By* drop-down, select the field you want to sort by.
- 12b. In the second drop-down, select whether you want to sort by Ascending or Descending.
13. Click **Search**.

Advanced Search Operators

The following search operators are available in the advanced search:

Advanced Search Operators

Operator	Description
Equal	Searches for the exact value entered.
Not Equal	Searches for everything in the selected field except the exact value entered.
Exists	Searches for the existence of data within the selected field.
Fails	Searches for all documents that do not contain data within the selected field.
GreaterThan	Searches for a number greater than the value entered.
GreaterThanEqualTo	Searches for a number greater than or equal to the value entered.
LessThan	Searches for a number less than the value entered.
LessThanEqualTo	Searches for a number less than or equal to the value entered.
Contains	Searches for the value entered within a string. The value should be a full word. If you want to search for a partial word, you need to include the * operator.
NotContains	Searches for everything except the value entered. The value should be a full word. If you want to exclude a partial word, you need to include the * operator.
Between	Searches between a range of dates or numbers.
NotBetween	Searches for all dates or numbers except the range selected.

The search operators available depend upon the field selected to search. Not all search operators are available for all fields.

Advanced Search Operators Exceptions

The ProductionSetID column contains values for exported files from both Export Sets and Production Sets and is used for associating exported files with the original file. This column is populated with queries from multiple

tables and does not operate like other standard metadata columns. Search operators will return different results than expected with other columns. You can expect the following results when searching the ProductionSetID column:

Search Operators Exceptions for ProductionSetIDs

Operator	Results
Exists	Search results return only the produced document.
Fails	Search results return source documents and not the produced copy.
Contains	Search results return only the produced document.
Not Contains	Search results return source documents and not the produced copy.

Understanding Advanced Variations

The following table describes the Variation options in the Information section of the *Advanced Search* dialog.

Variation Options in the Advanced Search Dialog

Search Variations	Description
None	No search variations are applied.
Stemming	Finds grammatical variations on word endings. For example, stemming reduces the words “fishing,” “fished,” “fishy,” and “fisher” to the root word “fish.”
Phonic	Finds words that sound like the word that you are searching and begins with the same first letter. For example, searching for “whale” using phonic, would also find wale and wail.
Synonyms	Finds word synonyms. For example, searching on “fast” would also find “quick” and “rapid.” You can enable this option for all words in a request. You can also add the “&” character after certain words in your request.
Related	Finds all words in the search criteria and any related words from the known related categories.
Fuzzy	<p>Finds words that have similar spellings, such as “raise” and “raize.” You can enable this option for all words in a request.</p> <p>The level of fuzziness that you can set is 1-10. The higher the level of fuzziness, the more differences are allowed when matching words, and the closer these differences can be to the start of the word. Setting too many letter differences may make the search less useful.</p> <p>Dragging the slider bar to the right increases the number of letters in a word that can be different from the original search term.</p> <p>Dragging the slider bar to the left decreases the number of letters in a word that can be different from the original search term.</p> <p>You can also add fuzziness directly in the search term you enter using the “%” character. The number of % characters that you add determines the number of differences that are ignored when you search for a word. The position of the % characters determines how many letters at the start of the word have to match exactly.</p> <p>For example, “ca%nada” must begin with “ca” and have just one letter difference between it and “canada.” Whereas, “c%%anada” must begin with “c” and have only two letter differences between it and “canada.” In another example, marijuana can be spelled “marihuana” or “maryjuana.” In this project, your search expression could be “mar%%uana.”</p> <p>As with the fuzzy slider bar setting, you should exercise care when you use multiple % symbols because the number of junk hits rises quickly with each added error.</p>

Using the Term Browser to Create Search Strings

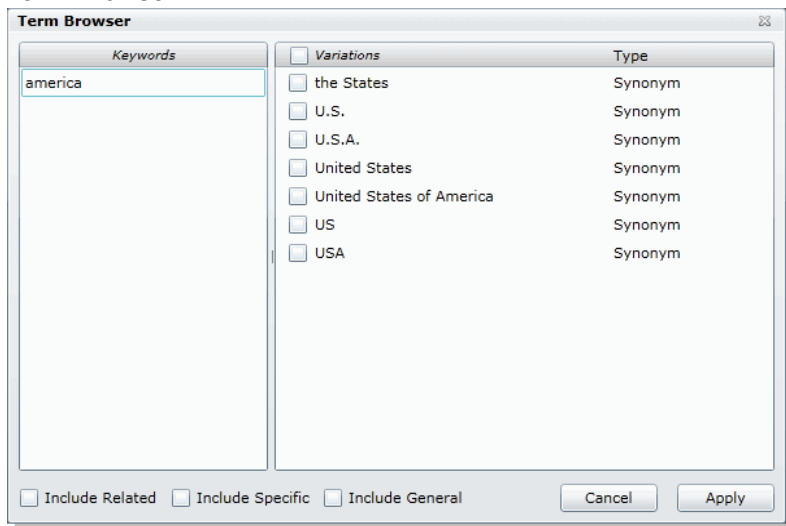
You can create a search using terms that are related to any keyword. You can use the Term Browser to generate a list of similar words. You then select which words you want to include in the search.

For example, you may start with a keyword of “delete.” By using the Term Browser, it will suggest synonyms, such as “erase” and “cut.” It will also suggest related terms, such as “cut,” “deletions,” “excise,” and “expunge.” It will also suggest general related terms, such as “censor,” “remove,” “take,” and “withdraw.” You can select which of those words to include in your search.

To search for terms using related words

1. In *Project Review*, in the Item List panel, click **Search Options > Advanced Search**.
2. Enter a keyword.
3. Click **Expand All**.

Term Browser



4. In the *Term Browser*, highlight the keyword.
A list of synonyms is generated.
5. To add other related words, select the **Include Related**, **Include Specific**, and **Include General** check boxes.
6. Select the words that you want to include in the search or click **Variations** to select all words.
7. To build a search including the words that you selected, click **Apply**.
8. You can edit the search or run it by clicking **Search**.

Importing Index Search Terms

You can import a list of search terms. This lets you reuse a list of search terms that you saved from previous searches, or that you saved for documentation purposes.

To import a saved search terms file

1. In *Project Review*, in the *Item List* panel, click **Search Options > Advanced Search**.
2. Click **Import** to import a set of search terms.
3. Select the text file that you previously saved.
4. Click **Open**.

Chapter 4

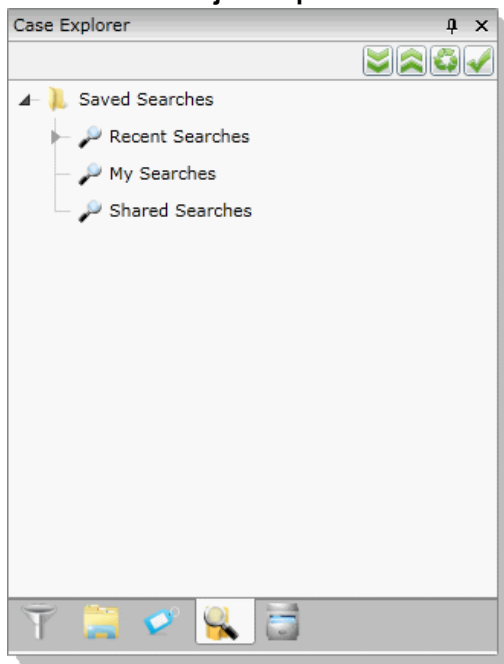
Re-running Searches

You can re-run searches by using the *Search* tab in the *Project Explorer* panel in the *Project Review*.

The Search Tab

The *Search* tab in the *Project Explorer* can be used to view recent searches, your searches, and shared searches.

Search tab in Project Explorer



Elements of the Search Tab

Element	Description
Saved Searches	Contains the Recent Searches, My Searches, and Shared Searches.


Elements of the Search Tab (Continued)

Element	Description
Recent Searches	Every time a search is performed, it is saved in the recent searches. The last 10 searches are saved here in chronological order. Users can execute and edit searches from Recent Searches.
My Searches	Displays all the searches that the user has saved. Users can execute, delete and edit searches from My Searches. Users can also share their searches.
Shared Searches	Displays all the shared searches that the user has permissions to access. Users can execute searches from Shared Searches.

Running Recent Searches

When you execute a search, the search conditions are saved. You can view and reuse recent searches. The last ten searches are saved in the Recent Searches. To run recent searches, you must have the Run Searches permission.

To run a recent search

1. Log in as a user with Run Searches permissions.
2. Click the *Project Review* button  in the *Project List* panel next to the project.
3. In *Project Review*, ensure the *Project Explorer* is showing.
4. Click on the **Searches** tab.
5. Expand the *Recent Searches*.
6. Right-click the search and select **Run Search**.
The search is run using the original search scope and the original search criteria. The search results appear in the *Item List* panel.

Clearing Search Results

After you have performed a search, the items in the *Item List* are the result of the list. You can clear the search result to view the documents in the Grid before you performed the search.


To clear search results

1. In *Project Review*, ensure the *Item List* panel is showing.
2. Click **Search Options > Clear Search**.

Saving a Search

You can save any advanced search that you design in the Advanced Search Builder. All saved searches are stored in the *Searches* tab of the *Project Explorer*. You can use saved searches to run past searches again or to share your search with a group of users.


To save a search

1. Log in as a user with Run Search privileges.
2. Click the *Project Review* button  in the *Project List* panel next to the project.
3. In *Project Review*, ensure that the *Project Explorer*, and the *Item List* panel are showing.
4. In the *Project Explorer*, the default scope selection includes all evidence items in the project. Using the check boxes, uncheck items to exclude them from the scope of the search. These scope items include:
 - Document Groups
 - Production Sets
 - Transcripts
 - Notes
 - Exhibits
 - Labels
 - Issues
 - Categories
5. In the *Facets* tab of the *Project Explorer*, you can select any combination of Facets to apply to the current search scope.
6. Click the **Apply** check mark button in the top of the *Project Explorer*. This applies the currently selected scope and any selected Facets to the *Item List*, allowing search and review on the resulting subset. The scope of a search is saved along with the query. This Facet will persist through searches until you clear it. Scopes may be changed and searches re-run by use of the *Apply* button. After updating a Facet or scope item, you may click the **Apply** button to update the scope and re-run any search that has not been cleared out by use of the **Clear Search** button in the *Search Options* menu.
7. Click the **Search Options** button in the *Item List* panel and select **Advanced Search**.
8. Enter a *Name* for the search.
9. Enter criteria for the search.
See [Running Recent Searches](#) on page 37.
10. Click **Save**.

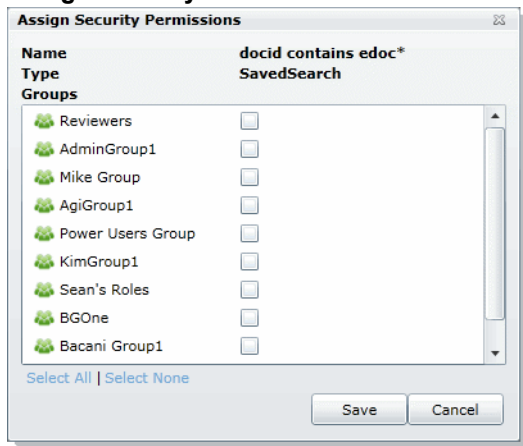
Sharing a Search

You can share your saved searches with other groups of users. To share a search, you need to have the Manage Searches permission.

To share a search

1. Log in as a user with Manage Searches permissions.
2. Click the *Project Review* button  in the *Project List* panel next to the project.
3. In *Project Review*, ensure the *Project Explorer* is showing.
4. Click on the **Searches** tab.
5. Expand *My Searches*.
6. Right-click the search and select **Manage Permissions**.

Assign Security Permissions



7. Check the groups with which you want to share the search.
8. Click **Save**.

Chapter 5

Using Filters to Cull Data

Filtering Data in Case Review

In *Project Review*, you can filter evidence to help view only relevant evidence for the project. After filtering data, the results are then displayed in the *Item List*. You can also use searches and column sorting to help you further review and cull down evidence.

About Filtering Data with Facets

You can filter data using facets. Facets are properties of a document that you can include or exclude. The following are a few example of facets:

- Object type and object sub-type (File > Email, File > Spreadsheet, Disk Image, Partition)
- File extension type (EXE, DLL, TXT, GIF, DOC, XLS)
- File category (Documents, Email, Graphics, Audio Multimedia, Video Multimedia)
- File Size (Small, Medium, Large)
- Email Senders Address
- Email Recipients Address
- Email by Date

See [Available Facet Categories](#) on page 45.

That facets that are available to use are based on your evidence. For example, if there are no XLSX documents in your evidence, the XLSX facet is not displayed.

By default, when you first open a project in *Project Review*, all facets are applied, and as a result, all evidence is listed in the *Item List*. You can use the facets to include or exclude evidence from the *Item List*. You can choose one or more facets within a single category or you can choose facets across multiple categories.

For example, you can filter evidence to only display emails sent by one person to another person with a certain date range. As another example, you can filter evidence to display only DOC or DOCX files that have a specific label applied.

Applied facets are persistent across searches and have to be cleared by you manually.

Note: When you cull data with facets, this filtering will override and clear other filters applied to the *Item List*, including Search and Column Filters.

About Dynamic Facets

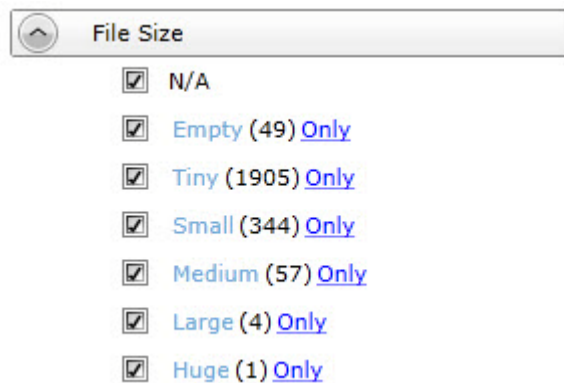
Most facets are now dynamic. When you select and apply a facet, all other facet categories will reflect the results of the previously selected facet. Other categories will only show facets that have data based on the applied facet.

For example, suppose that before applying any facets, that under *File Extensions*, there are 25 DOCX files of various file sizes. And then suppose you apply a facet to include only *Large* files. When you look at the *File Extensions* filter again, you will only see the number of DOCX files that have a *Large* file size.

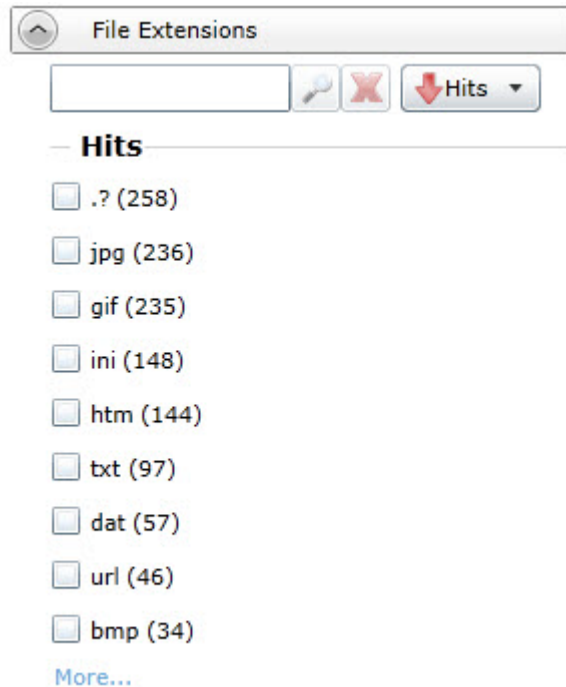
However, applying column filters, column filters, or searches does not affect facet counts.

About Sortable and Searchable Facets

Some facet categories include a pre-configured set of facets. For example, under the *File > File Size* facet category, there will be a maximum of five facets: Tiny, Small, Medium, Large, and Huge.



Some facet categories include a dynamic set of facets based on the files in the evidence. For example under the *File > File Extensions* facet category, facets are shown for all of the file extensions that exist in the evidence.



These facet categories can potentially have a very large number of facets. A project could easily include dozens of different file extensions.

Facet categories that have a large number of facets have additional features that help you use them:

- By default only nine facets are shown but you can select to see more.
- Facets are sortable.
By default, the facets are sorted by the facets with the most hits. When you open a category, by default the nine facets with the most hits are shown. You can use the following sort orders:
 - Ascending by name
 - Descending by name
 - Ascending by the number of hits
 - Descending by the number of hits
- You can search for specific values within the facets.
For example, if there are 100 email senders names, you can search for a certain name. You can clear the search by clicking the red **X**.

About Excluding Tags Filters From a Facet Search

You can exclude *Tags* filters (categories, issues, labels, and summaries) from a facet search. The default for the *Tags* facets are checked, or included. Clicking the check box once actively excludes the facet in filters group. Clicking the check box a second time clears the check box and the facet is not included in the facet search.

When excluded, a red **x** appears in the facet check box, indicating that the facet is excluded. The hyperlink to apply the excluded facet is disabled. You need to be aware of the following considerations when excluding *Tags* facets:

- For labels, the exclude feature applies to all labels in a group. However, if there are children under the labels, and one child label is selected for exclusion while another is not, the label group appears blank. This is because you cannot include a whole label group when one of the child labels is excluded.
- For issues, you can exclude or include an individual issue. Additionally, you can exclude a child issue while including a parent issue or vice versa.
- If you have a document that has been assigned a tagged item that is included in a facet in the *Tags* filter and has also been assigned a tagged item that is excluded in a facet in the *Tags* filter, the facet does not display the document. For example, a document may be tagged with both Tag 1 and Tag 2. If all documents with Tag 1 are included in the facet and all documents with Tag 2 are excluded in the facet, the document with both Tag 1 and Tag 2 is not posted to the Item List. The exclusion takes precedence. This is because exclusions and inclusions in facets act as an AND property, not as an OR property.

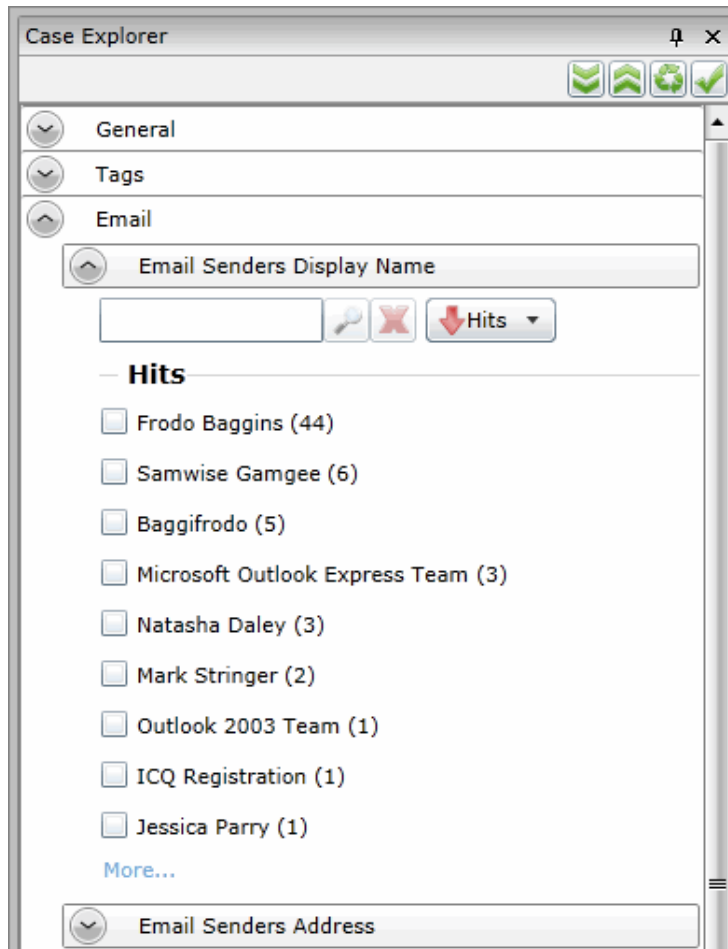
The Facets Tab

The *Facets* tab in the *Project Explorer* in *Project Review* lists the available facets to apply to documents. You can filter evidence to help view only relevant evidence for the Project. After you have applied facets, the results are then displayed in the *Item List*. You can also use searches along with column sorting and filtering to help you further review and cull down evidence.

The *Facets* tab in the *Project Explorer* allows you to filter before (and maintain after) conducting any searches. This allows targeting specific areas of data for search and review with persistent facets. You may maintain the applied facets as long as desired.

You can use one or more facets within a single filter or one or more facets across several categories to cull down the evidence. By default, when you first open a project in *Project Review*, all filter facets are applied, and as a result, all evidence is listed in the *Item List*. You use the facets to exclude evidence from the *Item List*.

Facets Panel



Only the top nine facets of a filter display when you expand a category. To see all the facets in a category, click **More...** to display a facet dialog. Many categories also contains a search field that searches for facet hits within that particular category.

The facets that appear in the Facets tab depends upon the product license that you have.

Available Facet Categories

The following table lists facets that may be available in the *Facets* tab of the Project Explorer.

Note: The Evidence Explorer and Custodian Facet counts are reduced when Family data uploaded by Evidence Processing is updated by a CSV import. Existing documents that are updated by the CSV import are removed from the Evidence Explorer and Custodian Facets.

Depending on your license, some filters may not be available.

General Facet Category

General Filters	Description
Evidence Explorer	Filters evidence based on the source of the evidence. Note: If you add new evidence to either an existing or an upgraded project, only the new evidence that has been added will populate this filter.
Custodians	Filters evidence based on people or custodians associated to the items in a project.
Authors	Filters evidence by author of Microsoft Office documents.
Object Types Object Sub-Type	Filters evidence based on the Object Type. You can expand an <i>ObjectType</i> facet for a list of object sub-type facets. See Object Types (page 56)

Tags Facet Category

Tags Filters	Description
Issues	Filters evidence based on issues tags. You can still filter for issues under the <i>Tags</i> tab.
Labels	Filters evidence based on labels tags. You can still filter for labels under the <i>Tags</i> tab.
Categories	Filters evidence based on category tags. You can still filter for categories under the <i>Tags</i> tab.
Case Organizer	Filters evidence based on summaries. You can still filter for summaries under the <i>Tags</i> tab.
Production Sets	Filters evidence based on production sets. You can filter out the produced records from the normal view. When a production set is created, a new facet is added to the Production Set Facet and by default this facet is set to exclude those records from the <i>Item List</i> grid. These records can be displayed by simply clicking the facet until you have a check mark and then applying the setting.

Email Facet Category

Email Filters	Description
Email Senders Display Name	Filters evidence based on the email senders display name.
Email Senders Address	Filters evidence based on the email senders address.
Email Senders Domain	Filters evidence based on the email senders domain.
Email Recipients Display Name	Filters evidence based on the email recipients display name.
Email Recipients Address	Filters evidence based on the email recipients address.
Email Recipients Domains	Filters evidence based on the email recipients domain.
Email Recipients BCC	Filters evidence based on BCC recipient address, display name, and domain.
Email Recipients CC	Filters evidence based on CC recipient address, display name, and domain.
Email Recipients To	Filters evidence by To recipient address, display name, and domain.
Email by Date	Filters evidence by email date. You can select to filter by the Delivered date or the Submitted date.
Email by Date Range	Filters evidence by either the delivered (received) date or by submitted (sent) date. You can enter a start range or/and an end range. Both fields are not required for the search.
Email Status	Filters evidence by email status, including: attachments, related items, replies, and forwarded.

File Filters Facet Category

File Filters	Description
File by Date Range	Filters evidence by the Date Range: by modified date, by creation date, and by accessed date. You can enter a start range or/and an end range. Both fields are not required for the search.
File Extensions	Filters evidence by file extension, including: .doc, .docx, .log, .msg, .rtf, .txt, .wpd, .wps. This filter is both sortable and searchable.
File Size	Filters evidence by file size. <ul style="list-style-type: none">● Empty = 0KB● 0KB < Tiny <= 10KB● 10KB < Small <= 100KB● 100KB < Medium <= 1MB● 1MB < Large <= 16MB● 16MB < Huge <= 128MB● 128MB < Gigantic

File Filters Facet Category (Continued) (Continued)

File Filters	Description
File Category	Filters evidence by file category, including: archives, databases, documents, email, executables, folders, graphics, internet/chat files, mobile phone data, multimedia, OS/file system files, other encryption files, other known types, presentations, slack/free space, spreadsheets, unknown types, and user types.
File Status	Filters evidence by file status, including: bad extension, email attachments, email related items, encrypted files, and OLE sub-items.

KFF Facet Category

KFF Filters	Description
KFF Vendors	Filters evidence by vendor as listed in the KFF Vendor field.
KFF Groups	Filters evidence by group as listed in the KFF Groups field.
KFF Statuses	Filters evidence by status according to the KFF Statuses field. There are two possible KFF Statuses, Unknown (0), Ignore (1), and Alert (2). The KFF Status, Ignore (1) is not included in an evidence search because it was already ignored by KFF during the initial evidence search.
KFF Sets	Filters evidence by sets at listed in the KFF Sets field. KFF Sets contain multiple document hashes.

For information about KFF, see [Reviewing KFF Results](#) (page 191)

Geolocation Facet Category

Geolocation Filters	Description
From Country Name	Filters evidence by the country that the communication originated from.
To Country Name	Filters evidence by the country that the communication was sent to.
From City Name	Filters evidence by the city that the communication originated from. Example: San Francisco, San Jose, Los Angeles.
To City Name	Filters evidence by the city that the communication was sent to. Example: San Francisco, San Jose, Los Angeles.
From Continent	Filters evidence by the continent that the communication originated from.
To Continent	Filters evidence by the continent that the communication was sent to.

For information about Geolocation, see [Using Visualization Geolocation](#) (page 72).

Document Content Facet Category

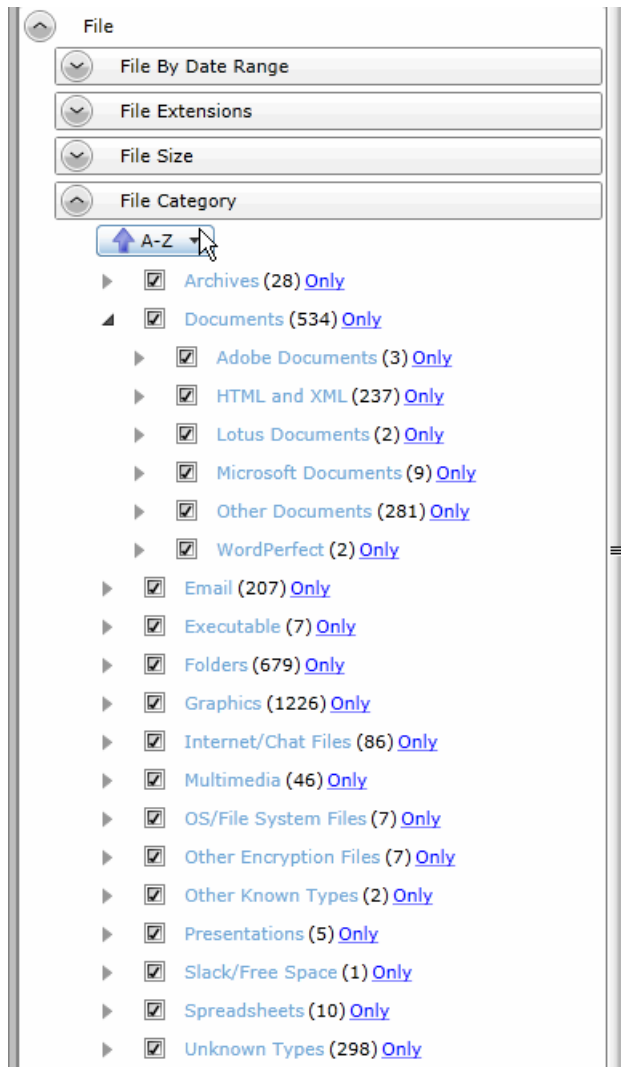
Document Content Filters	Description
Cluster Topic	Filters evidence by clusters of similar documents. These clusters are determined by cluster analysis of the documents. See <i>Using Cluster Analysis</i> in the <i>Admin Guide</i> .
Credit Card Numbers	Filters evidence based on extracted credit card numbers. See <i>Using Entity Extraction</i> in the <i>Admin Guide</i> .
Email Addresses	Filters evidence based on extracted email addresses found within the body of documents, not in the email meta data. For Email addresses found in To: or From: fields in Email meta data, use the Email facet category. See <i>Using Entity Extraction</i> in the <i>Admin Guide</i> .
People	Filters evidence based on extracted people's names. See <i>Using Entity Extraction</i> in the <i>Admin Guide</i> .
Phone Numbers	Filters evidence based on extracted phone numbers. See <i>Using Entity Extraction</i> in the <i>Admin Guide</i> .
Social Security Numbers	Filters evidence based on extracted social security numbers. See <i>Using Entity Extraction</i> in the <i>Admin Guide</i> .

Examples of How Facets Work

Including and Excluding Items

Next to each facet within a filter is a check box. By default, all facets within each filter are selected. Next to each facet is also a count of the number of files that match that facet's criteria.

The following figure shows an example of the *File Category* filter with all of the individual facets in that category.



As an example of how you can use this category, to help reduce irrelevant files, you can exclude executable and system files.

For each facet, there is also a link labeled *Only*. You can click *Only* for a facet and that one facet will be checked and all other facets within that filter will be cleared. This action only affects that particular filter that you are working with. All other filters in the Facet Panel will remain as you have previously set them.

You can also click on the facet name which will exclude all other facets and all other filters.

See [Using Facets](#) on page 53.

Excluding Tags Facets

In addition to using the *Only* link, you can exclude *Tags* filters (categories, issues, and labels) from a facet search. This allows you to further narrow and refine your facet scope.

The default for the *Tags* facet displays as checked or included. Selecting the check box once actively excludes the facet in the *Tags* filters. Selecting the check box a second time clears the check box and the facet is not included in the facet search.

When excluded, a red **x** appears in the facet check box, indicating that the facet is excluded. The hyperlink to apply the excluded facet is disabled.

You need to be aware of the following considerations when actively excluding *Tags* facets:

- For labels, the exclude feature applies to all labels in a group. However, if there are children under the labels, and one child label is selected for exclusion while another is not, the label group appears blank. This is because you cannot include a whole label group when one of the child labels is excluded.
- For issues, you can exclude or include an individual issue. Additionally, you can exclude a child issue while including a parent issue or vice versa.
- If you have a document that has been assigned a tagged item that is included in a facet in the *Tags* filter and has also been assigned a tagged item that is excluded in a facet in the *Tags* filter, the facet does not display the document. For example, a document may be tagged with both Tag 1 and Tag 2. If all documents with Tag 1 are included in the facet and all documents with Tag 2 are excluded in the facet, the document with both Tag 1 and Tag 2 is not posted to the Item List. The exclusion takes precedence. This is because exclusions and inclusions in facets act as an AND property, not as an OR property.

Using a Single Facet

You can filter your evidence based on one or more facets within a given filter or based on one or more facets across multiple filters. There may be times when you want to use a single facet.

For example, there is a filter category called *Tags*. Inside that category is a filter called Labels. Nested inside the Label filter are facets for each of the labels that have been used in the project. You can clear all but one label facet and only the files with that label are displayed; all other files are excluded.

However, the action of clearing all but one label facet will not exclude documents with multiple labels, if one of those labels is within the scope of the selected label facet. Even if the non-selected label facet is left unchecked, documents with multiple labels will be included.

Using Multiple Facets in a Single Category

You can filter evidence using multiple facets within a single filter category. For example, there is a filter category called *File Category*. Inside that category are individual filter facets for each type of files that are in the project (archives, documents, emails, graphics, spreadsheets, and so on.) You can exclude the types of files that you do not need to review while leaving the file types that you do want to review.

Using the N/A Facet

In most of the filter categories, there is a special facet that is labeled *N/A*, which stands for “not applicable.” If you check this, the filter will display items to the results that are not applicable to that category.

For example, if you apply a single facet for one or more email addresses, and *N/A* is unchecked for that category, then the only results will be records that contain an email address. If you also check *N/A*, then other file types will also be displayed, such as documents, spreadsheets, and PDFs, because they don’t have an email address property.

As another example, you can see a list of all files that do not have a person applied to them. In the *People* category, you can select only the *N/A* facet, and that excludes all files that have a person applied.

If your project has no files that pertain to a filter, it will show *N/A* as the only item in the facet.

Refining Evidence Using Facets in Multiple Categories

You can use multiple facets together in order to further refine your evidence. For example, you may have applied a facet for a single person and want to refine it further to only include spreadsheets and documents that are related to that person. You can apply another set of facets for file extensions choosing to exclude all files but *Documents* and *Spreadsheet* files. By combining the two facet categories, you can display only spreadsheets and documents that have a certain person.

Assume you want to find all the PDFs associated with a person named Sarah. In the Person filter, you would deselect all facets except for Sarah, who has 20 files of multiple file types associated with her. In the File Extensions filter, you would deselect all facets except for PDF, which has 40 different people associated with it. Since five of those PDFs are associated with Sarah, only those five PDF would display in the results.

Almost every filter can be used together to find information. Most filters treat the combination as a Boolean AND operator in conjunction with other filters. (In the example of Sarah and the PDFs, the search syntax was: Where Person = Sarah AND File Extension = PDF.) The only filters that cannot act as an AND operator against other filters are Email Sender’s Display, Address, and Domain, as well as the Email Recipient’s Display, Address, and Domain filters. These filters act as OR operators.

You would use the filters with the OR operator functionality when you wanted results that produced returns of two different sets of data. For example, if you were to select the Sarah facet under the Email Senders Display filter and the accessdata.com facet under the Email Senders Domain, you would get results of all emails where the email was sent by Sarah. You would also get results of all the emails that were sent within the accessdata.com domain. The search syntax would be: Where Email Senders Display = Sarah OR Email Senders = accessdata.com.

If you want to narrow the scope of your search using OR filters, you must use a filter that operates as an AND operator with one of the filters that operate as an OR. For example, if you were to select the *Sarah* facet under the *Email Senders Display* and the *Larry* facet under the *Email Recipients To*, this would return results of emails that contained both Sarah in the *Email Senders Display* field, and Larry in the *Email Recipients To* field.

Examples of Using Facets in Multiple Categories

Assume you need to create an export set of a specific person's data, but at the same time, remove anything that is obviously unimportant to reviewers. You can do the following:

- Using the *People* category, select only the one person.
- Using the *File Extensions* category, exclude unimportant file types, such as *EXE* and *DLL* files.
- Using the *Email Senders Domain* category, exclude all emails that came from *ESPN.com* and *Comcast.com*.

As another example, a development in a project may reveal that some very important evidence may exist as an email attachment sent either to or by a person within a specific date range. You can do the following:

- Using the *People* category, select only the one person.
- Using the *File Status* category, select only *Email Attachments*.
- Using the *Email by Date* category, select only emails delivered in March and April of 2009.

Email Recipient and Senders Facet Counts

When viewing facets, a count of the items related to each facet is displayed. For any given facet that is selected, the filter count will be part of the total number of items displayed in the Item List. For example, suppose you configure facets to show only PDF and XLS files and the facet counts show 6 PDF files and 4 XLS files. In the Item list, only the 10 PDF and XLS files will be displayed. The total of the two facet counts will match the number of files in the Item List.

There is a situation where the facet count may be higher than the count of items in the Item list. There are six different filters that are related to email recipients and senders. To help reduce the length of the list of recipients, there is a first-level division that contains alphabetical ranges of the names that are used. For example, ABurr --> AHamilton, ALincoln --> ASteverson, and so on. From that first level, you can drill down to individual names.

The facet counts displayed for the first levels (a range of names) may be higher than the number of emails in the Item List. The reason is that a single email may have been sent to multiple recipients. In the Item List, that email is reflected as one single item, yet in the first-level list of the facet, the counts may reflect 5 recipients of that one email. Because there can be more recipients than emails, this can cause the first-level facet count to be higher than the Item List count.



Using Facets

To use facets, you specify the items that you want to include. As you specify facets, the results are displayed to the *Item List*. As you clear facets, files are removed from the *Item List*.








The *Filters* list denotes with an icon which facets you have configured.

Note: You must be careful when filtering evidence. Once evidence has been culled using a facet in the *Facets* panel, the only way to display that evidence again is to recheck the specific facet or reset all of the facets. No other facet will return the evidence to the item list.

To apply a single facet to evidence

1. In the *Facets* panel on the *Project Review* page, expand the filter category that you want to use. For a list of filter categories, see [Available Facet Categories](#) (page 45).
To expand all categories, click  **Expand**.
2. In the expanded filter, click the *Facet name* link.
Click this link to filter out all other facets and filters.
For example, in the filter, if you click the facet named **Email**, you will only get email messages.
3. To reset a single facet, click .

To apply one or more facets to evidence

1. In the *Facets* panel on the *Project Review* page, expand the filter that you want to use. For a list of filters, see [Available Facet Categories](#) (page 45).
To expand all filters, click  **Expand**.
2. In the expanded filter, perform one of the following tasks:
 - **Check:** Manually check the items that you want to include.
 - **Uncheck:** Manually uncheck the items that you want to exclude.
 - **Only:** Click **Only** to uncheck all other facets in the filter.
 - **Expand:** Many facets can be expanded to show dynamic facets. For example, in the Email By Date filter, there is a Delivered facet. You can expand it to show detailed facets for years, months, or days.
3. Click  **Apply**.
The *Item List* will change to display only the items that you filtered for.
When you change the configuration of a category, a  appears next to the category name. This shows you which categories have been configured.
4. (Optional) Repeat steps 2 and 3 as often as needed. After making any changes, you must click  **Apply**.
5. (Optional) To reset facets, do any or all of the following:
 - To undo an individual facet, check the box for an item that you previously unchecked.
 - To reset all facets in a single filter category, click the  next to the filter name.
 - To undo all filters, click  **Reset**.
6. Click  **Apply**.

Caching Filter Data

If you use the same filters a lot, you can cache your results in the database so that the next time you use the filter, your results will appear faster.

To cache a filter result set

1. Set filters that you commonly use in the *Project Review*.
2. In the *Item List* panel, select **Options > Cache > Add** current filter to cache.
Your data is cached in the database and the cached icon turns orange.

Cached Icon in the Item List Panel

Views:  



Filtering by Column in the Item List Panel

You can filter the evidence in the *Item List* panel by the data in the columns. You cannot filter the content of the first three columns. You can apply multiple column filters.

For ore information, see [Filtering Content in Lists and Grids](#) (page 39).

Note: Column Filters are applied after facet scope filters and visualization filters. Changing your facets scope or visualization filters will clear the column level filters. Also, Column Filters do not persist and will be cleared out when you either execute a new search or use the **Clear Search** button.

To filter evidence by data in columns

1. In *Project Review*, ensure the *Item List* panel is showing.
2. Select the document groups, labels, or issues that you want to view from the *Project Explorer* and click Apply.
3. In the *Item List* panel, click on the column filters button .
4. Uncheck the items that you want to filter out of your view.
5. (Optional) You can use the *Search* field to search by keyword among the items in the column.
6. (Optional) Expand the Sort drop-down to sort the items in the column by ascending or descending hits or values.
7. Click  **Apply**.


All documents with the item that you unchecked are removed from the *Item List* panel.

Note: When you filter the ProductionDocID column, only the produced record value is displayed, not the source document.

Clearing Column Filters

You can clear column filters that you have applied to the *Item List* panel.

To clear column filters

1. In *Project Review*, ensure the *Item List* panel is showing.
2. Select the document groups, labels, or issues that you want to view from the *Project Explorer*.
3. In the *Item List* panel, click on the column filters button .
4. Click **Clear Filter**.

Object Types

You can use columns and facets to view an item's Object Type and cull data based on the Item Types in your evidence.

Some *Object Types* have *Object Sub-Type* data. For example, for the Endpoint Event object type, you can have the following object sub-types: File Event, Network Event, Registry Event, and Endpoint OS Event.

With the *ObjectType* and *ObjectSubType* columns, you can search, filter, and sort on these columns in order to quickly cull down the files that you are viewing.

The *Object Type* facets, which are under the *General* facet category, dynamically list facets for all of the object types in your evidence. You can expand an *ObjectType* facet for a list of object sub-type facets.

The following table lists the object types and object sub-types that may exist in your data.

Object Types and Object Sub-Types

Object Types	Object Sub-Types
Unknown	
Partition	
File System	
Live Folder	
Live File	
Directory	
File or Loose Files (Listed in the Facets as Files & Email) Files that are added through Import have the object type of <i>Loose Files</i> , whereas files added as evidence have the object type of <i>Files</i> .	<ul style="list-style-type: none">• Documents• Spreadsheet• Database• Presentations• Graphics• Multimedia• Email• Executable• Archives• Folders• Slack Free Space• Other Known• Mobile Device Items• Encryptions Files• Internet Chat• OS Files• Transcripts• Exhibits• Notes
Mailbox	
Archive	
Unpartitioned Space	

Object Types and Object Sub-Types (Continued)

Object Types	Object Sub-Types
Carved File	
Drive Remote	
File Slack	
File System Remote	
Custodian Group	
Removable Media File	<ul style="list-style-type: none"> • Devices Inserted • Devices Removed • Files Copied From Device • Files Copied To Device
Network Traffic	<ul style="list-style-type: none"> • There are many types, for example, WebMail, SMTP email, Chat, and FTP.
Threat Scan	
Endpoint Event	<ul style="list-style-type: none"> • File Event • Registry Event • Network Event • OSEvent • ProcessEvent
Mobile	
Case Organizer	<ul style="list-style-type: none"> • Event • Fact • Person • Question • Research • Pleading • Summary
Volatile	<ul style="list-style-type: none"> • There are many types, for example, Process, DLL, Socket, Driver, Service, Registry Key, Registry Value

Chapter 6

Using Visualization

Culling Data with Visualization

Visualization allows you to see visual representations of data in the selected project and to filter the data, based on the visualization graphs. The Visualization feature allows you to choose the type of graph in which to display the data. The graphs are interactive, allowing you to isolate and search on sections of the graph. Once you select how you want the data represented, you can apply the visualization filter to the data. The filtered data will appear in the Item List, and you can apply additional scope filters and column filters to further cull the data.

You can also clear previous visualization filtering sessions in the **Options > Visualization** dialog. If no previous visualization filter has been applied to the data, the Clear Visualization options are inactive.

You can apply visualization filters to the data in the following ways:

[Files Visualization](#) (page 59)

[Emails Visualization](#) (page 62)

[About Geolocation Visualization](#) (page 72)

[Using Visualization Social Analyzer](#) (page 65)

[Using Visualization Geolocation](#) (page 72)

Files Visualization

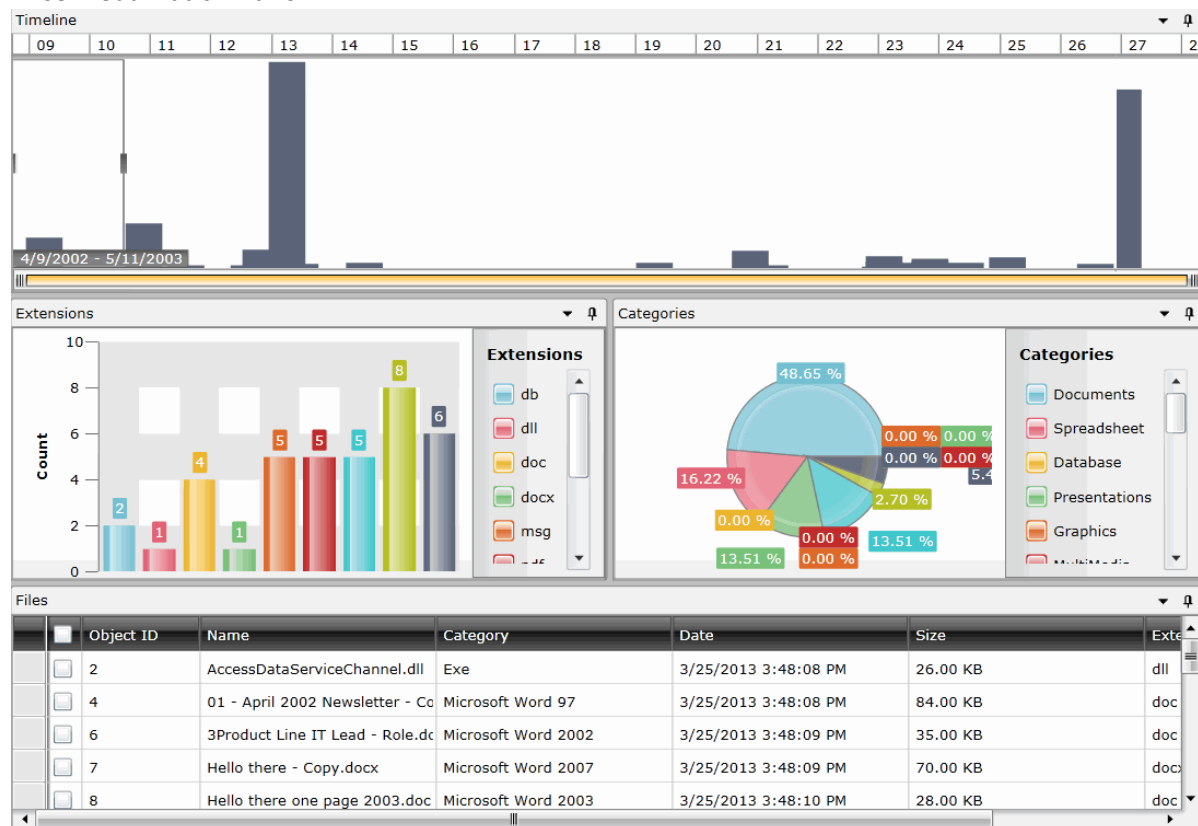
Files Visualization allows you to view and filter data in a project by using the same data that is posted in the *Item List* grid. This allows you to cull the data in the *Item List* grid with filters before applying Files Visualization to the data.

To access Files Visualization


1. Click **Project Review**.
2. In the *Item List* panel, click **Options > Visualization > Files**.





Important: When you first open File Visualization, the *Files* grid will show only a portion of the total files. The *Files* grid only shows the files that are currently filtered using the Visualization tool. Initially, the top *Timeline* filter only covers a small part of the total timeline, as a result, you may not see many files listed in the *Files* grid. You can expand or move the *Timeline* filter to show other files.

Files Visualization Panel



Files Visualization Options Panel

Options 

Data

Scale Linear

Metrics ByCount

View

Timeline Date Type Created








Timeline Graph Type Bar

Extension Graph Type Bar

Categories Graph Type Pie

The following table identifies the tasks that you can perform from the **File Visualization** panel.

File Visualization Panel Options

Element	Description
 Apply Visualization	<p>Applies the files that have been filtered in the visualization graph filters to the <i>Item List</i> grid. Once applied, only those items filtered with visualization appear in the <i>Item List</i> grid.</p> <p>To remove the filters, re-enter files visualization and click  Cancel.</p> <p>Note: If you use the “check all” button in the visualization Files grid, be aware that only the items on the current page will be selected.</p>
 Cancel Visualization	Cancel the visualization graph filters and exit out of Visualization.
Options	
 Refresh Timeline	Refreshes the Timeline pane.
 Refresh Extensions	Refreshes the Extensions pane.
 Refresh Categories	Refreshes the Categories pane.
 Refresh Files	Refreshes the Files pane.
Data	<ul style="list-style-type: none"> Scale - Choose to display the data scale either by logarithmic or by linear. If this field is changed, data in the panes will refresh automatically. Metrics - Choose to display the data metrics either by size or by count. If this field is changed, data in the panes will refresh automatically.
View	<ul style="list-style-type: none"> Timeline Data Type - Choose to display the data in the timeline, extensions, categories, and files panes by date created, modified, or accessed. Timeline Graph Type - Choose to display timeline data by bar, line, area, or scatter graph. Extension Graph Type - Choose to display extension data by bar or pie graph. Categories Graph Type - Choose to display category data by bar or pie graph.

File Visualization Panel Options

Element	Description
Timeline	Examine the data based on when the data was created, accessed, or modified. You can highlight a specific period of time in the timeline and filter data based on that specific time.
Extensions	Displays the data by document's extension, such as .doc or .dll. Only extensions found in the data set will display in the graph. You can click a specific extension in the graph's list or graphic, and all files with that extension will appear in the Files panel.
Categories	Displays the data by category. The categories available by which to sort are documents, spreadsheets, database, presentations, graphics, multimedia, email, executables, archives, folders, slack free space, encryption files, internet chat, operating system file, other known, unknown, user types, stego apps, and mobile device items. You can click a specific category in the graph's list or graphic, and all files within that category will appear in the Files panel.
Files	Displays the files represented by the visualization graphs. This list can be all of the data set, or only files filtered by either timeline, extensions, or categories. You can sort information in each column by clicking the column header.
History	The <i>History</i> tab captures the movement of the box that isolates a time period within the time line. Each time that you move the box along the timeline, a new tab is created for that section of the timeline. Each section can be identified by start date and end date. By clicking one of the History tabs, you can examine the data from that particular time period, allowing you to quickly return to a period that you have already examined.
Selected	Lists the files selected in the Files pane.

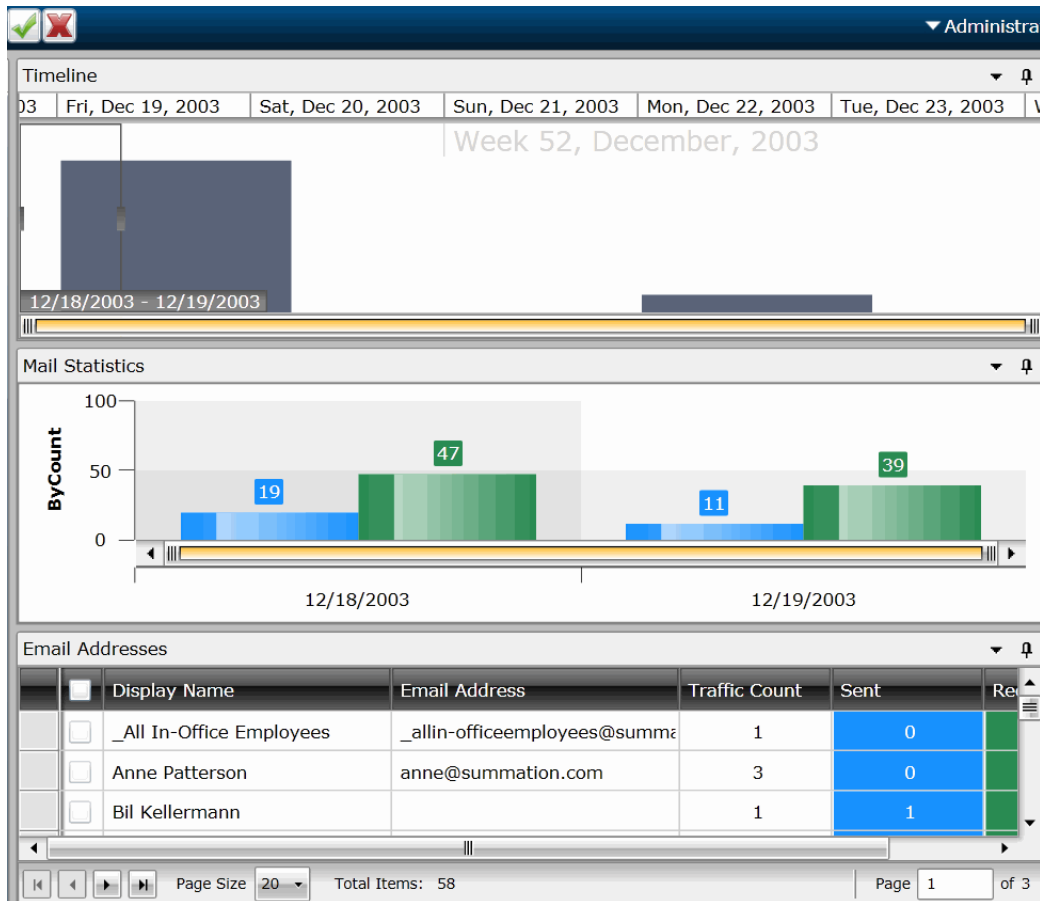
Emails Visualization

Emails Visualization allows you to view and filter data in a project by using the same data that is posted in the *Item List* grid. This allows you to cull the data in the *Item List* grid with filters before applying Emails Visualization to the data.

To access Email Visualization





1. Click **Project Review**.
2. In the *Item List* panel, select **Options > Visualization > Emails**.

Emails Visualization Panel



Email Visualization Options Panel

Options
⌵

Data

Scale Linear

Metrics ByCount







View

Timeline Graph Type Bar

Mail Stats Graph Type Bar

The following table identifies the tasks that you can perform from the **Emails Visualization** panel.

Emails Visualization Panel

Element	Description
 Apply Visualization	Apply the visualization graph filters to the <i>Item List</i> grid. Once applied, only those items filtered with visualization will appear in the <i>Item List</i> grid.
 Cancel Visualization	Cancel the visualization graph filters and exit out of Visualization.
Options	
 Refresh Timeline	Refreshes the Timeline pane.
 Refresh Mail Statistics	Refreshes the Mail Statistics pane.
 Refresh Email Addresses	Refreshes the Email Addresses pane.
 Launch Social Analyzer	Click to launch the Social Analyzer pane. See Using Visualization Social Analyzer on page 65.
Data	<ul style="list-style-type: none"> Scale - Choose to display the data scale either by logarithmic or by linear. If this field is changed, data in the panels will refresh automatically. Metrics - Choose to display the data metrics either by size or by count. If this field is changed, data in the panels will refresh automatically.
View	<ul style="list-style-type: none"> Timeline Graph Type - Choose to display timeline data by bar, line, area, or scatter graph. Mail Stats Graph Type - Choose to display mail stats graph by bar, line, spline, or scatter graph.
Timeline	Examine the email data set based on when the emails were created, accessed, or modified. You can highlight a specific period of time in the timeline and filter the emails based on that specific time.
Mail Statistics	Displays the Mail Statistics of the emails - the sent and receive dates. You can click a specific item in the graph and filter the email addresses in the email addresses list.

Emails Visualization Panel

Element	Description
Email Addresses	Lists the email addresses in the email data set. You can view display name, email address, traffic count, and the sent and received data. Expand either the sent or received field for a particular email address to obtain additional information.
Selected	Lists the history of the data set. By highlighting a tabbed date in <i>History</i> , you can examine the data from that particular time period.
History	Lists the files selected in the Files pane.

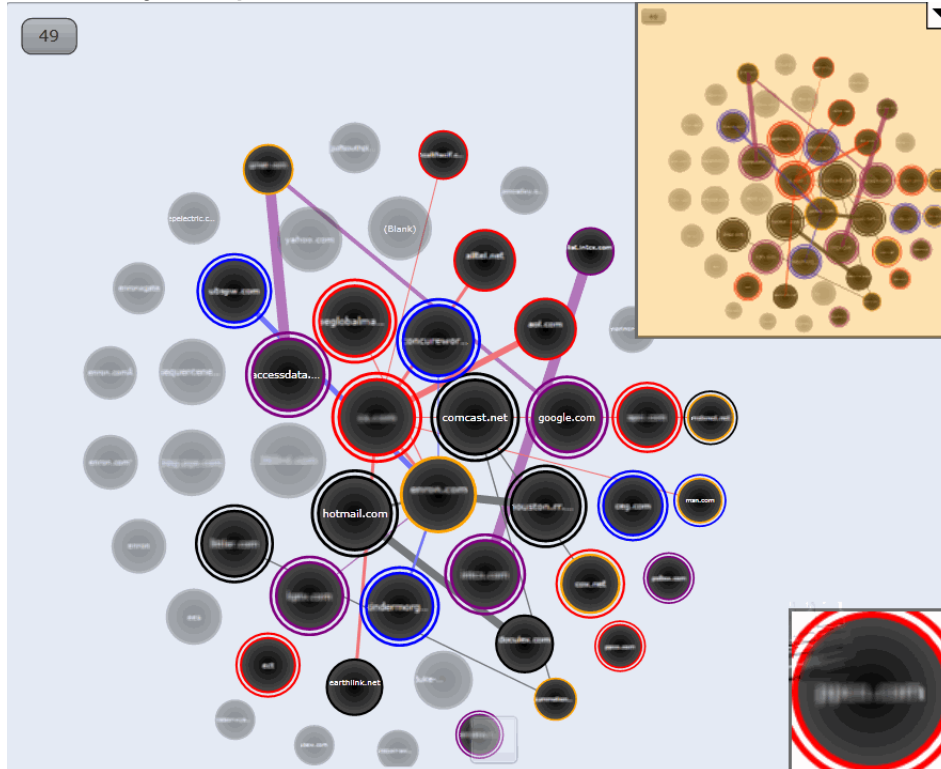
Chapter 7

Using Visualization Social Analyzer

About Social Analyzer

The Social Analyzer shows a visual representation of email volume contained in the data set. Social Analyzer will display all of the email domains in a project, as well as individual email addresses within the email domains.

Social Analyzer Map



The Social Analyzer map displays emails in the data set group by domain name. These domain names appear on the map in circles called “bubbles.” The larger the bubble, the more emails are contained within that domain. The bubbles in the map are arranged in a larger sphere according to how many emails were sent to that domain. The center bubble in the sphere will have the most emails sent from this domain, while domains radiating clockwise from the center will have fewer and fewer emails in their domain bubble. If you want to examine email domains with the most sent emails, concentrate on examining the bubbles in the center of the map.

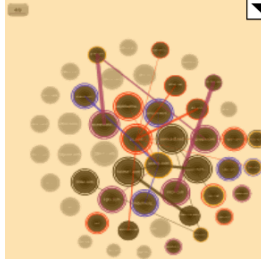




Email data in the Social Analyzer map can be examined on two different levels. On the first level, you can get an overall view of communications between domains. You can then select domains that you want to examine in a

more detailed view and expand those domains to view communications between specific email addresses from the domain. For example, if you search for high email traffic between two domains, you can see which two domains have the highest amount of traffic between them. Select the two domains, and expand them to view the email traffic between individual users from those two selected domains.

See [Analyzing Email Domains in Visualization](#) on page 69.

See [Analyzing Individual Emails in Visualization](#) on page 69.

Elements of the Social Analyzer Map

Element	Description
	<p>This map presents the overall view of the social analyzer data. The orange rectangle indicates the area displayed in the main social analyzer map. Black dots in the overall view show domains that are either selected or communicating. You can either expand or collapse the overall view by clicking on the triangle in the upper right corner.</p>
	<p>When you select a domain bubble, it is surrounded by a colored double ring. The ring may be colored blue, black, purple, or red. The different colors allow you to distinguish between different selected domains, but they do not have any significant meaning.</p>
	<p>Domain bubbles that are not selected, but have sent emails to the selected domain bubble, are surrounded by a single colored ring that is the same color as the selected domain bubble. This allows you to easily tell which domains have been communicating with the selected domain bubble. Domain bubbles that do not connect to any selected domains are greyed out.</p>
	<p>Lines connect other domain bubbles to the selected domain bubble. These lines represent emails sent to the selected domain from other domains. The more emails that have been sent to the domain, the thicker the line between domain bubbles are. You can also see emails sent from the selected domain. Select Show Reversed Connections in the Social Analyzer panel to show visual representations of emails sent from the selected domain.</p>
	<p>A domain bubble with an orange ring indicates that a domain has been connected to from another domain multiple times. This allows you to pinpoint domains that have heavy communication between them.</p>

Accessing Social Analyzer

To navigate throughout the **Social Analyzer** pane, click and drag inside the pane. Hover over an email domain bubble to view the total number of emails that were sent from the domain.

Note: Expansion of large datasets may result in slow server speeds and slow rendering the Social Analyzer visualization data.

To access Social Analyzer

1. Click **Project Review**.
2. In the *Item List* panel, click **Options > Visualization > Social Analyzer**.

Social Analyzer Options Panel

Options

View

- Show Reversed Connections
- Show Connections
- Preview Connections on Hover

Email Display:

Bubble Limit:

Stats - Level One

Total Domains:	3
Selected Domains:	0
Pending Bubbles:	0
Domains After Expand:	3
Emails After Expand:	0
Bubbles After Expand:	3









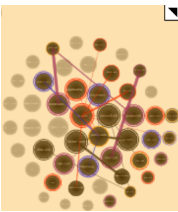
Legend

- Connected multiple times

Social Analyzer Options

The following table identifies the tasks that you can perform from the **Social Analyzer** panel.

Social Analyzer Options

Element	Description
 Apply Visualization	Applies the visualization graph filters to the <i>Item List</i> grid. Once applied, only those items filtered with visualization will appear in the <i>Item List</i> grid.
 Cancel Visualization	Cancels the visualization graph filters and exits out of Visualization.
 Refresh	Refreshes the Social Analyzer pane.
 Clear Selections	Clears the selected bubbles in the Social Analyzer pane.
 Select Most Connected Items	Selects the ten bubbles that have been most connected to in the Social Analyzer pane. Each time you click this icon, the next top ten bubbles will be selected, and so forth.
 Expand Selected Domains	Expands selected domains in the Social Analyzer pane. You can drill down to a second level to examine the email data. See Analyzing Individual Emails in Visualization on page 69.
 Zoom In	Zooms into the Social Analyzer pane. If you are unable to view the social analyzer data, click Zoom In to locate the data. You can also zoom in by expanding the slider bar located at the bottom of the Social Analyzer pane, by using the + key on the keyboard, or by scrolling the mouse wheel up.
 Zoom Out	Zooms out of the Social Analyzer pane. You can also zoom out by expanding the slider bar located at the bottom of the Social Analyzer pane, by using the - key on the keyboard, or by scrolling the mouse wheel down.
	Expands and collapses the overall map of the data set. Dots that appear in black in the overall map are domains/emails that are connected to the selected domain/email. The orange rectangle on the map shows where the expanded location is on the map.
View	<ul style="list-style-type: none"> • Show Reversed Connections - Select to show all reversed connections in the pane. Reversed connections are emails sent from a particular email or email domain. • Show Connections - Select to show the connections between domains in the pane. Connections are emails sent to a particular email or email domain. • Preview Connections on Hover - Select to view connections between domains when you hover over them. This option is not selected by default to speed rendering of the map. • Email Display - Display email domains either by the display name or address. • Bubble Limit - You can choose a display limit of either 2,500, 5,000, or 10,000 domains. Server issues may occur with larger display limits.

Social Analyzer Options


Element	Description
Stats	<p>Displays the statistics of either the first or second level of the email domain data. You can view:</p> <ul style="list-style-type: none">• The total number of domains, emails, and bubbles in the pane.• The total number of selected domains, emails, and bubbles in the pane.• The total number of domains, emails, and bubbles that have been expanded. <p>You can access the second level of data by clicking Expand Selected Data.</p>

Analyzing Email Domains in Visualization

Once you have you opened the Social Analyzer pane, you can isolate and examine individual email domains.

Note: Social Analyzer is very graphics-intensive. In order to avoid server issues, you should cull the data with facets and other filters to isolate the information that you want to examine before viewing it in Social Analyzer.



To analyze email domains in Visualization mode

1. Click **Project Review**.
2. In the *Item List* panel, click **Options > Visualization > Social Analyzer**.
3. Click the domain bubbles to select the domain(s) that you want to view.
4. (optional) If you want to view the top ten domains in terms of received emails. click . Each time you click this icon, the next top ten bubbles will be selected, and so forth.
5. (optional) You can zoom in and zoom out of the Social Analyzer panel. If you hover over a domain bubble, the full display name and address, as well as the count, is displayed in the tool tip.
6. You can expand selected email domains and examine individual emails in a domain. See [Analyzing Individual Emails in Visualization](#) on page 69.

Analyzing Individual Emails in Visualization

You can expand email domains to display individual emails and the traffic between those emails.

To analyze individual emails within selected email domains

1. Click **Project Review**.
2. In the *Item List* panel, select **Options > Visualization > Social Analyzer**.
3. Click the domain bubbles to select the domain(s) that you want to view.
4. (optional) If you want to view the top ten domains in terms of received emails. click . Each time you click this icon, the next top ten bubbles will be selected, and so forth.
5. (optional) You can zoom in and zoom out of the Social Analyzer panel. If you hover over a domain bubble, the full DisplayName and address, as well as the count, will be displayed in the tool tip.
6. Click  to expand the domain names to display the individual emails.



Chapter 8

Using Visualization Heatmap

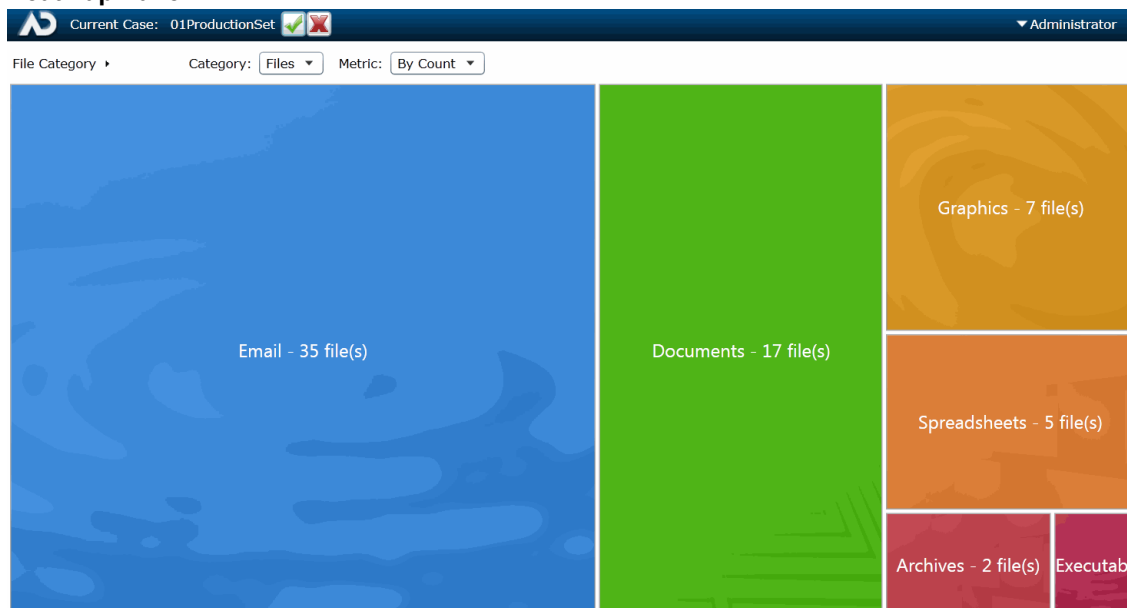
Heatmap allows you to view a visual representation of file categories and file volume within a project. Information displays in a grid comprised of squares of different colors and sizes. Each color represents a different file category, and the relative size of the square represents the file volume within the category. You can view each file category for more details about the files within that category (similar to a file tree) and navigate between file categories.

You can also switch between viewing the file volume by the physical size of each file and the file count. This allows you to see any discrepancies in the size of the files. For example, if someone were trying to hide a file by renaming the file extension, you could easily see the size discrepancy in the heatmap, and then investigate that particular file further.

To access Heatmap

1. In FTK, do the following:
 - 1a. Open the *Examiner*.
 - 1b. In the *File List* panel, click  (Heatmap).
2. In Summation, Resolution1 eDiscovery, Resolution1 CyberSecurity, or Resolution1, do the following:
 - 2a. Click **Project Review**.
 - 2b. In the *Item List* panel, click **Options > Visualization >  Heatmap**.



Heatmap Panel



Heatmap Options Panel

The following table defines the tasks from the **Heatmap** panel.

Heatmap Panel Options

Element	Description
	Cancels the heatmap filters and exits out of Visualization.
	Apply the visualization graph filters to the <i>Item List</i> grid. Once applied, only those items filtered with visualization appear in the <i>Item List</i> grid.
Options	
Category	<ul style="list-style-type: none">Files - Allows you to view files by the file category. You can view the files in each category:<ul style="list-style-type: none">By double-clicking that particular file category's square, orBy clicking the menu from the upper left side and choosing the file category that you want to view in the heatmap.Folders - Allows you to view files by the folders contained within the project. You can view the files in each folder:<ul style="list-style-type: none">By double-clicking that particular folder's square.By clicking the menu from the upper left side and choosing the folder that you want to view in the heatmap.Extensions - Allows you to view files by the file extension.
Metric	<ul style="list-style-type: none">By Size - Allows you to view file types by size of the files. The larger the files, the larger the represented square in the heatmap.By Count - Allows you to view file types by quantity. The more files of a particular type that are in the project, the larger the represented square in the heatmap.

Chapter 9

Using Visualization Geolocation

About Geolocation Visualization

Geolocation allows you to view a map with real-world geographic location of evidence items that have geolocation information associated with them. This lets you understand where certain activities/actions took place .

See [Using Visualization](#) on page 58.

For example, if you have photos in the evidence that have GPS data in the EXIF data, you can see where those photos were taken. For volatile/RAM data, you can see the lines of communication (both sent and received) between addresses, showing the location of all parties involved.

Geolocation supports the following data types:

- Photos with GPS information in the EXIF data.
- Live email sender and receiver IP data gathered using a Volatile Job in AD Resolution1 CyberSecurity and AD Resolution1.
- Email sender and receiver IP data gathered using a Network Acquisition Job in AD Resolution1 CyberSecurity and AD Resolution1. Because the data is gathered from Sentinel, the data displayed shows a snapshot of the traffic at the time that Sentinel captured the data.

Note: Geolocation IP address data may take up to eight minutes to generate, depending upon other jobs currently running in the application.

Geolocation Components

Geolocation includes the following components:

- Maps

When viewing geolocation data, you can use any of the three following maps:

- MapQuest Streets
- MapQuest Satellite
- OpenStreetMaps

You have the option to switch between the three map views while in the Geolocation filter.

- Geolocation Grid

Below the map, you can view a grid that shows details about the items in the map.

See [Using the Geolocation Grid](#) on page 78.

- Geolocation Data in columns in the *Item List*
You can view geolocation data for files in the *Item List*.
See [Using Geolocation Columns in the Item List](#) on page 79.
- Geolocation Facets
There are specific facets for filtering on Geolocation data.
See [Using Geolocation Facets](#) on page 80.

Geolocation Workflow

When you launch Geolocation, it will display all relevant files currently in the item list. You can cull the data using filters and other tools in the item list to limit the data that is displayed in geolocation.

General Geolocation Requirements


As a prerequisite, you must have the following:

- Access to a KFF Service Server.
 - The KFF Server can be installed on the same computer as the AccessData software or on a separate computer.
 - KFF Geolocation Data. This must be installed on the *KFF Server*.
See *Getting Started with KFF* in the *Admin Guide*.
- Internet access to view Web-based maps.
 - You can download the offline maps for Geolocation. Use the link **Geolocation Map for Offline Use** and **Geolocation Map for Offline ReadMe** on the FTK Product download page:
<http://www.accessdata.com/support/product-downloads/ftk-download-page>
- For AD Resolution1 Platform and AD Resolution1 CyberSecurity:
 - The Geolocation option selected when processing the evidence. This option allows the data to display properly in the Geolocation filter. Geolocation is selected by default when evidence is processed.
[Default Evidence Processing Options](#) (page 70)
- For FTK, FTK Pro, Lab, and Enterprise:
 - The File Signature Analysis option selected when processing the evidence.

Viewing Geolocation EXIF Data


When your evidence has photos with GPS information in the EXIF data, you can view photo locations.

To view EXIF data in FTK

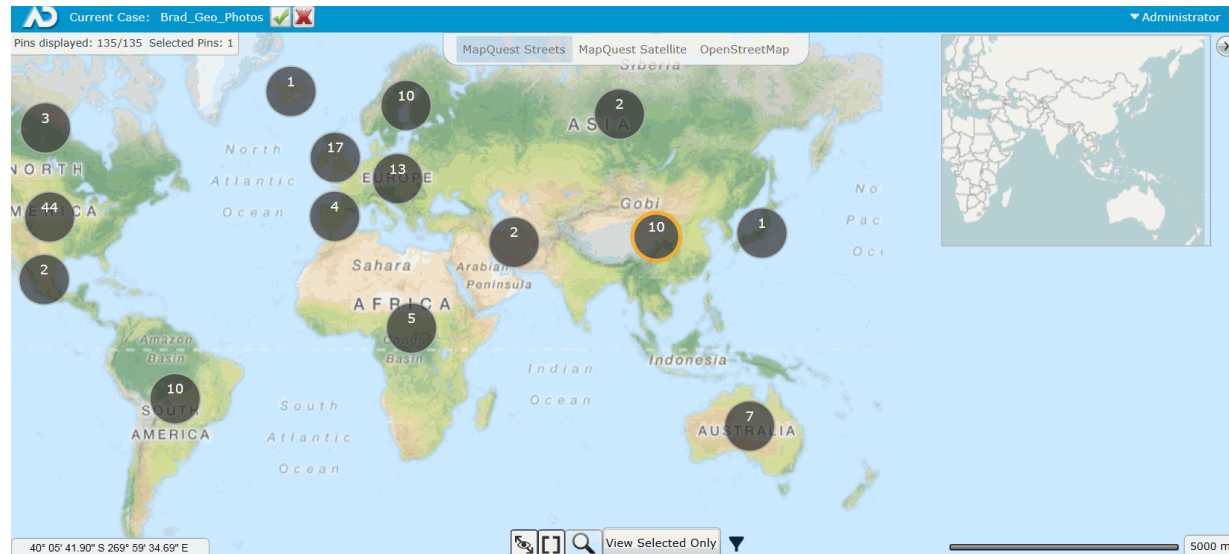
1. In FTK, open the *Examiner*.
2. In the *File List* panel, click  (Geolocation).
3. You can filter the items displayed and see item details..
See [Using the Geolocation Grid](#) on page 78.

To view EXIF data in Summation or Resolution1 products

1. Click **Project Review**.

- In the *Item List* panel, click **Options > Visualization >  Geolocation**.
- You can filter the items displayed and see item details..
See [Using the Geolocation Grid](#) on page 78.

Geolocation Panel - EXIF data



Using Geolocation Tools

The Geolocation Map Panel



Points of data in a particular area on the map are represented by large dots called clusters. The number on each cluster show how many points of data (known as pins) are represented by the cluster. Clicking a particular cluster on the map zooms in on a group of pins.

The general location of the clusters are determined by a central point on the map. The clusters radiate from this central point. When you zoom in and out of the map, your central point on the map moves as well, and clusters will shift position on the map. However, as you zoom into a cluster, the cluster rendered will more closely align itself with the location of the individual pins.

When viewing IP data, the connections between two pins display on the map as lines between clusters/pins. The width of the lines represent the amount of traffic between two IP address. The thicker the lines, the more traffic has occurred. Green lines represent traffic originating from the pin and red lines represent traffic entering the pin.



When you select a cluster and zoom in on a particular pin, you can select one or more pins. When a pin is selected, the outline and shadow of the selected pin turns orange. If you zoom out of the map, the cluster with one or more selected pins has an orange ring.

Hovering over the cluster displays the following icons:


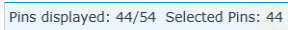

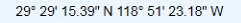




-  Selects all of the pins in a cluster.
-  Clears all of the selected pins in a cluster.

The following table describes the Geolocation panel options.

Geolocation Panel

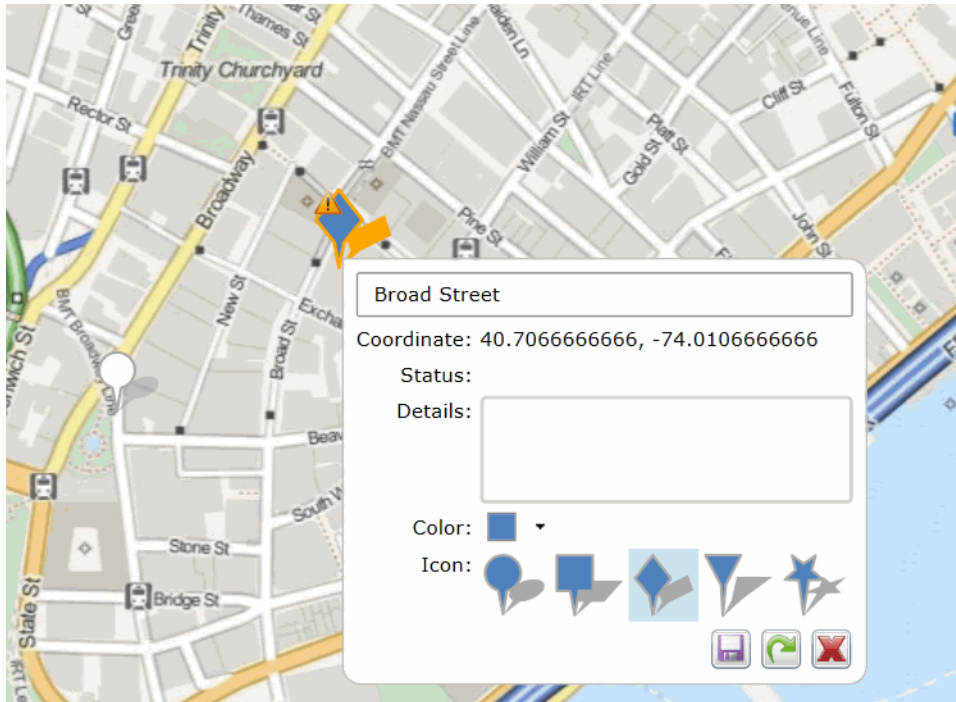
Element	Description
	<p>After filtering data by selecting one or more pins, this applies the selected geolocations to the <i>Item List</i> grid. Once applied, only those geolocations filtered with visualization appear in the <i>Item List</i> grid.</p> <p>For network data, you will see any communication from those pins to any other location. This may include one or more items.</p> <p>If you enter the Geolocation view again, only those geolocation will be displayed in the map.</p> <p>To reset the items in the <i>Item List</i>, click the Project Explorer's <i>Reset</i> and <i>Apply</i> icons.</p>
	<p>(Network Acquisition Job data from Resolution1 CyberSecurity or Resolution1 only)</p> <p>After filtering data by selecting one or more pins, this applies the selected geolocations to the <i>Item List</i> grid. Once applied, only those geolocations filtered with visualization appear in the <i>Item List</i> grid.</p> <p>This applies only the connections between the selected pins. As a result, it shows the communication between only the selected pins and not to other locations. This may include one or more items.</p> <p>If you enter the Geolocation view again, only those geolocations will be displayed in the map.</p> <p>To reset the items in the <i>Item List</i>, click the Project Explorer's <i>Reset</i> and <i>Apply</i> icons.</p>

Geolocation Panel

Element	Description
	Cancels the geolocation filters and exits out of Visualization.
<i>Pins displayed</i>	Shows the number of spins that are displayed and the number selected.
<i>Clear</i>	Clears and selected pins.
Options	
	Displays the number of pins selected in the map versus the number of pins available in the data.
Map Tab	
	Expands or collapses the overall view map.
	Displays the latitude and longitude where the mouse pointer resides. To view the position of a particular pin, hover the mouse over the pin. To view the exact coordinates of the pin, select the pin and right-click.
	Turns the connections between the pins/clusters either on or off.
	Displays all of the pins on the map.
	Zooms in or out on the map. A slide bar displays, allowing you to control the zoom feature.
View All/View Selected	
 Filter	Displays either EXIF data or network connection data. You can also view both types of data at the same time.

Right-clicking a pin displays more information about the pin.

Detail of Pin







In the pin dialog, you can:

- Add any notes
- View the exact coordinates and status of the pin
- View the IP Address of the pin

Note: To save processing time and to ensure data accuracy, the host name does not populate in the Geolocation pin. However, the host name does populate in the Item List.

- Change the color and shape of the pin

If you make any changes to the pin, a warning icon  displays that notifies you that changes were made to the pin and need to be saved. You can do the following in the pin dialog:

- Click  to save the changes that you have made to the pin
- Click  to reset the pin. If changes have been saved previously to the pin, this action resets the pin to the saved version
- Click  to close the dialog

Using the Geolocation Grid

When you open Geolocation, you can view a grid that shows details of the items on the map.

The Geolocation Grid has two tabs:

- **Network Communication:**

In Resolution1 CyberSecurity and Resolution1, this shows network acquisition and volatile data from security jobs.

In FTK, this show data from the *Volatile* tab.

You can see the following

- *Process Start Time* column
- *Machine* column
- *Process Name* column
- *Path* column
- *Host Name* column
- Bar chart (Resolution1 CyberSecurity and Resolution1 only)
 - Within the *Network Communication* tab, you can also view a bar chart that shows the count of items sorted by either *Process Name* or by *Machine* (computer IP address).

- **Exif:** This shows the following Exif data from photos

- *Capture Data* column
- *File Name* column
- *File Size Coordinate* column


When you click an item in the grid, the map will be centered to reflect the location of the selected item.

You can minimize the grid so that the whole map is visible.

Filtering Items in the Geolocation Grid

When you first launch Geolocation, all of the items on the map are shown in the grid.

You can filter the contents of the grid in the following ways.

- In the map, if you select a pin, only that item is displayed. You can click (and select) multiple pins.
- In the map, if you right-click a cluster and click  , that selects all of the pins in a cluster. This will filter the grid to those clustered pins. You can add multiple clusters to the grid.
- In the grid, the columns in the Geolocation Grid can be filtered to cull the items in the grid. For Network Communication data, the data in the bar chart is filtered as well when columns are filtered.

Using Geolocation Columns in the Item List

The data that the Geolocation filter uses to render the information is also available in columns in the *Item List*. You can find the following columns in the *Item List*, depending upon the data that has been collected. These columns can be sorted and filtered.

Data for geolocation columns require that the KFF Geolocation Data be installed.

See [General Geolocation Requirements](#) on page 73.

Geolocation EXIF Data Columns

When your evidence has photos with GPS information in the EXIF data, you can view data using the following columns.

Geolocation Columns: EXIF data

Column	Display name	Description
Geotagged Area Code:	Area Code	Area code location of geotagged photo or object.
Geotagged City:	City	City location of geotagged photo or object.
Geotagged Country Code:	Country Code:	ISO country code location of geotagged photo or object, such as USA, FRA, MEX, HKG, and EST.
Geotagged Direction:	Direction	Direction geotagged photo or object.
Geotagged Latitude:	Latitude	Latitude of geotagged photo or object.
Geotagged Longitude:	Longitude	Longitude of geotagged photo or object.
Geotagged Postal Code:	Postal Code	Postal code of geotagged photo or object.
Geotagged Region:	Region	Regional or State location of geotagged photo or object, such as NY, DC, IL, FL, and UT.
Geotagged Source:	Source	Source used to resolve geotagged GPS location to locality information.

Using Geolocation Column Templates

When using AD Forensics products, you can use the following Column Templates to help you quickly display Geolocation-based columns in the File List:

- *Geolocation* - Displays all available Geolocation columns.
- *GeoEXIF* - Displays all columns that contain EXIF-related Geolocation data.
- *GeoIP* - Displays all columns that contain IP-related Geolocation data.

Using Geolocation Facets

When using Summation, or Resolution1 products, you can also use facets to cull data based on Geolocation data.

See [Geolocation Facet Category](#) on page 47.

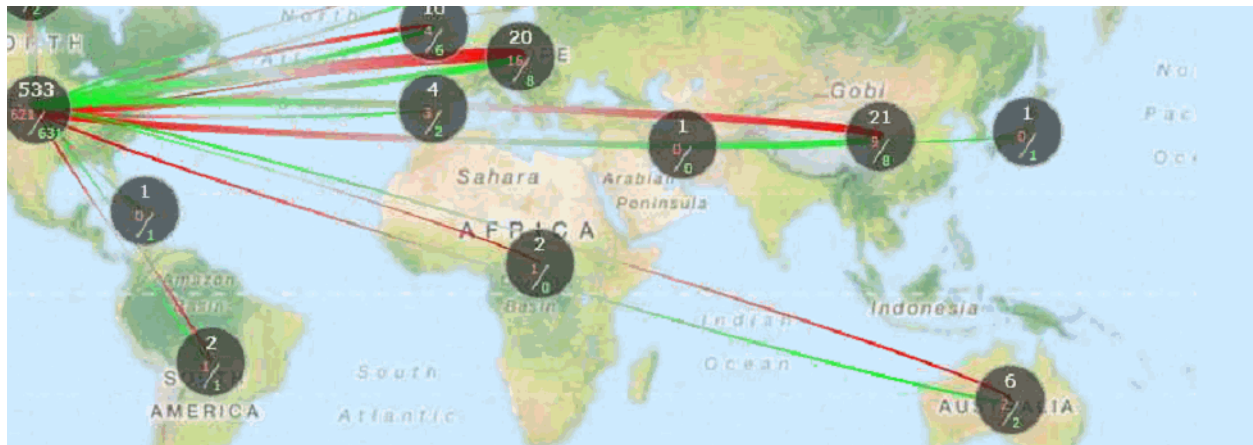
Using Geolocation Visualization to View Security Data

You can use geolocation to view IP location data to discover where in the world a computer is communicating. You can view IP locations data when using one of the following products:

- AD Resolution1 CyberSecurity and AD Resolution1 Platform, after running either a Volatile Job or a Network Acquisition Job
- AD Forensics products, after gathering Volatile data

The Geolocation view will display lines that trace internet traffic sent and received between IP addresses, indicating the physical location of all parties involved. You can drill into geographic regions to see multiple evidence items. You can then select specific data to post back to the case, where they can view information in the examiner or include it in reports.

Geolocation Panel - IP Locations To view IP data in Geolocation viewer



Note: For data collected by Geolocation Visualization, the *To Domain Name*, *To ISP*, *To Netspeed*, and *To Organization* columns do not populate in the *Item Grid*. If you require this data, you need to purchase a MaxMind Premier database license.

Prerequisites for Using Geolocation Visualization to View Security Data

- For FTK, Enterprise, AD Resolution1 Platform, and AD Resolution1 CyberSecurity:
 - For examining network acquisition and volatile data, enable the Geolocation option in the Web Config file. To enable this option, contact AccessData's support.
 - Also for examining network acquisition and volatile data, you need to generate a text file of your IP locations and place the text file in the GeoData directory. [Configuring the Geolocation Location Configuration File](#) (page 81)

Configuring the Geolocation Location Configuration File

When working with network acquisition and volatile data, some data may come from a private network where the physical location of the IP address is not known. For example, you may need to provide the location of your own network and any satellite offices that you interact with.

Normally you would start with block of IPs in your local network.

To set this information, you need to populate a configuration file for the KFF server.


The filename is `iplocations.txt`.

You can configure this file in one of two ways:

- Using the *Management* page > *System Configuration* > *Geolocation* page.
- Configuring the file manually

If you have already manually created this file, you will see the information in the configuration page interface.

Using the Geolocation Configuration Page

1. In the console, click *Management* > *System Configuration* > *Geolocation*
2. Click  to add an item.
3. Fill in the location data.

See sample data below. You can get latitude longitude data for an area from Google maps. Any data you save here is saved in the configuration file.

Important: Any time you save new data, the KFF Service is automatically restarted. This can affect running KFF jobs.

Configuring the Location Configuration File Manually

You can manually create and edit the `iplocations.txt` text file for the KFF server. It has the the following requirements:


- The text file needs to be saved with the filename `iplocations.txt`.
- The IP addresses must be written in CIDR format and need to be IPv4 addresses.
- Each comment line in the file must start with the character `#`. List only one address/network per line.
- The network line must contain the following information in the following order: address (in CIDR format), Id, CountryCode, CountryCode3, CountryName, Region, City, PostalCode, Latitude, Longitude, MetroCode, AreaCode, ContinentCode, Source.
- The `iplocations.txt` file must be placed in the **Geodata** folder of the **kffdata** folder on the server.

The following is an example of an `iplocations.txt` file:




```
#this file goes in the <kffdata>\GeoData directory
#address (in cidr
form),Id,CountryCode,CountryCode3,CountryName,Region,City,PostalCode,Longitude,
e,MetroCode,AreaCode,ContinentCode,Source
#192.168.0.0/24,1,,USA,United States,Utah,Taylorsville,84129,40.6677,-111.9388,,801,,
#10.10.200.252/30,1,,USA,United States,Utah,Orem,84042,40.2969,-111.6946,,801,NA,
#10.10.200.48/32,1,,USA,United States,Utah,Orem,84042,40.2969,-111.6946,,801,NA,
10.10.200.0/24,1,,USA,United States,Utah,Orem,84042,40.2969,-111.6946,,801,NA,
```

Viewing Geolocation IP Locations Data

To view IP location data in FTK

1. Open the *Examiner*.
2. Click the **Volatile** tab.
3. In the *Volatile* tab, click  (Geolocation).
4. You can filter the items displayed and see item details..
See [Using the Geolocation Grid](#) on page 78.

To view IP location data in Resolution1 CyberSecurity or Resolution1

1. Open **Project Review**.
2. In the *Item List* panel, click **Options > Visualization >**  **Geolocation**.
3. You can filter the items displayed and see item details..
See [Using the Geolocation Grid](#) on page 78.
For example, you can do the following:
 - You can click one or more pins and then click . This applies only the items you selected and displays them in the *Item List*. This displays any communication to or from those pins with any other location.
 - You can click one or more pins and then click . This applies only the items you selected and displays them in the *Item List*. This displays only the communication between the selected pins.
4. If you have both Network Communication and Exif pins in your data, you can select to turn on or off those pins in the map as well as items in the grid.
Click the “eye” icon for Network Communication or Exif.
If the icon is yellow, the data is displayed. If the icon is black, the data is not displayed.

Using the Geolocation Network Information Grid

- When viewing network acquisition and volatile data connection information, you can now view a grid that displays the following information:
 - Process Start Time
 - Machine
 - User Name
 - Process Name
 - Path
 - Host Name
 - IP Address
 - Coordinates
 - Ports

You can show the communication between multiple pins.

Geolocation Filter

You can filter your Geolocation data with filters in the Facets Panel. The following filters are available under the Geolocation filter categories for security jobs that contain geolocation data.

Geolocation Filters in the Facets Panel

Geolocation Filters	Description
From Country Name	Filters evidence by the country from which the communication originated.
To Country Name	Filters evidence by the country to which the communication was sent.
From City Name	Filters evidence by the city from which the communication originated. Example: San Francisco, San Jose, Los Angeles.
To City Name	Filters evidence by the city that the communication to which was sent. Example: San Francisco, San Jose, Los Angeles
From Continent	Filters evidence by the continent from which the communication originated.
To Continent	Filters evidence by the continent to which the communication was sent.

Geolocation IP Locations Columns

When using AD Resolution1 CyberSecurity and AD Resolution1, after running either a Volatile Job or a Network Acquisition Job, you can view IP location data using the following columns.

Geolocation Columns: IP Data

Column	Description
GeolocationFromAreaCode	The area code that the communication originated from. This is usually related to phone communication. Example: 415 is the area code for San Francisco.
GeolocationFromCity	The city that the communication originated from. Example: San Francisco, San Jose, Los Angeles.
GeolocationFromCountryCode	The numerical code of the country that the communication originated from. This is usually related to phone communication. Example: The United States's country code is 1, China's code is 86, and Australia's code is 61.
GeolocationFromDomainName	The identification string of a origin point of communication on the Internet. This can be to a website or the domain of a company. Example: Accessdata.com.
GeolocationFromISP	The Internet Service Provider that the communication originated from. Example: Comcast, AT&T, Time Warner Cable.
GeolocationFromLatitude	The exact numerical value of the North-South location on the globe that the communication originated from. Example: 37.783333 is the latitudinal value for San Francisco.
GeolocationFromLongitude	The exact numerical value of the East-West location on the globe that the communication originated from. Example: -122.416667 is the longitudinal value for San Francisco.
GeolocationFromMetroCode	The code assigned to a particular region. This code indicated the location in or near a large city where the communication originated from.
GeolocationFromNetspeed	The size of the connection, in bytes, that the communication originated from. Example: 5000 is 5000 bytes of data a second.
GeolocationFromOrganization	The place or group that the communication originated from. Example: AccessData.
GeolocationFromPostalCode	The code used for mailing identification of where the communication originated from. Example: 94127 is the postal code for San Francisco.
GeolocationFromRegion	The area from which the communication originated from. Example: Maidenhead's region is England, Tokyo's region is Tokyo.
GeolocationFromSource	The feed, or source from where the software obtained the information about the communication and the origin. Example: Sentinel or from a third-party source.
GeolocationToAreaCode	The area code that the communication is being sent to. This is usually related to phone communication. Example: 617 is the area code for Boston.
GeolocationToCity	The city that the communication was sent to. Example: Boston, Philadelphia, New York City.

Geolocation Columns: IP Data (Continued)

Column	Description
GeolocationToCountryCode	The numerical code of the country the communication is being sent to, usually related to phone communication. Example: The United States's country code is 1, China's code is 86, and Australia's code is 61.
GeolocationToLatitude	The exact numerical value of the North-South location on the globe of the communication's destination. Example: 42.358056 is the latitudinal value for Boston.
GeolocationToLongitude	The exact numerical value of the East-West location on the globe of the communication's destination. Example: -71.063611 is the longitudinal value for Boston.
GeolocationToMetroCode	The code assigned to a particular region. This code indicated the location in or near a large city where the communication was destined for.
GeolocationToPostalCode	The code used for mailing identification of where the communication was destined for. Example: 94127 is the postal code for San Francisco.
GeolocationToRegion	The area from which the communication was destined for. Example: Maidenhead's region is England, Tokyo's region is Tokyo.
GeolocationToSource	The feed, or source from where the software obtained the information about the communication and the destination. Example: Sentinel or from a third-party source.