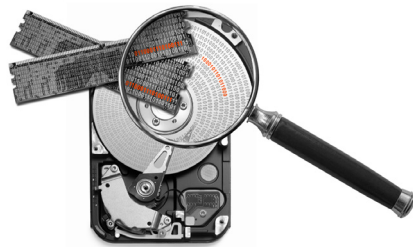


AccessData Registry Viewer



User Guide



AccessData[®]
A Pioneer in Digital Investigations Since 1987

AccessData Legal and Contact Information

Document date: March 4, 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.
588 W. 400 S.
Suite 350
Lindon, Utah 84042
U.S.A.
www.accessdata.com

AccessData Trademarks and Copyright Information

- AccessData® is a registered trademark of AccessData Group, Inc.
- AD InSight® is a registered trademark of AccessData Group, Inc.
- AD Summation is a registered trademark of AccessData Group, Inc.
- Distributed Network Attack® is a registered trademark of AccessData Group, Inc.
- DNA® is a registered trademark of AccessData Group, Inc.
- Forensic Toolkit® is a registered trademark of AccessData Group, Inc.
- FTK® is a registered trademark of AccessData Group, Inc.
- Password Recovery Toolkit® is a registered trademark of AccessData Group, Inc.
- PRTK® is a registered trademark of AccessData Group, Inc.
- Registry Viewer® is a registered trademark of AccessData Group, Inc.

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 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 MERCHANTABILITY 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. 588 W. 400 S. Suite 350 Lindon, UT 84042 USA <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 products.

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

AD Customer & Technical Support Contact Information

AD SUMMATION and 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 PRODUCTS	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, and Lab. They can help you resolve any questions or problems you may have regarding these products

Contact Information for Professional Services

Contact AccessData Professional Services in the following ways:

AccessData Professional Services Contact Information

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

Table of Contents

- AccessData Legal and Contact Information** 2
- Table of Contents** 7
- Chapter 1 Installing Registry Viewer** 8
 - Downloading the Installation File 8
 - Installing Registry Viewer 8
- Chapter 2 Using Registry Viewer** 9
 - About Registry Viewer 9
 - About Registry Viewer in Demonstration Mode 10
 - About the Windows Registry 11
 - Types of Windows Registry Files 11
 - Types of Registry Data 12
 - Opening and Closing Registry Files 13
 - Opening Registry Files from an Image File. 13
 - Searching 14
 - Using the Find Option 14
 - Using the Advanced Search Option. 14
 - Using the Full Registry View 17
 - Using the Common Areas View 17
 - Using the Reports View 18
 - Defining a Summary Report 20
 - Managing Summary Reports 22
 - Integrating Registry Viewer with Other AccessData Tools 24

Chapter 1 Installing Registry Viewer

This chapter explains how to install AccessData Registry Viewer.

Downloading the Installation File

The Registry Viewer installation file is included on the product discs. It is also located at <http://www.accessdata.com/support/product-downloads>.

To download the Registry Viewer install file

1. From the AccessData website, on the *Downloads* page, expand the *Registry Viewer* section.
2. Click **Registry Viewer x.x.x**.
3. Click **Download**.

Installing Registry Viewer

To install Registry Viewer

1. Browse to the installation file. It can be on the AccessData product disc, or on your hard drive in the download destination folder.
2. Run the file *AccessData Registry Viewer.exe*.
3. On the *Welcome* screen, click **Next**.
4. Read and accept the *License Agreement*.
5. Click **Next**.
6. You can accept the default destination folder, or you browse to another folder.
7. Click **Next**.
8. In the *Ready to Install* window, click **Install**.
9. In the *Completed* window, click **Finish**.

Chapter 2 Using Registry Viewer

About Registry Viewer

AccessData® Registry Viewer™ lets you view the contents of Windows® operating system registries. Unlike the Windows Registry Editor, which can only display the current computer's registry, Registry Viewer lets you view registry files from any computer.

Registry Viewer gives you access to a registry's protected storage. The protected storage can contain passwords, usernames, and other information that is not accessible in Windows Registry Editor.

Registry Viewer provides several tools for obtaining and reporting important registry information.

The *Full Registry* view shows all the contents of a registry file, while the *Common Areas* view displays sections of the registry that are most likely to contain significant data. From either view, you can select keys and subkeys to add to a report.

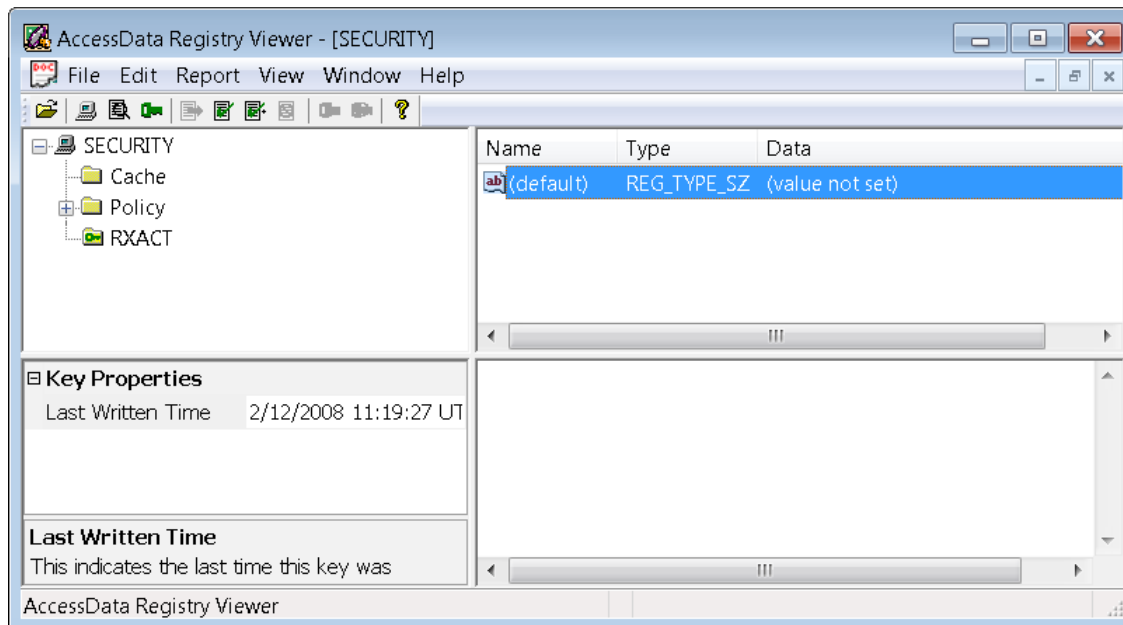
The *Report* view displays keys that you select. You can print only the relevant information.

All of the views also contain two detail panes: a *Key Properties* viewer and a hexadecimal viewer. The *Key Properties* viewer displays any property values that are associated with a key that you select. The hexadecimal viewer displays a value that you select in hexadecimal format.

When you open a registry file, a tree view is displayed in the left pane of the *Full Registry* view. The tree is organized in a hierarchical structure. It is similar in appearance to the folder and file structure of the Windows file system. Each registry entry is called a key. Keys are denoted by a folder icon. Some keys contain subkeys, which can also contain subkeys.

When you select a key, the top-right pane displays the key's values, or the information that is associated with that key. Each value displays a name, a data type, and a representation of the value's data. The data type tells you what kind of data the value contains as well as how it is represented. For example, values of the REG_BINARY type contain raw binary data and are displayed in hexadecimal format.

Registry Viewer



About Registry Viewer in Demonstration Mode

Registry Viewer requires a dongle to access all of its program features. Registry Viewer runs in Demonstration mode if a valid dongle is not installed.

In Demonstration mode, the following program features are disabled:

- Common Areas view
- Report view
- Generate Report function
- Decryption and interpretation of protected storage areas

Note: The dongle is checked at the program startup. If you insert or remove the dongle during a session, Registry Viewer does not switch from Demonstration mode to Full mode. You must restart Registry Viewer in order to switch between the Demonstration mode and the Full program modes.

About the Windows Registry

The Windows registry is a set of data files that the Windows operating system uses to control hardware, software, user information, and the overall functionality of the Windows interface. The files that make up the registry differ depending on the version of Windows. For forensic investigations, registry files are useful because they can contain the following information:

- The Usernames and passwords for programs, e-mail, and Internet sites.
- A history of the Internet sites that are visited, including the date and time for each.
- A record of the Internet queries done with Internet search engines such as Google™ or Yahoo®.
- A list of files that are recently accessed, such as documents and images.
- A list of all programs that are installed on the computer.

Types of Windows Registry Files

Registry Files for Windows

Version	File Name	Location	Contents
98/ME	system.dat	\Windows	Protected storage for all users on the computer. All installed programs, their settings, and any usernames and passwords associated with them System settings.
	user.dat	\Windows \Windows\profiles\user account	Most recently used (MRU) files.
2000/XP	ntuser.dat	\Documents and Settings\user account	Protected storage for the user. Most recently used (MRU) files. User preference settings.
	Default	\Winnt\system32\confi g	System settings.
	SAM	\Winnt\system32\confi g	User account management and security settings.
	Security	\Winnt\system32\confi g	Security settings.
	Software	\Winnt\system32\confi g	All installed programs, their settings, and any usernames and passwords associated with them.
	System	\Winnt\system32\confi g	System settings.

Types of Registry Data

Possible Data Types in the Registry

Data Type	Description
REG_BINARY	Raw binary data that is displayed in hexadecimal format. Most hardware component information is stored as binary data.
REG_DWORD	Data represented by a number that is four bytes long (a 32-bit integer). Many parameters for device drivers and services are this type, and are displayed in binary, hexadecimal, or decimal format. Related values are: <ul style="list-style-type: none">• DWORD_LITTLE_ENDIAN (the least significant byte is at the lowest address)• REG_DWORD_BIG_ENDIAN (the least significant byte is at the highest address)
REG_EXPAND_SZ	A variable-length data string. This data type includes variables that are resolved when a program or service uses the data.
REG_MULTI_SZ	A multiple string. Entries are separated by spaces, commas, or other marks. Values that contain lists or multiple values in a format that people can read are usually this type.
REG_SZ	A fixed-length text string.
REG_NONE	Data with no particular type. This data is written to the registry by the computer or application, and is displayed in hexadecimal format.
REG_LINK	A Unicode string naming a symbolic link.
REG_QWORD	Data represented by 64-bit integer.
REG_RESOURCE_LIST	A series of nested arrays designed to store a resource list used by a hardware device driver or one of the physical devices it controls. This data is detected by the computer and is displayed in hexadecimal format as a binary value.
REG_RESOURCE_REQUIREMENTS_LIST	A series of nested arrays designed to store a device driver's list of possible hardware resources it, or one of the physical devices it controls, can use. This data is detected by the computer and is displayed in hexadecimal format as a binary value.
REG_FULL_RESOURCE_DESCRIPTOR	A series of nested arrays designed to store a resource list used by a physical hardware device. This data is displayed in hexadecimal format as a binary value.

Opening and Closing Registry Files

You can only have one registry file open at a time in Registry Viewer. If you want to open another file, you must either close the current file or you can open another instance of Registry Viewer.

To open a registry file

1. Click **File > Open**.
2. In the *Open* dialog, locate and select the registry file that you want to view, and click **Open**.
You can also drag-and-drop a registry file into Registry Viewer to open it, or open a recently used file by selecting **File** and then the filename from the menu.
3. To close a registry file, click **File > Close**.

Opening Registry Files from an Image File

Image files are an exact, bit-by-bit copy of the contents of a device. Image files let you view registry files of a device without affecting the original contents. You can create an image, export it from the device, and analyze it on a separate computer.

Registry Viewer integrates with AccessData Forensic Toolkit (FTK). In FTK you can extract and open image registry files at the same time. FTK automatically identifies the registry files that are available within the image for selection to view.

Upon selection, FTK automatically creates a temporary registry file that you can then view in Registry Viewer; when you're finished, FTK deletes the temporary file. For more information, see *Integrating the Forensic Toolkit* or see the Forensic Toolkit documentation.

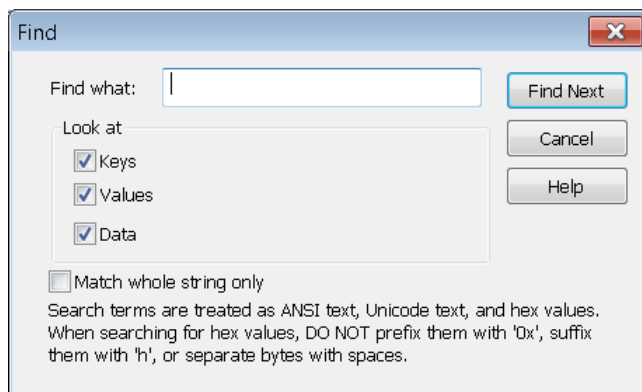
Searching

The Find option allows you to quickly search keys, values, and data for the next occurrence of a specified text string. Registry Viewer provides three ways to perform live searches for specific information in a registry file: a quick search, an advanced search, and a search by last written date.

Using the Find Option

Find searches only in the currently open view. If you want to search the entire registry file, you must search from the *Full Registry* view. Likewise, if you want to search only in common areas, you must search from the *Common Areas* view, and so forth.

Find Dialog



To use the Find option

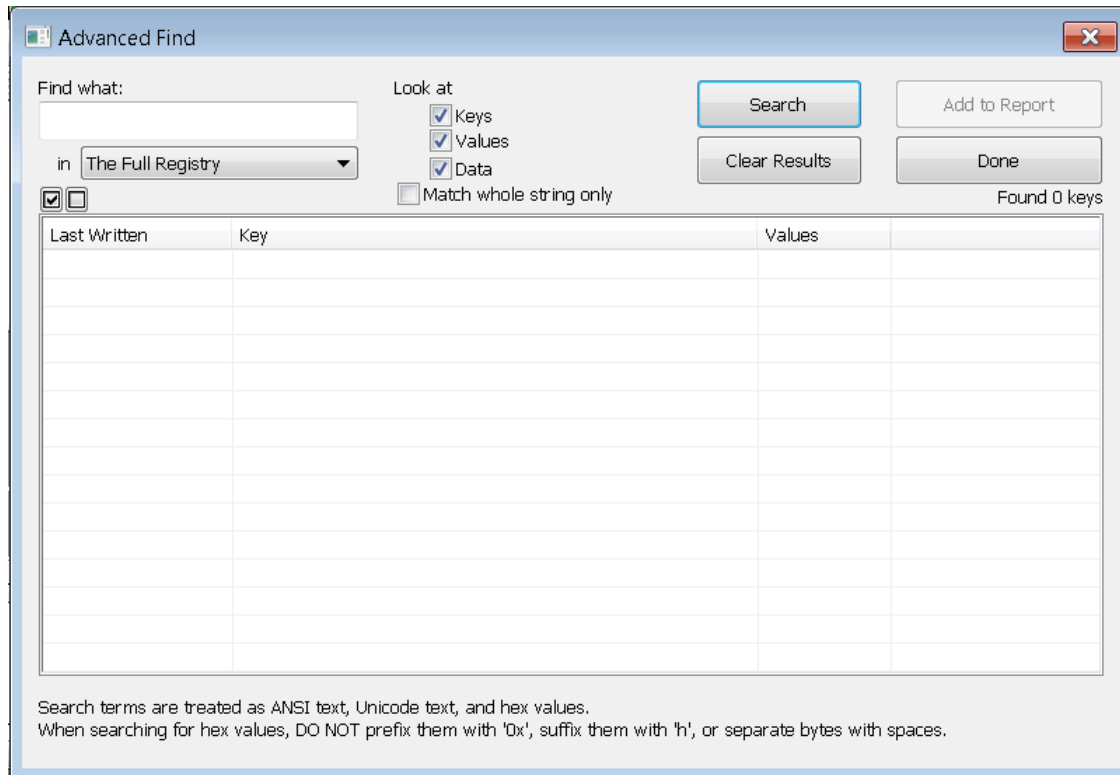
1. From the menu, select **Edit > Find**.
2. In the *Find What* field, enter the text string for which you want to search.
3. Select the registry file areas you want to search.
 - Mark the **Keys** check box to search for the specified string in all key names.
 - Mark the **Values** check box to search for the specified string in all value names.
 - Mark the **Data** check box to search for the specified string in all value data.
 - Mark the **Match Whole String Only** check box to find only data that matches the entire specified string.
4. Click **Find Next** to search for the specified string.

When Registry Viewer finds a match to the specified string, it expands the registry tree and highlights the key that contains the matching data.
5. To search for the next instance of the specified string, select **Edit > Find Next** from the menu, or press **F3**.

Using the Advanced Search Option

The *Advanced Find* option lets you search for and view all instances of a specific text string. You can also add the search results to the *Report* view.

Advanced Find Dialog



To use the Advanced Find Option

1. From the menu, select **Edit > Advanced Find**.
2. In the *Find What* field, enter the text string for which you want to search.
3. In the drop-down box, select the registry area you want to search: **Full Registry**, **Report Items**, or **Common Areas**.
4. Mark the registry file items you want to search:
 - Mark the **Keys** check box to search for the specified string in all key names.
 - Mark the **Values** check box to search for the specified string in all value names.
 - Mark the **Data** check box to search for the specified string in all value data.
5. Check **Match Whole String Only** to find only data that matches the entire specified string.
6. Click **Search** to look for all instances of the specified string.

Registry Viewer displays all keys that contain matching data in the results list. The total number of found keys is displayed at the upper-right corner of the list.
7. To add keys in the Results list to the Report view
 - 7a. Mark the check box next to the keys you want to add.
 - 7b. To check all listed keys, click the check mark button.
 - 7c. To uncheck all marked keys, click the empty button.
 - 7d. Click **Add to Report**.
 - 7e. The marked keys are added to the *Report* view at the root level.
 - 7f. Click **Clear Results** to clear all found keys from the *Results* list.
 - 7g. When finished, click **Done**.

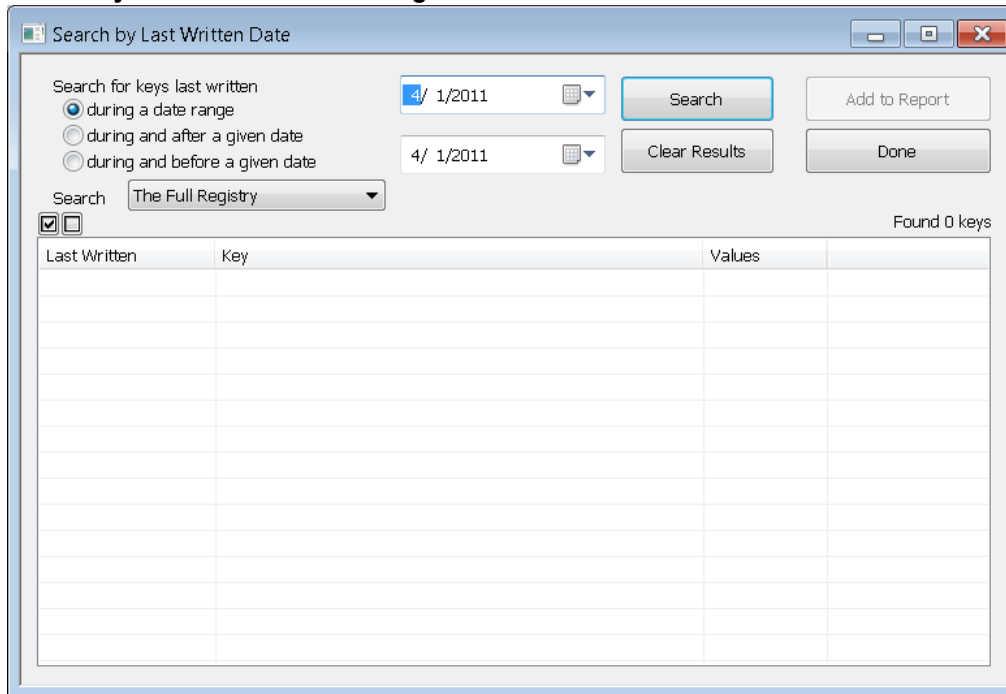
Using the Search by Date Option

The *Search by Date* option lets you search for keys based on the date they were last written to the registry file. You can add found keys to the *Report* view.

To use Search by Date to search for keys

1. From the menu, select **Edit > Search by Date**.

Search by Last Written Date Dialog



2. Select the date range you want to search.
 - Select **During a Date Range** to search for keys last written between two specified dates.
 - Select **During and After a Given Date** to search for keys last written on or after a specified date.
 - Select **During and Before a Given Date** to search for keys last written on or before a specified date.
3. In the **Search In** drop-down, select the registry area you want to search: **Full Registry**, **Report Items**, or **Common Areas**.
4. In the date fields, enter a date, or click the drop-down arrow to select a date from the pop-up calendar.
5. Click **Search** to look for all keys last written in the specified date range.

Registry Viewer displays all matching keys in the *Results* list. The total number of found keys is displayed at the upper-right corner of the list.
6. To add keys in the Results list to the Report view
 - 6a. Mark the check box next to the keys you want to add.
 - 6b. To check all listed keys, click the check mark button.
 - 6c. To uncheck all marked keys, click the empty button.
 - 6d. Click **Add to Report**.

The marked keys are added to the *Report* view at the root level.
 - 6e. Click **Clear Results** to clear all found keys from the *Results* list.
 - 6f. When finished, click **Done**.

Using the Full Registry View

The *Full Registry* view displays all the contents of the open registry file. A Windows registry is made up of multiple files. Because Registry Viewer opens one file at a time, it does not display the whole registry but only the information contained in the currently open file.

The *Full Registry* view is the default view when opening a file.

To open the Full Registry view

- ❖ Select **View > Full Registry** from the menu.

Using the Common Areas View

The *Common Areas* view helps you quickly access those areas of a registry file most likely to contain information important to you. Unlike the Full Registry view, which displays all the contents of a registry file, the *Common Areas* view shows only those keys, such as usernames, passwords, browser history, which you have marked in other registry files as forensically interesting.

Note: Registry viewer provides some customizable common areas by default.

Of course, the various files that make up a registry contain different information, so the keys and subkeys that appear in your *Common Areas* view depend upon whether they exist in the newer registry file as well.

To view the Common Areas

- ❖ Select **View > Common Areas** from the menu.

Adding Keys to the Common Areas View

Registry Viewer keeps track of each key you add, remembering them between registry files and sessions. Keys that have been added to the *Common Areas* view are identified by a folder icon overlaid by a green key .

To add a key to the Common Areas view

1. Select **View > Full Registry** from the menu.
2. In the registry tree, locate and select the key you want to add.
3. Select **Edit > Add to Common Areas**.

Removing Keys from the Common Areas View

Registry Viewer keeps track of each key you remove. The folder icon no longer appears next to the key.

To remove a key from the Common Areas view

1. In the *Common Areas* view, locate and select the key you want to remove.
2. From the menu, select **Edit > Remove from Common Areas**.

Using the Reports View

The *Report* view lists the keys you add to a report in the order you add them. You can reorder keys in the tree by dragging them up or down. You can also remove keys from the *Report* view. When you are finished, you can generate a report file containing all the selected keys and their associated information.




To view the Report view

- ❖ Select **View > Report Items** from the menu.

Adding Keys to the Report View

Keys added to the Report view are not saved between sessions or registry files. To save a record of this information, you must generate a report file or a summary report before closing the registry file or exiting Registry Viewer.

Keys that have been added to the Report view are identified by special folder icons in the registry tree:

- Keys added individually are denoted by: 
- Keys added with children are denoted by: 
- Keys added as children of a parent key are denoted by: 

To add a key to the Report view

1. Open the view that contains the keys you want to add.
 - To open the Full Registry, select **View > Full Registry** from the menu.
 - To open the Common Areas, select **View > Common Areas** from the menu.
2. In the registry tree, locate and select the key you want to add.
3. Add the key to the *Report* view by doing one of the following:
 - From the menu, select **Report > Add to Report**.
 - From the menu, select **Report > Add to Report with Children**.

Note: In the *Common Areas* view, if you select the **Common Areas** root item in the tree, this option becomes *Add Children to Report*. Each child key (with its subkeys) under the *Common Areas* root item is added individually to the *Report* view. Because each key is added at the main level of the *Report* tree, you can also remove individual keys. For more information on removing keys, see the following section “Removing Keys from the Report View.”

The selected key is added to the *Report* view at the root of the *Report* tree.

Removing Keys from the Report View

You can remove keys from the *Report* view. You can remove only keys at the main level of the *Report* tree. You cannot remove individual subkeys.

To remove a key from the Report view

1. In the *Report* view, *Full Registry* view, or *Common Areas* view, locate and select the key you want to remove.
2. From the menu, select **Report > Remove from Report**.
3. To remove all keys from the *Report* view, select **Report > Clear All Report Entries** from the menu.

Generating a Report

After you have finished adding keys to the *Report* view, you can generate a printable, HTML report file containing all the selected keys and their associated information.

To generate a report file

1. From the menu, select **Report > Generate Report**.
The *Create Report* dialog appears.
2. In the *Report Title* field, enter a title for the report.
3. In the *Report Location* field, enter the location where you want to save the report file or click **Browse** to navigate to the directory location. The default location for report files is `\AccessData\AccessData Registry Viewer\Report`.
4. In the *Report Filename* field, enter a filename for the report file.
5. The name of the current registry file is entered by default.
6. Mark the **Reduce Excess Data Output** check box to limit the data displayed for a value or string to the first 17 bytes.
7. In the generated report, you can view the additional data for a value or string by moving your cursor over the *Data* field. A pop-up displays the complete data.
8. Mark the **Also Show DWORD Values as Timestamps** check box to display timestamp equivalents for all DWORD values.
9. Timestamps are displayed in both UTC and local time formats.
10. Mark the **Show Key Properties Only** check box to include the items displayed in the *Key Properties* pane.
11. Mark the **View Report when Created** check box to automatically open the newly created report file (`Index.htm`) in your Internet browser.
12. Click **OK** to generate the report file.

If you integrate Registry Viewer with AccessData Forensic Toolkit (FTK), Registry Viewer uses the case report location defined in FTK as the default location for the generated report. For more information, see *Integrating the Forensic Toolkit* or see the *Forensic Toolkit manual*.

Generating a File-types Report

Registry Viewer lets you create a report that identifies all the file-type information stored in the currently open registry file. A file's type indicates what kind of information is stored in the file. Each file type is associated with one or more filename extensions (e.g., `.txt`, `.doc`, and `.htm`) and with the programs that can open those files.

To generate a file types report

1. From the menu, select **Report > Generate File Types Report**.
The *Create File Types Report* dialog appears.
2. In the *Report Title* field, enter a title for the report.

3. In the *Report Location* field, enter the location where you want to save the report file, or click **Browse** to navigate to the directory location. The default location for report files is \AccessData\AccessData Registry Viewer\Report.
4. In the *Report Filename* field, enter a filename for the report file. The name “<current registry file>-filetypes” is entered by default.
5. Mark the **View Report when Created** check box to automatically open the newly created report file (*.htm) in your Internet browser.
6. Click **OK** to generate the report file.

Defining a Summary Report

In addition to creating reports by adding keys to the *Report* view, Registry Viewer gives you the option to define summary reports. Summary reports differ from those created in the *Report* view in three important ways:

- You add individual key values to a summary report definition. Unlike the Report view in which adding a key automatically adds all the values contained in that key, a summary report definition allows you to select and add individual key values from any key in the registry file. Summary report definitions allow you to create reports that contain only those key values of forensic interest. You can also create multiple summary report definitions for the same registry file, each targeted to a different area of an investigation.
- You can group the added key values into user-defined sections. In a summary report definition, key values can be grouped in up to ten different sections. When the summary report is generated, grouped key values appear together under a specified section heading. You can use sections to combine information from different areas of a registry file. For example, you can group together all the key values containing information about a specific user (e.g., username, visited Internet Websites, and MRU lists).
- Summary report definitions are saved between registry files and sessions. Registry Viewer automatically saves the summary report definitions that you create. You can use these saved definitions again and again to generate summary reports from different registry files. The resulting reports contain the same key values, grouped in the same sections, but the actual information associated with those values is, of course, specific to each registry file.

To define a summary report

1. Open the view that contains the key values you want to add.
2. In the registry tree, locate and select the key that contains the values you want to add.
3. Do one of the following:
 - Select **Report > Define Summary Report**.
 - Right-click the key and select **Define Summary Report** from the quick menu.The *Define Summary Report* dialog opens.
4. In the *Summary Report Title* field, enter a name for the summary report definition. The name of the selected key is entered by default.

The *Summary Report Title* appears in the *Summary Reports* dialog and is also the filename for all reports generated with this definition. Be sure to choose a descriptive, easily identifiable name.
5. Define wildcard keys, if needed.

Note: A wildcard key allows you to add key values to the summary report definition for keys that may exist in the current registry file. There are two types of wildcard keys: a wildcard that finds the specified key values in any of the direct subkeys of a selected parent key, and a wildcard that finds the specified key values in the selected key and any of its descendants. For more information, see [Adding Wildcard Keys to a Summary Report \(page 21\)](#).

6. In the *Summary Key* registry tree, locate and select a key that contains key values you want to add. The key's values are displayed in the *Available Items* list.

7. If you want to group added key values into sections:
 - 7a. Select the appropriate section number (1–10) from the drop-down list. You must define sections sequentially (i.e., define section 1 first, then section 2, and so forth).
 - 7b. In the *Section Title* field, enter a name for the section. This is the name that appears as the section heading in a generated report, so be sure to choose a descriptive name.
8. Add specific key values to the summary report definition by doing any of the following:
 - Select a key value in the *Available Items* list and click **Add Value**.
 - Press the **Ctrl** button and click to select multiple key values. Click **Add Value** to add all the selected values to the report definition.
 - To add all the key values in the *Available Items* list, click **Select All > Add Value**. The key values appear in the *Included Items* list.
9. Select **Match any item >Add Value** to add a key-value wildcard to the summary report definition. A key-value wildcard reports all values for the selected key, even if those values change in name or number between registry files. For example, you can use a key-value wildcard to return all the values in the MUICache key, even though the number and names of those key values (program paths, links, etc.) are unique to each registry file.
10. Click **Add Unlisted Value** to specify a value for the selected key that is not available in the current registry file.
11. In the *Add an Unlisted Value* dialog, enter the name of the key value and then click **OK** to add it to the summary report definition. For example, if you know that a software key often contains a Version value, but that value is not present in the current registry file, you can still add it to the summary report definition using the Add Unlisted Value option. If you then use the summary definition to create reports from other registry files, the Version value is reported whenever it is present.
12. To remove key values from the *Included Items* list, do one of the following:
 - Select a key value and click **Remove Value**.
 - Click **Remove All** to remove all key values in the list.
13. Click **Preview Report** to generate and view a printable HTML report file from the summary report definition. Preview reports are temporary: they are deleted from memory when you close the browser window.
14. To generate a saved report, you must save the summary report definition and then generate the report from the *Managing Summary Reports* dialog.
15. When finished, click **Save and Close** to save the summary report definition, and to exit the dialog.

After you have created a summary report definition, you can use the *Manage Summary Reports* feature to generate and view additional summary report files.

Adding Wildcard Keys to a Summary Report

When you define a summary report, you add values from specific keys. Because each key has a set name and registry path, Registry Viewer can locate those keys in any registry file, and include their values in the generated report. Some keys, however, have names that change among registry files.

For example, registry files often include username keys, where the name of each key is the name of a user with an account on that computer. Because a username key is unique to a specific file, Registry Viewer cannot use its name and registry path to locate similar keys in other registry files.

A wildcard key allows you to select and include key values from the subkeys under a selected parent key, even though the number and names of those subkeys change from registry file to registry file. Using a wildcard key allows you to include username key values in a summary report definition.

When you add a wildcard key, you select a parent key that contains the subkeys you want to include in the report. You can then add specific key values from these subkeys (or children) to the summary report definition. Each value needs to be added only once for all the subkeys. When you generate the summary report, Registry Viewer uses the parent key's name and registry path to locate all of its subkeys, and display the selected key value information for each one.

For example, you may want to a summary report to include password and login key values for each username key in a registry file. In the current file, there are two username keys, peter1 and paul2. Both are children of Users key. To set the wildcard key, you select the Users key as the parent key. You then select the peter1 subkey and add its password and login key values to the definition. When you generate the summary report, Registry Viewer first lists the password and login key value information for peter1, then the password and login information for paul2.

Suppose you then use the summary report definition to create a report from a different registry file. In this file, the Users key contains three children: mary1, mary2 and mary3. The generated report lists the password and login information for mary1, followed by the password and login information for mary2, then mary3. If mary3 doesn't have a defined password, "This summary report item does not exist in the current registry file" displays for that value.

To add a wildcard key to a summary report definition

1. In the *Summary Key* registry tree, locate and select the parent key of the subkeys you want to include in the report.
2. In the *Wildcard Key* definition box, select the type of wildcard key you want to add:
 - *Match All Immediate Children* finds the specified key values in the direct subkeys of only the selected parent key.
 - *Match the Entire Subtree* finds the specified key values in the selected parent key and any of its descendants.
3. Click **Use Currently Selected Key**.
The full registry path of the parent key appears in the *Wildcard Key* field.

Managing Summary Reports

After you have created a summary report definition, you can use the Manage Summary Reports feature to preview and generate a printable HTML report file containing the summary report's selected key values and associated information. You can also edit or delete existing summary report definitions.

To manage summary report definitions

- ❖ Select **Report > Manage Summary Reports** from the menu.
The *Summary Reports* dialog lists the available summary report definitions.

Previewing a Summary Report

When you preview a summary report, Registry Viewer generates a temporary report using the information in the currently open registry file and then displays it in Internet Explorer. Preview reports are not saved; they are deleted from memory when you close the browser window.

To preview a summary report

1. In the *Available Summary Reports* list, select the report definition.
2. Mark the **Reduce Excess Data Output** check box to limit the data displayed for a value or string to the first 17 bytes. In the generated report, you can view the additional data for a value or string by moving your cursor over the Data field. A pop-up displays the complete data.
3. Mark the **Also Show DWORD Values as Timestamps** check box to display timestamp equivalents for all DWORD values. Timestamps are displayed in both UTC and local time formats.
4. Click **Preview**.
Registry Viewer asks if you want to include Empty Values in this report.
 - Click **Yes** to include all defined key values, even if they contain no data.
 - Click **No** to include only those key values that contain data.
5. Registry Viewer opens the summary report file in Internet Explorer.

Generating a Summary Report

When you generate a summary report, Registry Viewer uses the selected report definition to extract the specified key values from the currently open registry file. The resulting report is then saved.

To generate a summary report

1. In the *Available Summary Reports* list, select the report definition.
2. Mark the **Reduce Excess Data Output** check box to limit the data displayed for a value or string to the first 17 bytes. In the generated report, you can view the additional data for a value or string by moving your cursor over the Data field. A pop-up displays the complete data.
3. Mark the **Also Show DWORD Values as Timestamps** check box to display timestamp equivalents for all DWORD values. Timestamps are displayed in both UTC and local time formats.
4. Click **Generate** to make the HTML report file. Registry Viewer asks if you want to include Empty Values in this report.
 - Click **Yes** to include all defined key values, even if they contain no data.
 - Click **No** to include only those key values that contain data. The generated file is automatically saved in the `\AccessData\AccessData Registry Viewer\Reports` folder. A time and date stamp is added to the filename for easy identification.
5. After the report generates successfully, click **OK**.
6. To view a generated report, select **Report > View Existing Reports** from the menu.

Editing a Summary Report Definition

Registry Viewer allows you to edit previously created summary report definitions.

To edit a summary report definition

1. In the *Available Summary Reports* list, select the report definition.
2. Click **Edit**.
The *Define Summary Report* dialog opens.
3. Edit the summary report definition as needed.
4. Click **Save and Close** to save your changes. Changes made to a summary report definition are permanent and affect all subsequent reports generated from that definition.

Deleting a Summary Report Definition

Registry Viewer lets you delete previously created summary report definitions. Deleting a report definition does not delete any summary report files generated from that definition.

To delete a summary report definition

1. In the *Available Summary Reports* list, select the report definition.
2. Click **Delete**.
Registry Viewer asks if you want to permanently delete the summary report definition.
3. Click **Yes** to delete the definition.

Integrating Registry Viewer with Other AccessData Tools

AccessData forensic tools generate lists of words from the drive images taken. These word lists are then used to attack passwords and open locked files and computers. Much of the functionality of these tools overlaps, and understanding how the programs work together will help you apply them to your cases.

The AccessData Forensic Toolkit (FTK) indexes drive image files from which you can create your wordlists. This index includes all non-encrypted data in registry files such as the System Software and the unencrypted portions of the ntuser.dat file. By itself, FTK can't index encrypted portions of registry files such as the Protected Storage area of the registry files desired. FTK utilizes Registry Viewer to decrypt and obtain word lists from these files. Registry Viewer can also create an individual word list from a single registry file.

Use FTK to create your initial indexes and word lists. Use Registry Viewer to access the encrypted areas of ntuser.dat, then add Registry Viewer's word list to the larger FTK word lists. One large, comprehensive word list will be easier to manage, and more efficient to apply to your case.

Integrating Registry Viewer with the Forensic Toolkit (FTK)

Integrating Registry Viewer with FTK allows you to seamlessly view registry files and create registry reports from within FTK. Any created reports are saved by default in the current FTK case report location.

Integration also allows you to extract and open registry files on the fly from hard drive images. FTK automatically creates a temporary registry file from the image and opens it in Registry Viewer; after you're finished, FTK deletes the temporary file.

To run Registry Viewer from FTK

1. In FTK, open an existing case by selecting **File > Open Case**.
2. If you have chosen to always display the FTK Startup screen, select **Open an Existing Case** and then click **OK**.
3. Select the case you want to open.
4. Select **File > Registry Viewer**.
5. Select the registry file you want to view and then click **View File**.
6. If you have located registry files in the case in FTK, you can right-click on a file and then select **View in Registry Viewer**.
Registry Viewer automatically launches.

Updating Index.htm

Registry Viewer generates a list of the reports named Index.htm used for reference by the Forensic Toolkit. This list is updated every time you create new report, but must be manually updated when you remove reports from the Report folder.

To manually regenerate the Index.htm

1. Activate the *Report* menu by opening a file in Registry Viewer.
2. From the main menu, select **Report > Regenerate Index.htm** to update the list of reports currently in your *Report* folder.

Exporting a Word List

If you are using PRTK, you can export the case index to use as a dictionary in the password recovery process.

To export the word list

1. Select **Tools > Export Word List**.
2. Select the file and location to which you want to write the word list. The default filename is case_name.txt.
3. To add registry files, click **Add Files** and then select the registry files to add to the word list.
4. Click **Save**. For more information, see the AccessData Forensic Toolkit User Guide.

Integrating Registry Viewer with the Password Recovery Toolkit (PRTK)

Registry Viewer lets you create and export a word list containing all the strings in a registry file. The word list can then be used in AccessData® Password Recovery Toolkit™ (PRTK™) as a dictionary for decoding passwords and pass-phrases.

Exporting a Word List

When you export a word list, Registry Viewer searches the registry file for key values that are stored as strings. Each string it finds is exported into a text file as a separate line. The resulting file contains a list of every string value in the registry. If you save or copy the word list file into the PRTK Dictionary folder (i.e., \AccessData\PRTK6\Dictionaries), PRTK can access the file as a user-defined dictionary. PRTK uses each line in the file as a possible password or pass-phrase in a password recovery operation.

To export a word list

1. From the menu, select **Report > Export Word List**.
The *Generate Word List* dialog appears.
2. Navigate to the directory location where you want to save the word list file. The default path for word list files is \AccessData\AccessData Registry Viewer.
3. In the *Filename* field, enter a name for the word list file. The file (*.txt) is saved in plain-text format.
4. Click **Save** to export the word list.
For more information on PRTK user dictionaries or on password recovery, see the AccessData Password Recovery Toolkit User Guide.