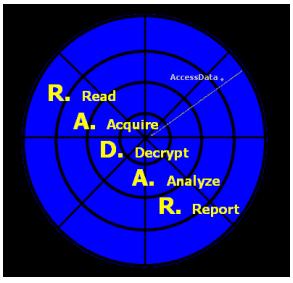
Registry Viewer

Sales and Promotional Summary



ACCESSDATA, ON YOUR RADAR

What is AccessData's Registry Viewer®?

Registry Viewer allows you to view the contents of Windows® operating system registries. Unlike the Windows Registry Editor®, which displays only the current system's registry, Registry Viewer lets you view registry files from any Windows system. Registry Viewer also provides access to a registry's encrypted protected storage, which contains passwords, usernames, and other information not accessible in Windows Registry Editor.

We'll Help Your Investigation

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

A Full Registry view shows all the contents of a registry file, while a Common Areas view displays only those sections of the registry most likely to contain significant data. From either view, you can select keys and subkeys to add to a report. A Report view displays the selected keys, allowing you to print only relevant information.

All views also contain two detail panes: a Key Properties viewer and a Hexadecimal viewer. The Key Properties viewer displays any property values associated with a selected key, while the hex viewer displays a selected value in hexadecimal format.

Registry Viewing Basics

The Registry Viewer provides access to the encrypted "Protected Storage System Provider" key, which potentially contains Form Data from Internet data entries, Microsoft Outlook and Outlook Express Passwords, Web site logon stored passwords, and search queries from Google, Yahoo, and potentially more.

The Windows registry is a set of data files that allows the Windows operating system to control hardware, software, user information, and the overall functionality of the Windows interface. For forensic work, registry files are particularly useful because they can contain the following important information:

- Usernames and passwords for programs, e-mail, and Internet sites
- A most recently used list of Internet sites visited
- A most recently used list of documents opened and accessed
- A record of Internet queries (i.e., searches performed on Internet search engines like Google*, Yahoo*, etc.)
- User logon info including last logged time
- System information including USB identification
- Possible identifying information of user and current operating system
- A list of all programs installed on the system

The files that make up the registry differ depending on the version of Windows. The tables below list the registry files for each version of Windows, along with their locations and the information they contain.

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

When you open one of these files in Registry Viewer, a registry tree appears in the left pane of the Full Registry view. The tree is organized in a hierarchical structure, similar in appearance to the folder and file structure of the Windows file system. Each registry entry, denoted by a folder icon, is called a key. Some keys contain subkeys, which may in turn contain other subkeys.

When you select a key, the top-right pane displays the key's values or the information associated with that key. Each value has a name and data type, followed by 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.

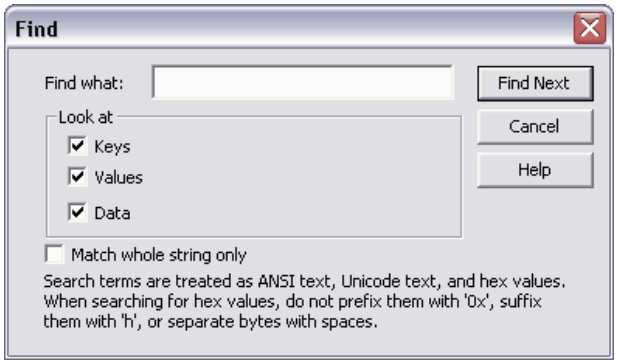
The following table lists the possible data types:

Data Type	Description
REG_BINARY	Raw binary data 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: • 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 system 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 system and is displayed in hexadecimal format as a binary value.
REG_RESOURCE_REQUIREMENTS_LIST	A series of nested arrays designed to store a

Data Type	Description
	device driver's list of possible hardware recourses it, or one of the physical devices it controls, can use. This data is detected by the system 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.

Searching

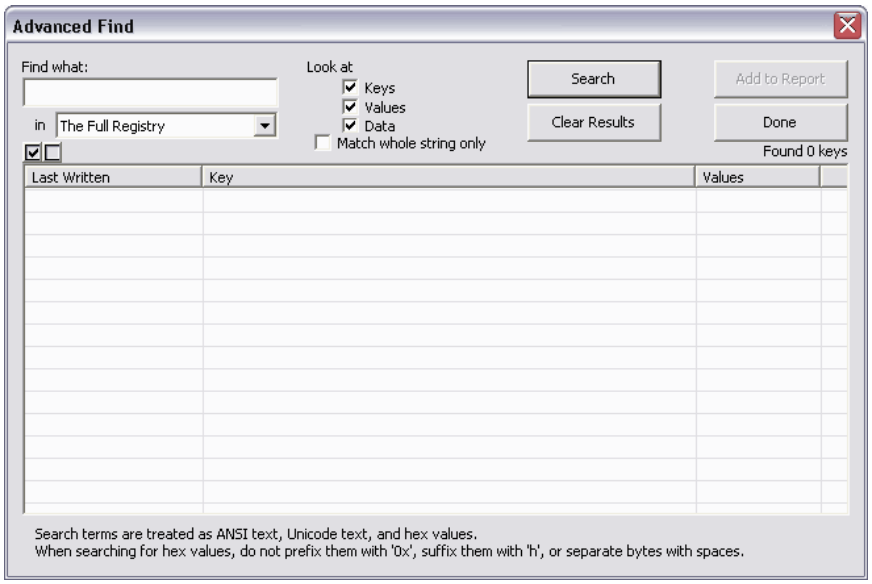
The Find option allows you to quickly search keys, values, and data for the next occurrence of a specified text string. Registry Viewer provides three ways to perform live searches for specific information in a registry file: a regular search, an advanced search, and a search by last written date.



Advanced Find

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.

Important: When you click on a hit, Registry Viewer will go to that key automatically.



Search by Date

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.

Reporting

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.

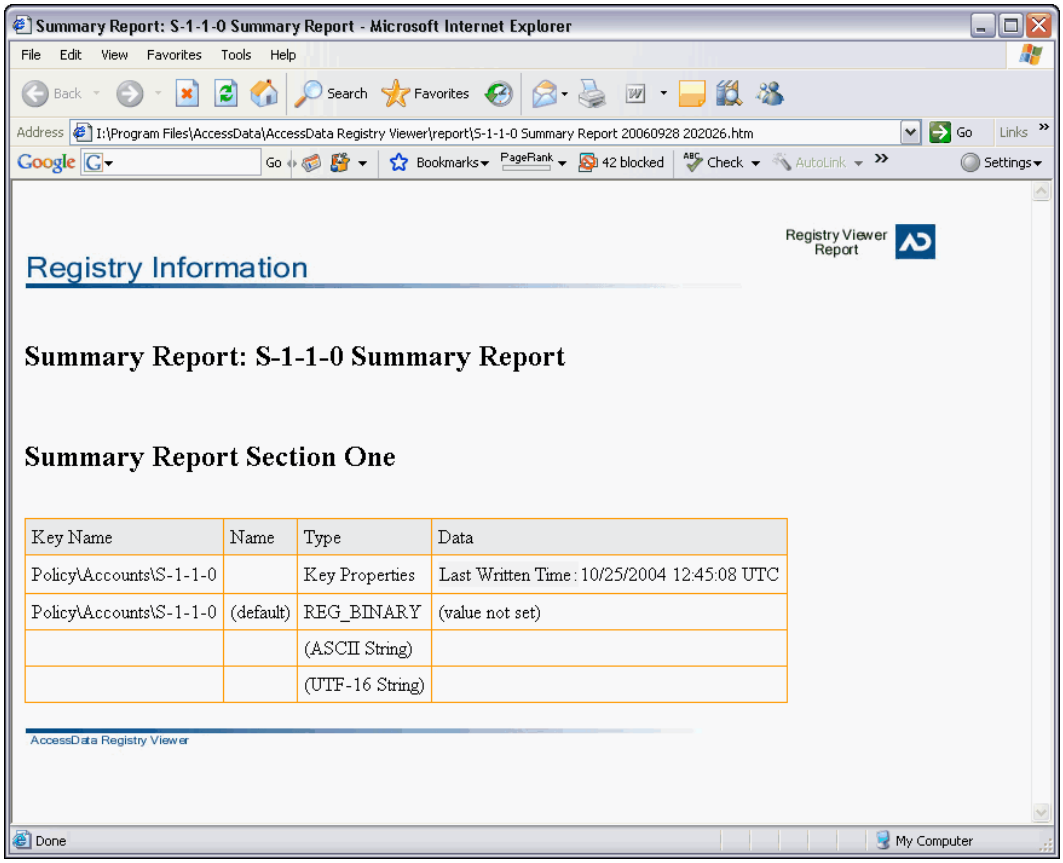
Registry Viewer also lets you create a report that identifies all the file-type information stored in the currently open registry file. A file's type indicates what kind of information is stored in the file. Each file type is associated with one or more filename extensions (e.g., .txt, .doc, and .htm)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

Summary Reports

Once you create a report, for example, a report that lists all users in the SAM file, that report becomes a template that can be run against any other SAM file to automatically report all users

Integrating Registry Viewer with Other AccessData Products

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 PRTK as a dictionary for decoding passwords and pass phrases.



Password Decryption Dictionaries

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. Registry Viewer can then easily generate a password list from its own full text index for use with PRTK. If you save or copy the word list file into the PRTK dictionary folder (\AccessData\Dictionaries), You can import this dictionary into PRTK. PRTK will add it to its list of available user-defined dictionaries. This can also be done from FTK as well. PRTK can then use each line in the file as a possible password or pass phrase in a password recovery operation.

Case Reports

Registry Viewer reports easily integrate with FTK case reports. Starting Registry Viewer from FTK will automatically display all registry files in the case to include in your FTK report. You don't have to "drill down" to each file individually, or have to remember where each piece of evidence is stored.

In Conclusion

Registry Viewer allows you full access to a user's registry files without having to mount all of the necessary files in a Windows Environment. This is a huge advantage to the investigator because it allows the ability to drill quickly into the registry to save time.

Contact Us

Sales
384 South 400 West
Suite 200
Lindon, UT 84042
USA

sales@accessdata.com
800.574.5199