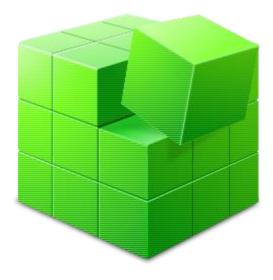
Registry Explorer User Guide



Registry Explorer RECmd

Eric R. Zimmerman saericzimmerman@gmail.com 501-313-3778

Page 1 of 81 Last revised: 5/19/2017 8:36:46 AM

Revision history

- 07/01/2015 Rev. 1 Initial release
- 06/08/2016 Rev. 2 Updated for v0.8.1.0
- 05/19/2017 Rev. 3 Updated for v0.9.0.0

Table of Contents

Requirements	5
Why another Registry tool?	5
Registry Explorer	5
Getting started	6
Interface sections	7
Registry hives	7
Available bookmarks	7
Values	7
Value details	7
Status bars	7
Main menu	
File	
Tools	
Options	
Bookmarks	
View	
Help	
Using Registry Explorer	20
General concepts	
Loading hives	
Key context menu	27
Value context menu	
Value details	
Data interpreter	
Interacting with deleted keys	
Creating bookmarks	
Managing bookmarks	
Available bookmarks	
Searching	
Technical details in depth	54
Plugins	

	Registry Explorer User Guide
RECmd	
Getting started	
General	
Query	
Search	
Version changes	
Version 0.9.0.0	
Version 0.8.1.0	
Version 0.7.1.0	
RECmd changes	
Registry Explorer changes	
Version 0.7.0.0	
RECmd changes	
Registry Explorer changes	
Version 0.2.0.0	
Version 0.1.8.0	
Appendix A – Contributors	
Appendix B – Additional resources	

Requirements

Registry Explorer and RECmd require Microsoft .net framework version 4.6 full runtime or greater to be installed. It is available at <u>https://www.microsoft.com/en-us/download/details.aspx?id=49982</u>.

Why another Registry tool?

The need for Registry Explorer and RECmd rose out of writing a fully managed offline Registry hive parser in C#. Existing parsers did not offer the features I was looking for and as such, research and coding began. The Registry <u>project</u> serves as the basis for several programs including ShellBags Explorer, AppCompatParser, etc. Once the back end was mature, I wanted an easy to use and powerful way to expose the capabilities of the parser.

Registry Explorer fills the gaps in existing tools and expands the capabilities of Registry viewers in many unique and powerful ways. It is GUI based and contains powerful searching, filtering, and other visualization concepts that makes exploring Registry hives very easy while exposing all of the technical information contained in Registry hives.

RECmd was created in order to be able to script access to Registry hives, conduct new research, and automate searching across multiple Registry hives at once from the command line.

Because both tools use the same back end, both have the same searching and viewing capabilities including the full recovery of deleted keys and values. The parser also exposes value slack.

In summary, the capabilities of Registry Explorer and RECmd allows for quickly examining multiple hives at once and they can be leveraged to find new places where currently understood data is located in an easy to use and systematic way. It can be used in educational settings to not only understand the Registry from a functional level, but also from a deeply technical perspective.

Registry Explorer

Registry Explorer is a GUI based tool used to view the contents of offline Registry Hives. It has the ability to load multiple hives at once, search across all loaded hives using strings or regular expressions, exporting of data, and much more.

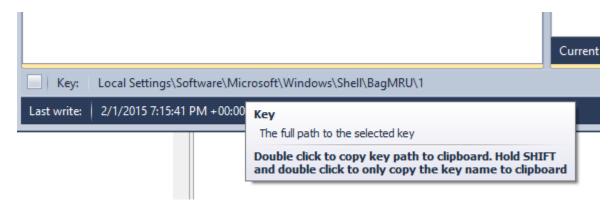
Getting started

After starting Registry Explorer, the main interface is displayed.

Registry Explorer v0.0.4.7				
File Tools Options Bookmarks (0/0) View Help				
Registry hives (0) Available bookmarks (0/0)		Values		
Key name	# values Last write	Drag a column header here to group by that column		
		Value name 🔺 Value type Data Value slack		
		P		
Hives, keys, and subke are displayed here	ys	Values for selected key are displayed here		
		Value details for the selected value are displayed here		
Key: None		Value: None Collapse all hives		
Last write: None Load hives via File menu or drag and	l drop anywhere above	Hidden keys: 0 1		

Settings for various things like program options, window size, slider positions, window positions, recent searches, etc. are all saved and reloaded between program executions. You can reset these options by deleting the relevant files under the Settings directory in the main Registry Explorer folder. The .layout files are for the trees and grids.

Tooltips are shown when hovering over different areas of the program. For example, hovering over the Key section of the status bar shows the following:



Interface sections

There are five sections to the main interface.

Registry hives

On the left side of the window is the Registry hives tab. This tab displays the Registry hives that have been loaded and the keys contained therein. Once at least one hive is loaded and a key is selected, a context menu is available by right clicking on a key. The context menu options will be discussed below in the <u>Key context menu</u> section.

Available bookmarks

Next to the Registry hives tab is the Available bookmarks tab. This tab will be discussed in detail below.

Values

The Values grid shows all of the values contained in the key that is selected in the Registry hives tab. Once a value is selected, a context menu is available by right clicking on a value. The context menu options will be discussed <u>below</u>.

Value details

The Value details area contains one or more tabs that dynamically adjust depending the type of value selected. In every case, a type viewer will be displayed that shows the value of the selected key. If a value has slack, a separate tab will be shown that allows you to view the slack space in a hex viewer.

These concepts will be explained in more detail in the <u>Using Registry Explorer</u> section below.

Status bars

Across the bottom of the interface are several status bars as seen below.

Key: None	Value:	None Collapse all hives
Last write: None	Load hives via File menu or drag and drop anywhere above	Hidden keys: 0 1

Top status bar

The top status bar contains details about the path to the selected key and the selected value. On the far left is a check box that toggles whether to show the root key name in the key path. By default, the root key path is not shown. The screen shot below shows what this option does when turned on and off.

Key:	Local Settings\Software\Microsoft\Windows\Shell\BagMRU	Value: 0 Collapse all hives	
✓ Key:	S-1-5-21-146151751-63468248-1215037915-1000_Classes\Local Settings\Software\Microso	oft\Windows\Shell\BagMRU Value: 0 Collapse all	hives

By hiding the root key name, longer key paths will not be truncated as different keys are selected.

To the far right of the top status bar is a button that, when clicked, will collapse all loaded hives back to their default state. This is a handy shortcut to clean up the Registry hives tree after interacting with it and expanding many keys and subkeys.

Double clicking the key path will copy the key path to the clipboard. Holding **Shift** and double clicking will copy only the key name to the clipboard.

Page 7 of 81 Last revised: 5/19/2017 8:36:46 AM Double clicking the value will copy the value's name to the clipboard. Holding **Shift** and double clicking will copy the value's data to the clipboard.

Bottom status bar

The bottom status bar contains the last write timestamp, the status of filters for values, a section for general status messages, an indicator of the total number of keys that are hidden from view, and the total number of messages available on the Messages form.

Double clicking on the Total messages counter will show the Messages form. If there are any errors in the Messages form, the background will be changed to yellow. If there are any errors, the background will be changed to red. When the Messages tab is viewed, the background color will be changed back to its default.

Double clicking the last write timestamp will copy it to the clipboard.

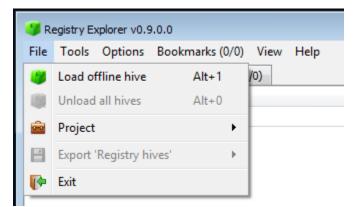
Main menu

The main menu contains options that allows for loading hives, searching hives, opening bookmarks, and so on. In many cases, the menu items will have shortcut keys associated with them. Pressing the keys shown by a menu item on the keyboard will activate that menu item.

The various sections below will explain these submenus. Where things are obvious (like File | Exit), no additional information will be provided.

File

The File menu contains options for loading hives (you can also simply drag and drop one or more hives onto the main interface to load them) and exporting.



- Load offline hive: Allows for loading one or more hives. To select more than one file, select a file, then hold Shift and select the last file to load. You can also hold Ctrl and click files to select them individually.
- Unload all hives: Unloads all hives at once vs. removing one at a time
- **Project:** Allows for loading/saving of projects. Projects will be discussed below.
- **Export 'Registry hives':** Exports what is shown in the Registry hives tab to a variety of formats. As an example, if the Registry hives tree looked like this:

Registry Explorer v0.9.0.0

<u>File Tools Options Bookmarks (33/2) View H</u>elp

Registry hives (1) Available bookmarks (33/2)

	Key name	# values	# subkeys	Last write timestamp
Ŷ	R D C	=	=	=
	⊿ 🥮 D:\Sync\RegistryHives\NTUSER.DAT			2013-08-22 13:25:4
	⊿ 🚞 CsiTool-CreateHive-{00000000-0000-0000-0000-000000000	0	12	2014-11-28 16:52:1
	AppEvents	0	2	2014-05-20 14:19:3
	AppLifeUpdateShortcuts	1	0	2014-05-20 18:43:0
	a 🚞 Console	39	3	2014-10-15 20:28:3
	%SystemRoot%_system32_cmd.exe	3	0	2014-10-15 20:28:2
	%SystemRoot%_System32_WindowsPowerShell_v1.0	10	0	2014-05-20 14:19:3
	%SystemRoot%_SysWOW64_WindowsPowerShell_v1	10	0	2014-05-20 14:19:3
	Control Panel	0	14	2014-11-06 16:24:5
	Environment	3	0	2014-06-27 19:12:1
۲	D EUDC	0	4	2014-05-20 14:19:3
	Identities	0	1	2014-05-20 18:43:1
	Keyboard Layout	0	3	2014-05-20 14:19:4
	⊿ 💳 Network	0	1	2014-10-24 15:17:4
	r Y	6	0	2014-11-06 17:17:1
	Printers	0	4	2014-10-10 20:42:5
	Software	0	79	2014-12-08 13:51:2
	▷ 💳 System	0	1	2014-05-20 14:19:3
	Associated deleted records	0	0	
	Unassociated deleted records	0	0	

Exporting to PDF would generate a PDF file that contains the following:

Key name	# values	# subkeys	Last write timestamp
U:\Sync\RegistryHives\NTUSER.DAT			2013-08-22 13:25:44
CsiTool-CreateHive-{0000000-0000-0000-0000-000000000000}}	0	12	2014-11-28 16:52:17
田	0	2	2014-05-20 14:19:35
AppLifeUpdateShortcuts	1	0	2014-05-20 18:43:07
Console	39	3	2014-10-15 20:28:31
SystemRoot%_system32_cmd.exe	3	0	2014-10-15 20:28:23
SystemRoot%_System32_WindowsPowerShell_v1.0_power	10	0	2014-05-20 14:19:35
SystemRoot%_SysWOW64_WindowsPowerShell_v1.0_pow	10	0	2014-05-20 14:19:35
田 Control Panel	0	14	2014-11-06 16:24:57
Environment	3	0	2014-06-27 19:12:14
EUDC	0	4	2014-05-20 14:19:35
⊞ Identities	0	1	2014-05-20 18:43:10
H Keyboard Layout	0	3	2014-05-20 14:19:40
Network	0	1	2014-10-24 15:17:40
Y	6	0	2014-11-06 17:17:13
± Printers	0	4	2014-10-10 20:42:53
⊞ Software	0	79	2014-12-08 13:51:22
± System	0	1	2014-05-20 14:19:35
Associated deleted records	0	0	
🗄 🚡 Unassociated deleted records	0	0	

This is useful for generating reports or other documentation that is easier to manipulate than simply taking a screen shot.

Tools

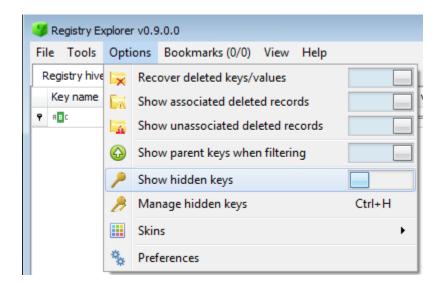
The Tools menu contains a single item, Find.

Registry Explorer v0.0.4.3			
File	le Tools Options Bookmarks (1/0) View		
Regi	Regi 🕖 Find Ctrl+F arks (1/0)		
Key name			

Using this option will be explained in full detail below in the Using Registry Explorer section

Options

This menu contains several options that control such things as recovering deleted records, viewing hidden keys, etc.



- **Recover deleted keys/values**: When enabled (the selector is to the right), Registry Explorer will recover any deleted records available during hive loading
- Show associated deleted records: When enabled, all associated deleted records will be shown in a special group under the main Registry hive data. Any recovered keys that could be associated with an active (that is, not deleted) key will also be shown in relation to the active key. This will be explained more in a subsequent section.
- **Show unassociated deleted records**: Similar to the previous option, but this group contains all of the keys that could not be associated with an active key.
- Show parent keys when filtering: This option changes the way the Registry hives tree works when using the column filters. When this option is enabled, any keys that match a filter will be displayed, along with the parent keys that the matching key belongs to as seen in the screen shot below.

The keys highlighted in yellow are parent keys that may not contain the text entered in the filter column.

F	Registry hives	Available bookmarks (1/1)			
	Key name	<u> </u>	Ŷ	#	Last write tim
Ŷ	0				
	⊿ 🎒 D:\ter	np\re\UsrClassDeletedBag	gs.dat		2/1/2015 7:1
	🔺 🚞 S-1	-5-21-146151751-63468248-1	215037915-1000_Classes	0	9/19/2011 4:
	4 🚞	Local Settings		0	9/19/2011 4:
	⊿	Software		0	9/19/2011 4:
		⊿ 🚞 Microsoft		0	9/19/2011 4:
		⊿ 🚞 Windows		0	9/19/2011 4:
		🔺 🚞 Shell		0	9/19/2011 4:
		⊿ 🚞 BagMRU		4	2/1/2015 7:1
		⊿ 🚞 0		3	2/1/2015 7:1
		⊿ 🚞 0		2	2/1/2015 7:1
			0	2	2/1/2015 7:1
		⊿ 🔀 1		2	2/1/2015 7:1
		⊿ 🙀 0		2	2/1/2015 7:1
		⊿ 🙀	0	3	2/1/2015 7:1
			🔀 0	2	9/19/2011 4:
		🔺 🚞 Bags		0	2/1/2015 7:1
		⊿ 🚞 1		0	9/19/2011 4:
		🔺 🚞 She	II.	0	9/19/2011 4:
			{5C4F28B5-F869-4E84-8E60-F11DB97C5CC7}	12	9/19/2011 4:
		a 🚞 2		0	9/19/2011 4:
		🔺 🚞 She	ll de la companya de	0	9/19/2011 4:
			{5C4F28B5-F869-4E84-8E60-F11DB97C5CC7}	12	9/19/2011 6:
		⊿ 🚞 3		0	9/19/2011 4:
		🔺 🚞 She	ll in the second se	0	9/19/2011 4:
			{5C4F28B5-F869-4E84-8E60-F11DB97C5CC7}	12	9/19/2011 4:

If we turn off this option, we get a much different result as seen below.

Registry hives	Available bookmarks (1/1)			
Key name		Ŷ	# values	Last write timestamp
P 0				
🚞 S-1-5-2	21-146151751-63468248-121	5037915-1000_Classes	0	9/19/2011 4:30:48 PM +
⊿ 🚞 0			3	2/1/2015 7:14:41 PM +0
⊿ 🚞	0		2	2/1/2015 7:14:41 PM +0
	0		2	2/1/2015 7:14:41 PM +0
⊿ 🙀 0			2	2/1/2015 7:15:41 PM +0
⊿ 🙀	0		3	2/1/2015 7:15:41 PM +0
	🔀 0		2	9/19/2011 4:42:44 PM +
5	4F28B5-F869-4E84-8E60-F1	1DB97C5CC7}	12	9/19/2011 4:41:32 PM +
5	C4F28B5-F869-4E84-8E60-F1	1DB97C5CC7}	12	9/19/2011 6:56:43 PM +
5	4F28B5-F869-4E84-8E60-F1	1DB97C5CC7}	12	9/19/2011 4:42:44 PM +

Notice in this screen shot only the keys that match the filter criteria are shown. This can greatly reduce noise in the results in addition to lessening the need to scroll to the keys that match the filter criteria.

Page 11 of 81 Last revised: 5/19/2017 8:36:46 AM • Show hidden keys: When enabled, any keys that have been hidden will be shown in the Registry hives tree. In the screen shot below, several keys are shown.

	Key name	# values	Last write timestamp
٩			
	⊿ UsrClassDeletedBags.dat		2/1/2015 7:15:49 PM +0
	⊿ 💳 S-1-5-21-146151751-63468248-1215037915-1000_Classes	0	9/19/2011 4:30:48 PM +
	⊿ = Local Settings	0	9/19/2011 4:31:27 PM +
	🛛 🚞 MuiCache	0	9/19/2011 7:02:08 PM +
•	⊿ 💳 6	0	9/19/2011 7:02:08 PM +
	52C64B7E	163	2/1/2015 7:15:05 PM +0
	Software	0	9/19/2011 4:31:27 PM +
	VirtualStore	0	9/19/2011 6:58:04 PM +
	Associated deleted records	0	

While we haven't discussed how to hide keys yet (it has its own section below), if we right click on a key, an option to hide the selected key (based on the key path, not just the key name) is shown.

For example, if we hide the MuiCache key	, it will disappear from view, as seen below.
--	---

	Key name	# values	Last write timestamp
٩			
	⊿ 🥮 D:\temp\re\UsrClassDeletedBags.dat		2/1/2015 7:15:49 PM +0
	⊿ 🚞 S-1-5-21-146151751-63468248-1215037915-1000_Classes	0	9/19/2011 4:30:48 PM +
	🛛 🚞 Local Settings	0	9/19/2011 4:31:27 PM +
۲	Software	0	9/19/2011 4:31:27 PM +
	VirtualStore	0	9/19/2011 6:58:04 PM +
	Associated deleted records	0	

Notice the MuiCache key is no longer visible (assuming the Show hidden key option is off). If we enable this option, the MuiCache key will be shown in its original place, but the icon is different to show that it is in fact a hidden key.

Registry Explorer User Guide

	Key name	# values	Last write timestamp
٩			
	a 🥞 D:\temp\re\UsrClassDeletedBags.dat		2/1/2015 7:15:49 PM +0
	▲ = S-1-5-21-146151751-63468248-1215037915-1000_Classes	0	9/19/2011 4:30:48 PM +
	▲ <u>Cotal Settings</u>	0	9/19/2011 4:31:27 PM +
	🖉 🛓 MuiCache	0	9/19/2011 7:02:08 PM +
	2 0	0	9/19/2011 7:02:08 PM +
	52C6487E	163	2/1/2015 7:15:05 PM +0
۲	Software	0	9/19/2011 4:31:27 PM +
	VirtualStore	0	9/19/2011 6:58:04 PM +
	Associated deleted records	0	

When a key is hidden, the lower right corner will have a red dash to indicate this.

- Manage hidden keys: Brings up an interface to remove keys from the auto hide list. There are two options available when hiding keys: hide for session, and hide and add to auto hide. The Manage hidden keys interface only displays key paths that have previously been added to the auto hide list. Any key paths removed from the auto hide list will be unhidden when the Manage hidden keys interface is closed. Additional ways to unhide keys will also be discussed in a subsequent section.
- **Skins:** Allows for selecting a skin or theme that Registry Explorer will use.
- **Preferences:** Program options such as timestamp format, binary data as base64, etc.

The Preferences dialog allows you to change the default timestamp format and other parameters as seen below.

% Preferences		
 Display RegBinar Display value sla 	y values as Base64 ck as Base64	
Date/Time format	yyyy-MM-dd HH:mm:ss	Examples
	2017-05-19 08:00:28	
		Save Cancel

Page 13 of 81 Last revised: 5/19/2017 8:36:46 AM

Bookmarks

The Bookmarks menu contains both common (included with Registry Explorer) and user created bookmarks to "of interest" Registry keys. Bookmarks can be created for any Registry key (we will see how to create our own bookmarks soon). Bookmarks that are included with Registry Explorer will show up under the 'Common' menu and any user created bookmarks will appear under the 'User created' menu.

Bookmarks live in a subdirectory of the main Registry Explorer program directory in a directory named Bookmarks. The Bookmarks directory contains two subdirectories, Common and User. To move a user created bookmark from the User created to Common submenu, simply move the bookmark file from the User directory to the Common directory.

The Manage bookmarks interface can be used to edit or delete bookmarks. Additionally, simply deleting the bookmark file from the Common or User directory will also remove the bookmark.

Bookmarks are simple json files and can also be edited with any text editor. Since they are simple json files, exchanging a good set of bookmarks with other users is as easy as sending someone else the bookmark files from the User directory. There is a project on Github, found <u>here</u>, that you can push your Bookmarks to.

J.U	.0.4.3							
s	Bool	cmarks (1/1) View Help						
ilał	숤	Common (1)	Ø	Bag	MRU (ShellBag root ke	y)		ł
	\star	User created (1)	# valu	les	Last write timestamp	Ī		Valu
	Ē	Manage bookmarks Ctrl+B	L				Ŷ	
or	an gi o	עבו קלבקוטע איובאיבו ב עטו טומטטטבובנ			2/1/2015 7:15:49 P			

The main Bookmarks menu contains two numbers at the end. The first number is the total number of Common bookmarks *that exist in the selected hive* and the last number is the number of User bookmarks *that exist in the selected hive*. Clicking on any of the bookmarks will cause Registry Explorer to jump to the bookmarked key.

Bookmarks are tied to a Registry hive type and a key path within that hive type. When we discuss creating bookmarks below this will become clearer, but for now remember that each bookmark is associated with a certain flavor of Registry hive (NTUSER, UsrClass, SYSTEM, etc).

The Bookmarks menus dynamically adjust as hives are loaded and selected. For example, suppose you have the following bookmarks by hive type:

- NTUSER.DAT: 40 bookmarks
- USRCLASS.DAT: 8 bookmarks

You then load an NTUSER and USRCLASS hive. The NTUSER hive contains 27 out of the 40 key paths as defined in the NTUSER.DAT related bookmarks (27 from Common). The USRCLASS hive contains two out of the eight bookmarks (one from common and one from user created). If you click on anything in the NTUSER.DAT hive, the Bookmarks menu will change to show you *only the bookmarks that actually exist* in the NTUSER hive, like this:

olorer v0.8.0.0

Options Bookmarks (27/0) Vie	w <u>H</u> elp		
; (1) 🗛 🖕 Common (27)	•		7-Zip (7-Zip history and config)
Manage bookmarks Ctrl+B			CD Burning (CDROM burning info)
emp\win10ERZamcachepreso			ComDlg32 (Common dialog)
ют	0		Compression (7-Zip archive history)
sociated deleted records	0		CurrentVersion (Windows)
associated deleted records 0			CurrentVersion (Wndows NT)
		Ø	Default (Terminal server hosts)
			FileExts (List of programs used to open files by extension)
		ø	FileHistory (File history info)
		Ø	FirstFolder (Programs executed)
		Ø	FTP (FTP server and username info)
		Ø	Internet Settings (Internet Explorer settings)
			Map Network Drive MRU (Recently used network shares)

If you then click on the USRCLASS hive, the Bookmarks menu will again dynamically adjust to show what is available in the USRCLASS hive.

s	Book	cmarks (1/1) View Help							
ilał	☆	Common (1)	-	IJ	Bagl	MRU (ShellBag root ke	ey))	a co
	\star	User created (1)	•	# va	alues	Last write timestamp			Value
_	ø	Manage bookmarks Ctrl+B						۴	
ork	ingr or	טבו קלבטואט איובאיבו ביוטא טומאטבובנבי				2/1/2015 7:15:49			
146151751-63468248-1215037915-1000_Cl 0 9/19/2011						9/19/2011 4:30:48			

Again, clicking a bookmark will jump to the key as defined in the bookmark. For example, clicking on the BagMRU bookmark results in the following key being selected (and of course all parent keys will be expanded so the bookmarked key is visible).

Registry Explorer User Guide

Key name	# values	Last write timestamp
۹		
⊿ (¥) D:\temp\re\UsrClassDeletedBags.dat		2/1/2015 7:15:49 PM +0.
▲ = S-1-5-21-146151751-63468248-1215037915-1000_Classes	0	9/19/2011 4:30:48 PM +.
⊿ Cocal Settings	0	9/19/2011 4:31:27 PM +.
⊿ 🚞 MuiCache	0	9/19/2011 7:02:08 PM +.
⊿ 🚞 6	0	9/19/2011 7:02:08 PM +.
52C6487E	163	2/1/2015 7:15:05 PM +0.
⊿ 🚞 Software	0	9/19/2011 4:31:27 PM +.
⊿ microsoft	0	9/19/2011 4:31:27 PM +
⊿ 🚞 Windows	0	9/19/2011 4:31:27 PM +
CurrentVersion	0	9/19/2011 4:31:34 PM +
z Enel	0	9/19/2011 4:41:32 PM +
▶ ► E BagMRU	4	2/1/2015 7:15:41 PM +0.
ags bags	0	2/1/2015 7:14:41 PM +0
VirtualStore	0	9/19/2011 6:58:04 PM +
Associated deleted records	0	

Because the Bookmarks menu dynamically adjusts itself based solely on what exists in the active hive, you do not have to click on bookmarks before you know whether they exist. This is a huge time saver and makes drilling down into hives much easier.

As you interact with loaded hives, the Bookmarks menu will show you at a glance how many bookmarks are available, but as we will soon see, Registry Explorer has an even easier way to interact with bookmarks (the Available bookmarks tab).

The bookmark names are sorted alphabetically as well so it's easy to find the bookmark you are interested in.

View

The View menu contains two options: Messages and Plugins.

Messages toggles visibility of the Messages window. The Messages window displays status messages and other feedback as hives are loaded and so on.

Hives tend to process and load faster when the Messages window is hidden, so keep that in mind when loading many hives at once or when processing large hives.

Message Date	1	Message Type	Message	Hive Path
=		=	a 🖸 c	RBC
2017-05-19 0	7:56:23	Info	Registry Explorer version 0.9.0.0 ready!	
2017-05-19 0	7:57:48	Warning	Header length is smaller than the size of the file.	D:\Sync\Regi
2017-05-19 0	7:57:48	Warning	hbin header incorrect at absolute offset 0x9BE000!!! Percent done: 99.92 %	D:\Sync\Regi
2017-05-19 0	7:57:48	Info	Initial processing complete. Building tree	D:\Sync\Regi
2017-05-19 0	7:57:48	Info	Found root node! Getting subkeys	D:\Sync\Regi
2017-05-19 0	7:57:49	Info	Hive processing complete!	D:\Sync\Regi
2017-05-19 0	7:57:49	Warning	Extra, non-zero data found beyond hive length! Check for erroneous data s	D:\Sync\Regi
2017-05-19 0	7:57:49	Info	Associating deleted keys and values	D:\Sync\Regi
2017-05-19 0	7:57:49	Warning	When getting values for nk record at absolute offset 0x1E2338, not enough	D:\Sync\Regi
2017-05-19 0	7:57:49	Warning	When getting values for nk record at absolute offset 0x1E2C80, not enough	D:\Sync\Regi
2017-05-19 0	7:57:49	Warning	When getting values for nk record at absolute offset 0x1E2DD0, not enoug	D:\Sync\Regi
2017-05-19 0	7:57:49	Warning	When getting values for nk record at absolute offset 0x1E3100, VK record a	D:\Sync\Regi
2017-05-19 0	7:57:49	Warning	When getting values for nk record at absolute offset 0x1E3100, VK record a	D:\Sync\Regi
2017-05-19 0	7:57:49	Warning	When getting value offsets for nk record at absolute offset 0x1E3278, not \ldots	D:\Sync\Regi
ishing record li:	sts			

The total number of messages is also shown on the main window's bottom status bar to the far right. Double clicking the message count will show the Messages form.

Data interpreter
Value: 0 Collapse all hives
Hidden keys:

As mentioned above, the background of the messages count will be yellow if and warning message exists and red if an error message exists. The background color will return to default when the Messages window is shown.

The Plugins option displays a list of available plugins and includes such details as the author, key paths, and descriptions of what the plugin does.

Rugins		×
7-Zip archive hist Ares P2P informa ComDlg32 CIDSiz DHCPNetworkHin File Extensions First folder Known networks ComDlg32 LastVis Office MRU	ation zeMRU hts sitedMRU	
Plugin name	7-Zip archive history	
Author	Eric Zimmerman, saericzimmerman@gmail.com, 501-313-3778	
Key paths	Software\7-Zip\Compression	*
		-
Value name	ArcHistory	
Version	0.5	
Internal GUID	6b1296a2-d3fb-441f-89c1-fd3706855acc	
Short description	Extracts archive history from ArcHistory key	
Lana da stationa	Eutropia erabius bistory from Antilistary lau	
Long description	Extracts archive history from ArcHistory key	^
		-
Plugins loaded:	22	

Plugins will be discussed in more detail in a dedicated section of this manual.

Help

The Help menu contains three options: Quick help, Legend, and About. The Legend shows the various icons seen in the Registry hives tree and a description about them.

The legend contains descriptions for the different icons used for various Registry objects such as hives, keys, and existing key placeholders. The legend can be seen below.



Using Registry Explorer

General concepts

Once hives are loaded into Registry Explorer, Registry Explorer allows you to sort, filter, etc. on both the tree on the left as well as any grids on the right.

Sorting

Sorting works like most every other program in that you can click on a column header to sort that column. Here the Value Name column has been sorted.

 Values				
Drag a column header here to group by that column				
Value Name	alue Type	Data	Value Type Raw	Value Slack
•				
!Do not use this registry key F	RegSz	Use the SHGetFolderPath or S	1	00-00
{00BCFC5A-ED94-4E48-96A1-3F6217F21990} F	RegSz	C:\Users\Donald\AppData\Lo	1	00-00
[1025AEDC 0507 4704 0465 0D 100223AEAE]	Deefe	Cultiones/Departd/AppData/D	1	42 42 2D 4B

Notice the small arrow indicating the sort order.

Other options

Right clicking on a column header will bring up a context menu that allows for sorting (as well as removing any existing sorting), grouping, and customization of columns including hiding or showing any columns.

header here to group	by that column
N	Mru Position
~∌↓	Sort Ascending
Z↓	Sort Descending
8	Group By This Column
	Hide Group By Box
	Hide This Column
	Column Chooser
F.	Best Fit
	Best Fit (all columns)
7	Filter Editor
	Show Find Panel
	Hide Auto Filter Row
E	Conditional Formatting 🔸

Filtering

A column can be filtered by clicking in the blank space below the column header and entering something to filter by. The data will be filtered in real time and the bottom status bar will indicate how many things have been filtered out.

When filters are in place (by entering text in the areas below the column name), information about the active filter will be shown at the bottom of the tree or grid as shown below.

THE 10013 OF	nons bookmarks (0/0) view ricip
Registry hives	Available bookmarks (1/1)
Key name	
🕈 Bag	
⊿ 🎁 D:\ten	np\re\UsrClassDeletedBags.dat
⊿ 🚞 S-1	-5-21-146151751-63468248-1215037915-1000_Cl
⊿ 🚞	Local Settings
4	Software
	⊿ 🚞 Microsoft
	⊿ 🚞 Windows
	⊿ 🚞 Shell
_	E BagMRU
	E Bags
Ass	ociated deleted records
X 🗹 Contains([Key name], 'Bag') 🔻
New No	

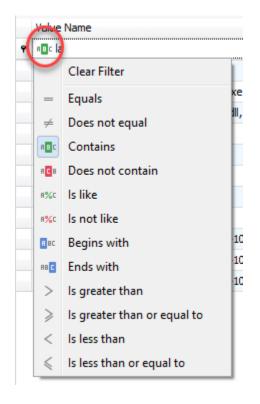
The leftmost X can be used to clear the active filter, the checkbox can be used to disable the filter without clearing it, and the down arrow on the right side contains a history of the different filters that have been recently used.

The 'Edit filter' button on the far right allows you to edit the current filter as needed. This is the same option that is available in the context menu from above.

💙 Registry Explorer vi	0.0.4.3	
File Tools Option Registry hives Av	Filter Editor	
Key name P Bag	And O [Key name] Contains Bag 🛇	st write timestamp
⊿ 🥞 D:\temp\	[# values] Contains 4 🕲	1/2015 7:15:49 PM +0
⊿ 🚞 S-1-5-2		19/2011 4:30:48 PM +
⊿ 🚞 Loc		19/2011 4:31:27 PM +
⊿ 🚞		19/2011 4:31:27 PM +
4		19/2011 4:31:27 PM +
		19/2011 4:31:27 PM +
		19/2011 4:41:32 PM +
		1/2015 7:15:41 PM +0
	OK Cancel Apply	
X V Contains([Key	name], 'Bag') And Contains([# values], '4') 🔻	Edit Filter

Using these options, very detailed filters can be created.

Clicking the icon in the left side of the filter area allows for changing the filter criteria as well. The default is 'Contains'



Conditional formatting

The Registry hives tree, Available bookmarks tree, values grid, and Find results grid all support creating rules to format any column contained therein.

Key name #... Last w ₽Ļ Sort Ascending ٩ D:\temp\re\Us Z Sort Descending 2/1/20 ⊿ 📕 S-1-5-21-1461 9/19/2 lasses 0 Clear Sorting 9/19/2 Local Setti 0 Column Chooser 响 MuiCad 0 9/19/2 \triangleright **Right** click • Softwa 🗔 Best Fit 9/19/2 9/19/2 ⊿ 🚞 Mic 0 Best Fit (all columns) here 0 9/19/2 4 Filter Editor... 9/19/2 ⊳ 0 Show Find Panel 0 9/19/2 Δ 4 2/1/20 ۶ Hide Auto Filter Row 0 2/1/20 🗅 🚞 VirtualStor 🖽 Conditional Formatting Highlight Cell Rules)/19/2 ۶ Associated deleted records t I Top/Bottom Rules ۲ ▲ Contemporary and a state of the state 8 Unique/Duplicate Rules Electric local Settings 5 Manage Rules... D:\temp\re\5.dat /23/2

For example, by right clicking on the Key name column in the Registry hives tree, the following menu is shown.

There are options to format things on a variety of conditions, as seen below.

51001110	i unci		×			
Hide Auto	Filter Row		0	9/19/2011 4:31	L:34 PM	1 +00:00
			1	9/19/2011 4:31	-34 PM	1 +00:00
Condition	al Formatting 🕨	🖽 H	ighlight C	ell Rules 🔹 🕨	≥	Greater Than
🗧 Shell		To	p/Bottom	n Rules 💦 🕨	<	Less Than
🕨 🚞 BagMRU		🖬 Ui	nique/Dur	licate Rules 🔸		Between
🖌 🚞 Bags			inque, pup	incuce nunco y		between
4 🚞 1		ttos M	anage Rul	es		Equal To
🔺 🚞 Shell			0	9/19/2011 4:4:	L:3 ab	Text that Contains
E	5C4F28B5-F869-4E8	4-8E6	12	9/19/2011 4:4:	L:3	Custom Condition
a 🚞 2			0	9/19/2011 4:42	2:37	1 100.00

If we select the 'Text that contains...' option and enter 'Bags' along with how we want any matching rows to be formatted, the tree will reflect these changes. For example, if we entered the following conditions:

Text that Contains			×
Format cells that contain the text:	:		
Bags	with	Red Fill with Red Text 🔹	
Apply formatting to an entire row			
		OK Cancel	

The Registry hives tree would then look like the screen shot below. The instances of 'Bags' in the highlighted rows have been circled for emphasis.

	Key name	#	Last write tim
٩			
	⊿ 🦉 D:\temp\re\UsrClassDelet@Bags.@at		2/1/2015 7:1
	⊿ 💳 S-1-5-21-146151751-63468248-1215037915-1000_Classes	0	9/19/2011 4:
	⊿ Cocal Settings	0	9/19/2011 4:
	MuiCache	0	9/19/2011 7:
	⊿ 🚞 Software	0	9/19/2011 4:
	⊿ 🚞 Microsoft	0	9/19/2011 4:
	⊿ 💳 Windows	0	9/19/2011 4:
	CurrentVersion	0	9/19/2011 4:
	⊿ 🚞 Shell	0	9/19/2011 4:
۲	▷ C BagMRU	4	2/1/2015 7:1
	▷ C Bags	0	2/1/2015 7:1
	VirtualStore	0	9/19/2011 6:

These formatting options allow you to create powerful visual indicators when data that is relevant to you is present in the hives you are looking at. Of course, all formatting options are remembered.

Use the same conditional formatting menu to edit rules.

Loading hives

To load hives into Registry Explorer, either select one or more hives and drag/drop them onto the main interface. You can also use **File | Load offline hive** or press **Alt+1** to select hives.

Registry Explorer will load the hives in parallel and as such, smaller hives will show up in the interface before larger ones. When loading more than one hive at a time, check the status bar at the bottom of the main window to see how many more hives are being processed.

After selecting a hive, Registry Explorer will fully process the hive. Once that is done, the hive will be displayed on the main interface. The top level node for a hive is the full file path to the hive as seen below. The hive node has a green icon and is also in **bold** to differentiate it from keys.

Registry Explorer User Guide

	Key name	# values	Last write timestamp
٩			
<	☑		2/1/2015 7:15:49 PM +0
۲	S-1-5-21-146151751-63468248-1215037915-1000_Classes	0	9/19/2011 4:30:48 PM +
	Local Settings	0	9/19/2011 4:31:27 PM +
	VirtualStore	0	9/19/2011 6:58:04 PM +
	Associated deleted records	0	

The last write timestamp for the hive is the timestamp value from the header of the hive.

Below the hive name is the root key for the hive. The root key name can vary for every hive that is loaded. All other keys in the active (that is, not deleted) portion of the Registry will be displayed under the root key.

If the option to recover deleted records is enabled, up to two different virtual keys may be created: one for Associated deleted records and one for unassociated deleted records. These virtual keys will not be shown if there aren't any deleted records of that type available. As discussed above, these keys can also be hidden using the relevant option under the Options menu.

The number after Registry hives in parenthesis is the total number of hives loaded. In the example below, there are 18 hives loaded.

Registry Explorer v0.0.4.7	
File Tools Options Bookmarks (1/0) View Help	
Registry hives (18) Available bookmarks (41/0)	
Key name	# values
P	
⊿ ⁽³⁾ C:\Temp\UsrClass account rename.dat	
> 5-1-5-21-1141529136-2431258765-826847743-1000_Cla	1
🛛 🖉 C:\Temp\UsrClass CDburn UNC fat filesystem .dat	
▷ 💳 S-1-5-21-1876483248-2010845669-2174274418-1000_Cl	1
⊿ 鍐 C:\Temp\UsrClass zip file network stuff.dat	
▷ 💳 S-1-5-21-2036804247-3058324640-2116585241-1114_Cl	0
⊿ () C:\Temp\UsrClass unicode and network.dat	
▷ 💳 S-1-5-21-3640650475-3814930019-1523317725-1003_Cl	1
⊿ 鍐 C:\Temp\usrclass.dat	
S-1-5-21-1141529136-2431258765-826847743-1000_Cla	1
⊿ 鐣 C:\Temp\UsrClass FTP.dat	
▷ 💳 S-1-5-21-2417227394-2575385136-2411922467-1105_Cl	0
Unassociated deleted records	0
4 🕮 C·\Temp\usedace2 dat	

Projects

Projects allow you to load one or more hives into Registry Explorer and save the currently loaded hives into a project file. This allows you quickly load the same hives for a particular case quickly vs having to load a bunch of hives individually. You can also drag and drop Registry Explorer project files (.re_proj) just like you would a registry hive.

Selecting keys

Selecting keys in Registry Explorer works much the same as it does in regedit or selecting directories in Windows Explorer. Clicking the small arrow to the left of the key name or double clicking a key will expand that key, displaying any subkeys that are present. If the arrow is not visible, the key does not have any subkeys.

Keys can be double clicked and expanded, drilling down into the key hierarchy, until the key you are interested in is located. Alternatively, you can simply start typing a key's name and the keys will be dynamically expanded as matching keys are found in the tree.

For example, assume Registry Explorer looks like this:

	Key name	# values	Last write timestamp
٩			
	⊿ UsrClassDeletedBags.dat		2/1/2015 7:15:49 PM +0
۲	S-1-5-21-146151751-63468248-1215037915-1000_Classes	0	9/19/2011 4:30:48 PM +
	⊿ 🚞 Local Settings	0	9/19/2011 4:31:27 PM +
	D 🧮 MuiCache	0	9/19/2011 7:02:08 PM +
	Software	0	9/19/2011 4:31:27 PM +
	VirtualStore	0	9/19/2011 6:58:04 PM +
	Associated deleted records	0	
	⊿ 🦉 D:\temp\re\5.dat		9/23/2013 7:17:31 PM +
	S-1-5-21-718126207-1171771683-1750804747-1001_Classes	1	8/1/2013 7:21:56 PM +0
	Associated deleted records	0	
	Unassociated deleted records	0	
	⊿ 🥞 D:\temp\re\4.dat		5/20/2014 2:19:35 PM +
	S-1-5-21-2417227394-2575385136-2411922467-1105_Classes	0	1/27/2015 4:47:10 AM +
	⊿ 🥞 D:\temp\re\6.dat		4/24/2014 3:02:54 PM +
	S-1-5-21-2208335738-3127931778-3832183526-1002_Classes	2	8/23/2014 3:20:25 AM +
	Associated deleted records	0	

If you want to look at the contents of the BagMRU key, click on either the hive path or the root key, then start typing *BagMRU*. As each letter is typed, Registry Explorer will search for matching keys and select them. After a few keystrokes, the following key is selected.

			ine Bisti
	Key name	#	Last write tim
٩			
	⊿ 🥮 D:\temp\re\UsrClassDeletedBags.dat		2/1/2015 7:1
	⊿ 🚞 S-1-5-21-146151751-63468248-1215037915-1000_Classes	0	9/19/2011 4:
	⊿ 💳 Local Settings	0	9/19/2011 4:
	MuiCache	0	9/19/2011 7:
	🛽 🚞 Software	0	9/19/2011 4:
	⊿ Constant	0	9/19/2011 4:
	⊿ 🚞 Windows	0	9/19/2011 4:
	CurrentVersion	0	9/19/2011 4:
		0	9/19/2011 4:
۲	BagMRU	4	2/1/2015 7:1
	Bags	0	2/1/2015 7:1
	VirtualStore	0	9/19/2011 6:

Notice also the part of the key that matched what was typed is highlighted. While a bookmark can be used to quickly jump to a particular key, using this technique can save a lot of time when you know the name of the key you are interested in.

Filtering keys

The top of the Registry hives tree contains areas to enter text to filter that column. One thing to note is that *only expanded keys are included in the filter results*. To filter against all keys in a hive, use the context menu option to expand all subkeys (or press **Alt+Down**) before filtering. The next section will cover the context menu in detail.

The **Options | Show parent keys when filtering** option affects what is shown when filtering keys. See the <u>Options</u> section for a full discussion on how this option works.

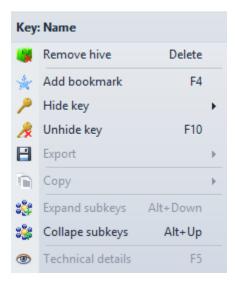
While it may seem that filtering is the quickest way to find a certain key, it is quite often faster to type the name of a key you are interested in (or better yet, using **Tools | Find** if it exists in more than one place).

Key context menu

As in other places, the context menu changes dynamically depending on what you right click on. For example, if you right click on a hive's full path, you will see the option to remove the hive from Registry Explorer. Right clicking anywhere else but the hive's path will hide this option from view. Similarly, if a key is hidden, an option to unhide the key will be shown, else it will be hidden, and so on.

The key context menu looks like this:

Page 27 of 81 Last revised: 5/19/2017 8:36:46 AM



The name of the currently selected key is shown at the top. Most options also have shortcuts which can be used in lieu of using the mouse.

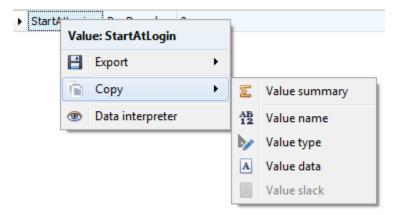
- **Remove hive**: Removes the loaded hive from Registry Explorer. This option is only shown when a hive is selected (denoted by the full path to the hive name, shown in **bold**, and with a different icon).
- Add bookmark: Creates a new user bookmark. Full details will be discussed below.
- Hide key
 - For this session only: Hides keys matching the selected key's path from all loaded hives until Registry Explorer is restarted
 - **Hide and add to auto hide**: Same as the above option, except the key's path is remembered between restarts of Registry Explorer. This option is useful to hide non-useful keys in the Registry that get in your way.
- **Unhide key**: Unhide previously hidden keys with the same path as the selected key. If a key has been auto hidden, this option will remove it from the auto hide list.
- Export
 - **To .reg format**: Exports the selected key and its values to plaintext format. This file can then be imported into the active Registry by double clicking on the generated file.
 - **To .reg format recursively**: The same as above, except all keys and values for the selected key and all subkeys are exported.
- Сору
 - **Key name**: Copies the selected key's key name to the clipboard. Double clicking the key path in the status bar while holding **Shift** also copies the key name to the clipboard.
 - **Key path**: Copies the selected key's key path to the clipboard. Double clicking the key path in the status bar also copies the key path to the clipboard.
 - Last write time: Copies the selected key's last write timestamp to the clipboard. Double clicking the last write timestamp in the status bar also copies the last write timestamp to the clipboard. Double clicking the status bar while holding **Shift** will copy the key name and last write timestamp to the clipboard.
- **Expand subkeys**: Recursively expands the selected key and all subkeys. You can also hold the CTRL key while right clicking a node to expand each key.

Page 28 of 81 Last revised: 5/19/2017 8:36:46 AM

- Collapse subkeys: Collapse all subkeys below the selected key
- **Technical details**: Displays full technical details about the selected key, its subkeys, values, security records, and hive header. This option will be fully explored <u>below</u>.

Value context menu

A typical value context menu may look like this:



The name of the currently selected value is shown at the top.

- Export
 - Value data: Exports selected value's data in *binary form* to a file
 - Value slack: Exports selected value's slack data in binary form to a file. If a value has no slack, this option is disabled
- Сору
 - Value summary: Copies a summary of the selected value to the clipboard. An example is shown below.
 - 1 Registry file: D:\Sync\RegistryHives\1UsrClass.dat
 - 2 Key: Local Settings\MuiCache\24\52C64B7E
 - 3 Last write: 2014-09-11 21:24:22
 - 4 Value: @C:\Windows\system32\OobeFldr.dll,-33056 (RegSz)
 - 5 Data: Getting Started
 - 6 Slack: 69-00-6E-00
 - 7
 - Value name: Copies the selected value's name to the clipboard
 - Value type: Copies the selected value's type to the clipboard (RegBinary or RegSz for example)
 - Value data: Copies the selected value's value data to the clipboard. For RegBinary values, the hex values, separated by a hyphen, are copied to the clipboard as a string
 - **Value slack**: Copies the selected value's value slack to the clipboard. This option formats the data the same as the Value data option. If a value has no slack, this option is disabled.
- Data interpreter: Brings up the Data interpreter window for the currently selected value and converts the value's raw data to a variety of formats. The image below is shows how binary data for a 128 bit timestamp gets converted to different formats.

7 Data Interpreter	-
Numbers	6
8 bit, signed	-35
8 bit, unsigned	221
16 bit, signed	2,013
16 bit, unsigned	2,013
32 bit, signed	591,837
32 bit, unsigned	591,837
64 bit, signed	3,377,716,900,988,893
64 bit, unsigned	3,377,716,900,988,893
Float	8.293403E-40
Double	1.66881388215597E-308
Dates and times	4
DOS FAT Time/date (32 bit)	n/a
DOS FAT Date/time (32 bit)	n/a
Unix/Posix (32 bit)	1970-01-07 20:23:57
Windows FILETIME (64 bit)	1611-09-15 09:28:10
OLE 2.0 Date/time (64 bit)	1899-12-30 00:00:00
Windows SYSTEM Date/time (128 bit)	2013-09-12 02:45:19
Other	4
⊿ GUID	000907dd-0004-000c-0200-2d0013008902
Maps to	
IP Address	221.7.9.0
Strings	6
ASCII	Ýロ
Unicode	d⊡★ -⊡⊎
To Base64	3QcJAAQADAACAC0AEwCJAg==
From Base64	n/a
NOTE: Data is interpreted from the currer	nt offset and is not based on the selected bytes
Offset: 0 (0x0)	Always on top

Value details

The Value details area will change depending on the type of value selected.

Type viewer

For all values except RegBinary values, a simple string representation of the value is shown as seen below.

▶ DDC:\Windov	vs\system32\FXSRESM.dll,-114	RegSz	Windows Fax and Scan
@C:\Windov	ws\system32\mstsc.exe,-4000	RegSz	Remote Desktop Connection
@"v"ndir%	%\System32\je4uinit.exe",-732	RegSz	Finds and displays information and Web sites on the Int
@C:\Windo	system.32\noten.ad.exe469	ReaSz	Text Document
Type viewer	Slack v. r		
Value name	@C:\Windows\system32\FXSRESM.dll,-114		
Value type	RegSz		
Value	Windows Fax and Scan		
Raw value	57-00-69-00-6E-00-64-00-6F-00-77-00-73-00-20-00-46-0	0-61-00-78-00-20-00-6	51-00-6E-00-64-00-20-00-53-00-63-00-61-00-6E-00-00-00
Slack	63-73		
DIDUK	03-73		

The other thing to notice here is the raw value is also shown (highlighted in yellow above). This allows you to export out raw data into other tools, etc.

For RegBinary keys, a hex viewer will be shown to display the value's binary data.

	Value Name	Va	lue T	ype	D	ata							Valu	ie Sla	ck	
٩	R B C	R B	C		Я	BC							R B C			
	NodeSlot	Re	egDw	ord	3	6										
_	MRUListEx	Re	egBin	ary	0	0-00-	00-00	D-FF-	FF-FI	F-FF			00-0	00-00	-00	
•	0	Re	egBin	ary	4	A-00-	31-0	0-00-	-00-0	0-00-	5E-4	3				
1	Type viev	00	01	02	03	04	05	06	07	08	09	0 A 0	0 B	0C	0 D	
00	0000000 4	4A	00	31	00	00	00	00	00	5E	43	FB	9 F	10	00	J. 1 ^Cû
											45					
	000000	· · ·	63		65	00	00	36	00	08	00	04	00	EF	BE	Астебï³4
00	000001C	5 E	43	FB	9 E	00 5E	43	FB	9E	2A	00	00	00	E F 23	BE 00	
00	000001C 5 000002A 0	5 E 0 0	43 00	F B 00	9E 00	5E 01	43 00	F B 00	9E 00	2 A 0 0	00 00 00	00	00 00 00	EF 23 00	BE 00 00	Acme6ï³⁄4 ^Cû.^Cû.*#.
00	000001C 5 000002A 0 0000038 0	5 E 0 0 0 0	43 00 00	F B 00 00	9E 00 00	5E 01 00	43 00 00	FB	9E	2A	00	00	00	E F 23	BE 00 00	Acme6ï³⁄4 ^Cû.^Cû.*#.
00	000001C 5 000002A 0 0000038 0	5 E 0 0 0 0	43 00	F B 00	9E 00	5E 01	43 00	F B 00	9E 00	2 A 0 0	00 00 00	00	00 00 00	EF 23 00	BE 00 00	Acme6ï³⁄4 ^Cû.^Cû.*#.

Selecting a byte or a range of bytes will update the Current offset and Bytes selected values at the bottom of the hex viewer.

Page 31 of 81 Last revised: 5/19/2017 8:36:46 AM

	Value Name	Value Type	Data Value Slack	t
٩	RBC	R B C	RBC RBC	
	NodeSlot	RegDword	36	
	MRUListEx	RegBinary	00-00-00-FF-FF-FF 00-00-00-00-00-00-00-00-00-00-00-00-00-	00
Þ	0	RegBinary	4A-00-31-00-00-00-00-00-5E-43	
Т	ype viewer			
	0000000 000000E 000001C 000002A 0000038 0000046	4A 00 31 0 41 63 6D 6 5E 43 FB 9 00 00 00 00 00 00 00 0	00 00 00 00 00 5E 43 FB 9E 10 0 55 00 00 36 00 08 00 04 00 EF E 0E 5E 43 FB 9E 2A 00 00 00 23 0 00 01 00 00 00 00 00 00 00 00 00	00 J. 1 ^Cû BE Ac me 6 ï ¾ 00 ^Cû. ^Cû. * #. 00
C	urrent offset:	62 (0x3E)	Bytes selected: 8 (0x8)	Data interpreter ?

Slack viewer

For values that have value slack, a Slack viewer tab will be added. This viewer works the same as the Type viewer for RegBinary values.

	Type viewe	Slack vie	wer	D												
Г		00 01	02	03	04	05	06	07	08	09	0A	0 B	0 C	0 D		
L	00000000	5C 57	69	6E	64	6F									∖Windo	
	Current offset	: 0 (0x0))	Byte	s sel	ected	:	0 (0x	(0)						Data interpreter	?

Double clicking on the offset allows for entering an offset to jump to in the hex display.

			Enter 0xC	offse 2	et. Pr	efix ı		0x' fo DK	or hex		imal (Cance					
	Type viewer	Slad	ck vie	wer]											
		00	01	02	03	04	05	06	07	08	09	0A	0 B	0C	0 D	0 E
=	00000000	00	03	00	00	4 C	00	00	00	01	14	02	00	00	00	00
	0000001B	00	20	00	00	00	A5	22	C4	4D	76	95	CE	01	94	ЗF
	0000036	CE	01	AD	05	00	00	00	00	00	00	01	00	00	00	00
	00000051 0000006C	01 FF	32 BF	00	1F 00	80 00	C8	27 3B	34 AF	1F	10 4 D	5C 76	10 95	42 CE	AA 01	03 B7
	00000087	00	00	00	00	00	37	43	F	9D	11	00	54	61	73	6F
	000000A2	0A	43	8A	18	37	43	F4	JD	2E	00	00	00	0D	45	04
	00000BD	00	00	00	00	00	00	J	0A	34	C5	00	54	00	61	00
	00000D8	16	00	18	01	32	2	AD	05	00	00	37	43	EC	9D	20
	00000F3	4 B	00	00	AA	00	09	00	04	00	EF	BE	0A	43	8A	18
	0000010E	00	00 65	05	92	00	00 6F	00	00 65	00	00 74	00	00 20	5A 00	00 45	00
-	Current offset	1		0xC1)				cted		1 (0x	1		20		41	- TH

When viewing binary data, you can copy the selected bytes to the clipboard as either hex, ASCII, or Unicode via the context menu:

14:1	6	RegBinary	43-00-3A-00-	5C-00-78-00-77	7-00-66-00-5	C-00-57-00-6	9-00-6E-00-48-00-6	5-00-78-00-2E-00-65-00	0-78-00-65-00-00 6C
22:2	13	RegBinary	43-00-3A-00-	5C-00-32-00-30	0-00-31-00-3	4-00-31-00-3	1-00-31-00-33-00-3	0-00-38-00-34-00-39-00	-34-00-35-00-5F
14:1	14	RegBinary	43-00-34-00-	50-00-50-00-73	2-00-6E-00-6	7-00-72-00-6	1-00-60-00-20-00-4	6-00-69-00-60-00-65-00	0-73-00-20-00-28- 00
14:5	Type viewer	Slack viewer							
14:2		00 01 02 0	03 04 05 0	6 07 08 0	9 OA OB	0C 0D 0E		13 14 15 16 1	7 18 19 1A 1B 1
14:1	00000000	43 00 3A	00 5C 00 7	8 00 77 0	0 66 00	50 00 79 D Cop	2 00 77 00 66 by hex	Ctrl+Shift+H	0 65 00 6E 00 7
14:1 16:4							y bytes as ASCII	Ctrl+Shift+A	
14:1						🐴 Cop	y bytes as Unicode	≥ Ctrl+Shit	
12:5									
18:3 18:3									

Data interpreter

In the lower right corner of the hex viewer is a Data interpreter button. Clicking this button will bring up the Data interpreter that converts the raw hexadecimal data into a variety of formats including dates and times, GUIDs, IP addresses, and more. The Data interpreter window is shown below.

Data Interpreter	
Numbers	<u> </u>
8 bit, signed	112
8 bit, unsigned	112
16 bit, signed	27,760
16 bit, unsigned	27,760 Value Slack
32 bit, signed	1.634.036.848
32 bit, unsigned	1,634,036,848
64 bit, signed	111,546,229,681,264
64 bit, unsigned	111,546,229,681,264
Float	2.645074E+20 5C-57-69-6E-64-6F
Double	5.51111600086297E-310 65-00
Dates and times	▶
DOS FAT Time/date (32 bit)	2028-11-05 13:35:32
DOS FAT Date/time (32 bit)	2034-03-16 12:11:10
Unix/Posix (32 bit)	2021-10-12 11:07:28
Windows FILETIME (64 bit)	1601-05-10 02:30:22
OLE 2.0 Date/time (64 bit)	1899-12-30 00:00:00
Windows SYSTEM Date/time (128 bit)) n/a
Other	▲
⊿ GUID	61656c70-6573-0000-3a00-08000400efbe
Maps to	
IP Address	112.108.101.97
Strings	▶
	- la ser
ASCII	please
ASCII Unicode	piease 汰 III 微
Unicode	汰燈數
Unicode To Base64 From Base64	太隨勤 cGxlYXNIAAA6AAgABADvvitFHLErRQA4KgAAAKDCQQAAAA
Unicode To Base64 From Base64	汰隨勤 cGxlYXNIAAA6AAgABADvvitFHLErRQA4KgAAAKDCQQAAAA n/a
Unicode To Base64 From Base64 NOTE: Data is interpreted from the curre	汰隨勤 cGxlYXNIAAA6AAgABADvvitFHLErRQA4KgAAAKDCQQAAAA n/a
Unicode To Base64 From Base64 NOTE: Data is interpreted from the curre	太 (提
Unicode To Base64 From Base64 NOTE: Data is interpreted from the current ffset: 14 (0xE)	太 (提
Unicode To Base64 From Base64 NOTE: Data is interpreted from the curre ffset: 14 (0xE) 0 2014-09-111 . 5:58	次 臆動 cGxIYXNIAAA6AAgABADvvitFHLErRQA4KgAAAKDCQQAAAA n/a ent offset and is not based on the selected bytes Always on top ? Type viewer Slack viewer
Unicode To Base64 From Base64 NOTE: Data is interpreted from the current ffset: 14 (0xE) 0 2014-09-11 1 5:58 5 2013-11-20 21:16: 0 2013-08-31 00:10:35	次 間数 cGxIYXNIAAA6AAgABADvvitFHLErRQA4KgAAAKDCQQAAAA n/a ent offset and is not based on the selected bytes Always on top ? Type viewer Slack viewer 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D
Unicode To Base64 From Base64 NOTE: Data is interpreted from the current ffset: 14 (0xE) 0 2014-09-11 1 5:58 5 2013-11-20 21:16: 0 2013-08-31 00:10:35 0 2013-08-31 00:10:36	次 臆動 cGxIYXNIAAA6AAgABADvvitFHLErRQA4KgAAAKDCQQAAAA n/a ent offset and is not based on the selected bytes Always on top ? Type viewer Slack viewer
Unicode To Base64 From Base64 NOTE: Data is interpreted from the current ffset: 14 (0xE) 0 2014-09-111	次 次 次 CGXIYXNIAAA6AAgABADvvitFHLErRQA4KgAAAKDCQQAAAA n/a ent offset and is not based on the selected bytes Always on top 7 Ype viewer Slack viewer 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 00000000 50 00 31 00 00 00 00 2B 45 1C B1 10 00 P1+E. ±
Unicode To Base64 From Base64 NOTE: Data is interpreted from the current ffset: 14 (0xE) 0 2014-09-111	次間数 cGxlYXNIAAA6AAgABADvvitFHLErRQA4KgAAAKDCQQAAAA n/a n/a ent offset and is not based on the selected bytes Always on top ? Type viewer Slack viewer 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 00000000 50 00 31 00 00 00 00 00 2B 45 1C B1 10 00 70 C 65 61 73 65 00 00 3A 00 08 00 04 00
Unicode To Base64 From Base64 NOTE: Data is interpreted from the current ffset: 14 (0xE) 0 2014-09-111 5:58 5 2013-11-20 21:16: 0 2013-08-31 00:10:35 0 2013-08-31 00:10:36 0 2013-08-31 00:10:37 1 2013-08-31 00:36:51	法階韻 CGxlYXNIAAA6AAgABADvvitFHLErRQA4KgAAAKDCQQAAAA n/a ent offset and is not based on the selected bytes Always on top ? Ype viewer Slack viewer 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 00000000 50 00 31 00 00 00 00 00 2B 45 1C B1 10 00 00000000 70 0C 65 61 73 65 00 00 3A 00 08 00 04 00 00000000 FB E 2B 45 1C B1 2B 45 00 38 2A 00 00 00 0000001C EF BE 2B 45 1C B1 2B 45 00 38 2A 00 00 00 0000002A A0 C2 41 00 00 00 00 00 00 00 00 00 00 00 00 00000028 00 00 00 00 00 00 00 00 00 00 00
Unicode To Base64 From Base64 NOTE: Data is interpreted from the current ffset: 14 (0xE) 0 2014-09-11 1 . 5:58 5 2013-11-20 21:16: 0 2013-08-31 00:10:35 0 2013-08-31 00:10:36 0 2013-08-31 00:10:36 0 2013-08-31 00:10:37 1 2013-08-31 00:36:51 0 2013-08-31 00:36:51	次間数 cGxlYXNIAAA6AAgABADvvitFHLErRQA4KgAAAKDCQQAAAA n/a n/a ent offset and is not based on the selected bytes Always on top ? Type viewer Slack viewer 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 00000000 50 00 31 00 00 00 00 00 2B 45 1C B1 10 00 00000000 70 0C 65 61 73 65 00 00 3A 00 08 00 04 00 0000001C EF BE 2B 45 1C B1 2B 45 00 38 2A 00 00 00 0000002 A0 C2 41 00 00 00 00 00 00 00 00 00 00 00 00 00
Unicode To Base64 From Base64 NOTE: Data is interpreted from the current ffset: 14 (0xE) 0 2014-09-11 1 5:58 5 2013-11-20 21:16: 0 2013-08-31 00:10:35 0 2013-08-31 00:10:36 0 2013-08-31 00:10:37 1 2013-08-31 00:36:51 0 2013-08-31 00:36:51 0 2013-08-31 00:10:38	法階韻 CGxlYXNIAAA6AAgABADvvitFHLErRQA4KgAAAKDCQQAAAA n/a ent offset and is not based on the selected bytes Always on top ? Ype viewer Slack viewer 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 00000000 50 00 31 00 00 00 00 00 2B 45 1C B1 10 00 00000000 70 0C 65 61 73 65 00 00 3A 00 08 00 04 00 00000000 FB E 2B 45 1C B1 2B 45 00 38 2A 00 00 00 0000001C EF BE 2B 45 1C B1 2B 45 00 38 2A 00 00 00 0000002A A0 C2 41 00 00 00 00 00 00 00 00 00 00 00 00 00000028 00 00 00 00 00 00 00 00 00 00 00
Unicode To Base64 From Base64 NOTE: Data is interpreted from the current ffset: 14 (0xE) 0 2014-09-11 1 5:58 5 2013-11-20 21:16: 0 2013-08-31 00:10:35 0 2013-08-31 00:10:36 0 2013-08-31 00:10:37 1 2013-08-31 00:36:51 0 2013-08-31 00:36:51 0 2013-08-31 00:10:38 5 2014-03-21 15:13:34	法階韻 CGxlYXNIAAA6AAgABADvvitFHLErRQA4KgAAAKDCQQAAAA n/a ent offset and is not based on the selected bytes Always on top ? Ype viewer Slack viewer 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 00000000 50 00 31 00 00 00 00 00 2B 45 1C B1 10 00 00000000 70 0C 65 61 73 65 00 00 3A 00 08 00 04 00 00000000 FB E 2B 45 1C B1 2B 45 00 38 2A 00 00 00 0000001C EF BE 2B 45 1C B1 2B 45 00 38 2A 00 00 00 0000002A A0 C2 41 00 00 00 00 00 00 00 00 00 00 00 00 00000028 00 00 00 00 00 00 00 00 00 00 00
Unicode To Base64 From Base64 NOTE: Data is interpreted from the current ffset: 14 (0xE) 0 2014-09-11 1 5:58 5 2013-11-20 21:16: 0 2013-08-31 00:10:35 0 2013-08-31 00:10:36 0 2013-08-31 00:10:37 1 2013-08-31 00:36:51 0 2013-08-31 00:36:51 0 2013-08-31 00:10:38	法階韻 CGxlYXNIAAA6AAgABADvvitFHLErRQA4KgAAAKDCQQAAAA n/a ent offset and is not based on the selected bytes Always on top ? Ype viewer Slack viewer 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 00000000 50 00 31 00 00 00 00 00 2B 45 1C B1 10 00 00000000 70 0C 65 61 73 65 00 00 3A 00 08 00 04 00 0000001C EF BE 2B 45 1C B1 2B 45 00 38 2A 00 00 00 000002A A0 C2 41 00 00 00 00 00 00 00 00 00 00 00 00 00

In the example above, a RegBinary value is selected and the 14^{th} byte has been selected (click on a byte to select it). To the right of the hex display is an ASCII interpretation of the binary data. In this case, 70 corresponds to the 'p' character.

Registry Explorer User Guide The Data interpreter also shows the same offset, 14, but it goes a step further and decodes the ASCII string 'please' from bytes 70 6C 65 61 73 65. Registry Explorer will look for a single Null terminator for ASCII strings (00) and double Null terminators (00 00) for Unicode strings. If no Null terminators are found, the bytes will be interpreted from the current offset to the end of the data.



The Data interpreter can also convert GUIDs to known folder/location names as seen below.

In this case, a GUID was found at offset 0x04, 26ee0668-a00a-44d7-9371-beb064c98683, that maps to 'Control panel.'

To copy values from the Data interpreter to the clipboard, press Ctrl+C.

Interacting with deleted keys

Registry Explorer can recover both deleted Registry keys and values. It also reassociates deleted values with their parent keys and subkeys to their parent keys.

In some cases, it is not possible to reassociate recovered keys to an active Registry key because the deleted key's parent cell index does not correspond to a key's offset in the active Registry.

Registry Explorer shows recovered deleted keys in up to three ways: "Inlined' with existing keys (that is, deleted keys are shown where they used to exist), Associated deleted records (the same info as inlined keys, but the parent keys are placeholders), and Unassociated deleted records (no parent key could be found in the active Registry).

Inlined with existing keys

When Registry Explorer can reassociate a key with an active parent key, it is shown under the root key under its parent key. The icon for the deleted key (and all its subkeys) is the same as an active key, but a red X is shown in the lower right corner to denote it is a deleted key. The font for deleted keys is red.

Re	egistry hives (1)	Available bookmarks (1/0)		
ł	Key name		# values	Last write
٩				
4	🖉 🙄 C:\Project	:WorkingFolder\RegistryViewerZ\UsrC		2/1/2015
	⊿ 🚞 S-1-5-21-	-146151751-63468248-1215037915-1000_C	0	9/19/2011
	⊿ 🚞 Local S	iettings	0	9/19/2011
	⊳ 🚞 Mui0	Cache	0	9/19/2011
	⊿ 🚞 Soft	ware	0	9/19/2011
	⊿ 🪞 M	icrosoft	0	9/19/2011
	⊿ 🚞	Windows	0	9/19/2011
	⊳ [CurrentVersion	0	9/19/2011
	⊿ [Shell	0	9/19/2011
	4	a 💳 BagMRU	4	2/1/2015
			3	2/1/2015
•			2	2/1/2015
	(⊿ 🙀 0	2	2/1/2015
	(⊿ 🙀 0	3	2/1/2015
			2	9/19/2011
	D	Bage	0	2/1/2015
	⊳ 🚞 VirtualS	Store	0	9/19/2011
	Associate	ed deleted records	0	

Associated deleted records

All associated deleted records are also shown under a virtual key called 'Associated deleted' records. Under this key, placeholder keys (keys with a link icon in the lower right) are created that denote active keys, down to the point where the deleted key can be found. In the example below, the same path as seen above is reflected down to the 'BagMRU' key. At this point, the icon and font color changes to indicate the key is in fact deleted and has been reassociated.

F	Registry hives (1)	Available bookmarks (1/0)		
	Key name		# values	Last write
٩				
	⊿ 🎁 C:\Project	:WorkingFolder\RegistryViewerZ\UsrC		2/1/2015
۲	▷ 💳 S-1-5-21	-146151751-63468248-1215037915-1000_C	0	9/19/2011
	🔺 📊 Associate	ed deleted records	0	
	⊿ 🚞 S-1-5-:	21-146151751-63468248-1215037915-1000	0	
	⊿ 🚞 Loca	al Settings	0	
	⊿ 🚞 S	oftware	0	
	⊿ 📜	Microsoft	0	
	⊿ [Windows	0	
	4	a 📜 Shell	0	
		⊿ 📜 BagMRU	0	
			2	2/1/2015
	(⊿ 🙀 0	2	2/1/2015
		⊿ 🙀 0	3	2/1/2015
			2	9/19/2011

Unassociated deleted records

In the cases where an active parent key could not be found, the recovered deleted key will be placed under another virtual key called 'Unassociated deleted records' that functions in a similar way to the Associated deleted records. The primary difference between the two is that there will not be any active parent keys shown for unassociated records. Unassociated records can be explored like any other records (looking at values, viewing Technical details, etc.).

• •		
⊿ (¥) C:\ProjectWorkingFolder\RegistryViewerZ\NTUSER.DAT		
CsiTool-CreateHive-{0000000-0000-0000-0000-000000000000}	0	
Associated deleted records	0	
Unassociated deleted records	0	
41a5c7e00-a12e-4cb3-9cd2-30597f5f1d8e	3	
[] {1BC4FA57-AEBC-4152-BD7A-075EE0B96381}	2	
{1C6A51C9-D07D-4e82-BD3E-0EB7F88AC004}	5	
{1F0DA31F-1C61-4b96-B1CC-CBF2D3872353}	5	
🙀 {1F411263-3A1D-43F5-96AF-F5648CB89186}	3	
🏹 {1faf3cb1-30ac-40ca-b115-5999e7daf938}	2	
{1202F5B4-3522-4149-BAD8-58B2079D704F}	12	
{22189D02-CCA4-40AE-A874-6C2A764FB071}	26	
a 🙀 {2E36F1D4-B23C-435D-AB41-18E608940038}	34	
🙀 IncompatibleList	6	
PortSupplier	0	

Creating bookmarks

To create a bookmark, right click on a key and select Add bookmark.

⊿ 🦉 C:\ProjectWorkingFo	lder\RegistryViewerZ\UsrClass	DeletedB	
⊿ 🚞 S-1-5-21-14615175:	l-63468248-1215037915-1000_Class	ses	0
Local Settings			0
⊿ CirtualStore			0
D 🚞 MACHII Key	e VirtualStore		0
🗅 🙀 Associated 🔬	Add bookmark F4	D	0
P	Hide key	•	
8	Export	•	
	Сору	•	
:	Expand subkeys Alt+Down		
***	Collape subkeys Alt+Up		
۲	Technical details F5		

Since Registry Explorer knows the hive type and key path already, these values will be prepopulated. In the example below, a UsrClass hive is active and the VirtualStore key is selected.

Adding bookmar	k 💽
Hive type	UsrClass
Category	▼
Name	VirtualStore
Key path	VirtualStore
Short description	
Long description	A
	· · · · · · · · · · · · · · · · · · ·
	Save

The Category field allows you to place this particular Registry key into a high-level group. This will eventually be used for reporting. Several preexisting categories are included, but typing a new Category will add it to the list.

The Short description serves as a summary for what the key means or why it is relevant. The value entered for Short description will show up after the name of the bookmark in the bookmarks menu.

The Long description should contain technical information, links to web pages with more information, or any other information you want to convey.

Recall the bookmarks menu is dynamic and will update according to the keys that are available for the selected hive. If, before adding the bookmark, the Bookmarks menu looked like this:

1										
	Bool	kmarks (1/0)	/iew H	Help						
3	☆	Common (1)			F		BagMR	U (ShellBag r	oot key)	
		Manage book	marks	Ctrl+B		-		# values	Last w	rite tim
6	orkingFolder\RegistryViewerZ\UsrClassDeletedB 2/1/2015 7:								15 7:1	

And our new bookmark looks like this:

Adding bookmar	k 💌
Hive type	UsrClass
Category	User virtualization -
Name	VirtualStore
Key path	VirtualStore
Short description	Storage that's virtual
Long description	This key contains vero eos et accusamus et iusto odio dignissimos ducimus qui blanditiis praesentium voluptatum deleniti atque corrupti quos dolores et quas molestias excepturi sint occaecati cupiditate non provident, similique
	Save Cancel

The Bookmarks menu will look like this once the Save button is clicked:

0	.4.3									
	Bookmarks (1/1) View Help									
a	☆	Common (1)		F					
	*	User created (1)		۲		Virtual	Store (Storage that'	s virtual)	estamp	
1		Manage boo	okmarks	Ctrl+B		Delet	edB		2/1/2015 7:	15:49 Pl
1	146151751-63468248-1215037915-1000 Classe					es		0	9/19/2011 4	:30:48 F

A 'User created' menu is now visible as is our VirtualStore bookmark (with the short description shown in parenthesis after the key name).

Selecting the 'VirtualStore' bookmark expands all child keys to the bookmarked key in the selected Registry hive.

Managing bookmarks

Recall bookmarks are kept in two folders, one for included bookmarks and one for user created bookmarks. Registry Explorer contains a Bookmark manager that is available under the Bookmarks menu.

ag a colum	in header here	to group by that column				
Туре	Hive Type	Key Path	Category	Name	Short Description	Long Description
User	USRCLASS	Local Settings	Aaa	Local Settings	a	A
Common	NTUSER	Software\Microsoft\Windows\CurrentVersion\Run	Autoruns	Run	User run key	A
Common	NTUSER	Software\Microsoft\Windows\CurrentVersion\UnreadMail	Communication	UnreadMail	Unread email accounts	a
Common	NTUSER	$\verb"Software" \cite{Microsoft} \cite{CorrentVersion} \cite{CorrentVersion} \cite{Corrent} \cite{CorrentVersion} \cite{Corrent} \cite{Corrent}$	Operating system	CD Burning	CDROM burning info	A
Common	SOFTWARE	Microsoft\Windows NT\CurrentVersion	Operating system	CurrentVersion	Windows version information	A
Common	SOFTWARE	Microsoft\Windows NT\CurrentVersion\Image File Executio	Operating system	Image File Execution O	Force a program to run via de	A
Common	SYSTEM	ControlSet001\Control\ComputerName\ComputerName	Operating system	ComputerName	The name of the computer	A
Common	SYSTEM	ControlSet001\Control\Windows	Operating system	Windows	Last shutdown time	A
Common	NTUSER	${\tt Software} {\tt Microsoft} {\tt Windows} {\tt CurrentVersion} {\tt Explorer} {\tt Ru} \dots$	Program execution	RunMRU	Most recently run programs	A
Common	NTUSER	Software\Sysinternals	Program execution	Sysinternals	Sysinternals config info	A
Common	NTUSER	$Software \verb Microsoft Windows CurrentVersion Explorer Us$	Program execution	UserAssist	Recently accessed items	A
Common	SYSTEM	ControlSet001\Control\Session Manager\AppCompatCache	Program execution	AppCompatCache	System compatibility database	A
Common	SYSTEM	MountedDevices	Storage	MountedDevices	Currently mounted volumes	A
Common	SYSTEM	ControlSet001\Enum\USBSTOR	Storage	USBSTOR	USB devices	A
Common	NTUSER	$Software \verb Microsoft Windows CurrentVersion Explorer Co$	User files and fo	ComDlg32	Common dialog	A
Common	NTUSER	$Software \verb Microsoft Windows CurrentVersion \verb FileHistory $	User files and fo	FileHistory	File history info	A
Common	NTUSER	${\tt Software} {\tt Microsoft} {\tt Windows} {\tt CurrentVersion} {\tt Explorer} {\tt Re} \dots$	User files and fo	RecentDocs	Recently opened files by exte	A
Common	NTUSER	Software\WinRAR	User files and fo	WinRAR	WinRar history	a

The column headers in **bold** (Type, Hive Type and Key Path) are read only. To edit any of the other columns, click on that column's value and adjust. The bookmark is saved automatically and the Bookmarks menu will be updated accordingly.

Available bookmarks

The Available bookmarks tab is an optimized way to view all available bookmarks across all loaded hives. Using the Available bookmarks tab allows you to see all bookmarks that exist without the distraction of parent keys or having to drill down into different hives to review things.

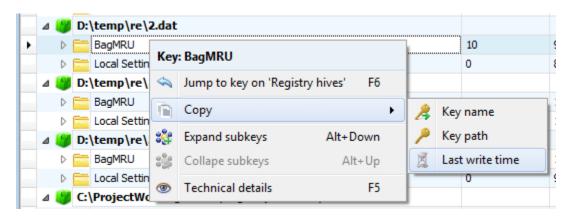
After loading one or more hives, click on the Available bookmarks tab. An example of this is shown below.

Key name		# values	Last write timestamp			
	mp\re\3.dat					
	gMRU	14	11/26/2014 4:14:15 PM			
	cal Settings	0	5/20/2014 2:26:24 PM			
	mp\re\4.dat					
⊳ 🔚 Ba	gMRU	30	1/30/2015 7:00:34 PM			
⊳ 🚞 Lo	cal Settings	0	5/20/2014 2:26:24 PM			
⊿ 🎁 D:\te	mp\re\2.dat					
D 🚞 Ba	gMRU	10	9/23/2014 11:07:17 PM			
⊳ 🚞 Lo	cal Settings	0	8/1/2014 10:38:18 PM			
⊿ 🦉 D:\te	mp\re\1.dat					
D 🔚 Ba	gMRU	156	10/25/2013 2:15:20 PM			
⊳ 🚞 Lo	cal Settings	0	10/23/2009 10:22:25 P			
⊿ 🎁 D:\te	mp\re\5.dat					
D 🚞 Ba	gMRU	17	10/23/2013 3:09:17 AM			
⊳ 🚞 Lo	cal Settings	0	9/23/2013 7:52:03 PM			
⊿ 🦉 C:\Pr	ojectWorkingFolder\RegistryViewerZ\NTUSEF	R.DAT				
🚞 Ru	in	13	12/8/2014 1:19:24 PM			
⊳ 🚞 Ur	readMail	0	7/29/2014 12:26:56 PM			
> 🚞 CI	Burning	2	11/28/2014 4:57:04 PM			
🚞 Ri	InMRU	0	5/20/2014 2:26:30 PM			
⊳ 🚞 Sy	sinternals	0	5/29/2014 1:06:41 PM			
D 🔚 Us	erAssist	0	5/20/2014 2:31:27 PM			
Co	mDlg32	0	5/20/2014 3:21:50 PM			
D 🚞 Fil	eHistory	0	5/20/2014 2:19:35 PM			
⊳ 🚞 Re	centDocs	150	12/8/2014 2:59:56 PM			
⊳ 🧰 W	nRAR	0	9/12/2014 10:45:53 PM			
	es	19	8/26/2014 5:52:22 PM			
D 🚞 De	fault	5	11/29/2014 6:06:33 PM			
▷ 🚞 F1	P	2	11/25/2014 4:52:19 PM			
Bookmark infor	nation					
live	D:\temp\re\3.dat					
Category	User files and folders					
Name	BagMRU	BagMRU				
Key path	Local Settings\Software\Microsoft\Wind	Local Settings\Software\Microsoft\Windows\Shell\BagMRU				
Short descriptio	n ShellBag root key	ShellBag root key				
ong description	ShellBags hold user activity related to a computer	accessing resources on a				

When the root folder for a bookmark is selected (BagMRU in the example above), information about the bookmark is shown at the bottom of the window in the Bookmark information section.

The numbers at the end of the Available bookmarks tab indicate the total number of common bookmarks (20 in this case) and the total number of user created bookmarks (5 in this case). Available bookmarks dynamically updates as hives are loaded/unloaded, bookmarks are created/removed, etc.

Right clicking on a key brings up a context menu. The options work the same way as on the Registry hives tab. The 'Jump to key' option will change the active tab to the 'Registry hives' tab and select the bookmarked key. This is useful to see the bookmarked key in context with other keys.



Finally, common bookmarks are differentiated from user created bookmarks by showing user created bookmarks in blue, as shown below:

F	Registry hives (1) Available bookmarks (2/1)			
	Key name	# values	# subkeys	La
٩	RBC	=	=	=
	a 🦉 D:\Sync\RegistryHives\1UsrClass.dat			20
	BagMRU	15	12	20
	VirtualStore	0	1	20
۲	MuiCache	0	1	20

This makes it easy to spot bookmarks you have added vs ones that were included with Registry Explorer.

Searching

Registry Explorer contains powerful searching capabilities including standard string searches and regular expression based searches. It can also search for keys where the last write timestamp is before, between or after a given timestamp or pair of timestamps, or for values that have a data size greater than a certain number of bytes.

්රී Find					
Options Help					
Standard		Last write timestamp	0	Minimum value size	
Search for Sear	rch in	Earliest (UTC)	· ·	Minimum size (bytes)	1,000 ‡
V Ke	ey name 🔲 Value name	Latest (UTC)	•		Search
	alue data 🔲 Value slack		Before Betwee After	Base64 in values	
Sear	rch type		Search	Minimum length	50 🛟
S S	imple Regular expression				Search
History					
	iteral Search	NOTE: Unassociate	d deleted records are not searched in	this version	
Results (Double click a	row in the Results grid to	select the search hi	t in the main window)		
Drag a column header here to group by that column					
P					
Hive path: None Search hits: None Enter search criteria and click 'Search'			Cancel search	Always on top	Export results

Registry Explorer allows you to search all hives at once across key names, value names, value data and/or value slack. Searching is done against each hive asynchronously and results will appear as they are available.

Options menu

Clear recent

When conducting a standard search, search terms in the 'Search for' box are remembered between program executions. Use this option to clear these recent searches.

Convert

The convert menu contains options to convert the selected search string in the 'Search for' box to its ASCII or Unicode hexadecimal value. This is useful when searching for patterns in Value data.

For example, selecting 'Eric' (without the quotes) and using the conversion options results in the following being shown in the 'Search for' box:

- ASCII: 45-72-69-63
- Unicode: 45-00-72-00-69-00-63-00

The converted value can now be used to search for the initial string in its encoded form. You can also convert terms to ROT-13 and search for encoded strings as well.

Help menu

Search tips

Shows several tips for different kinds of searches

Page 43 of 81 Last revised: 5/19/2017 8:36:46 AM

Regular expressions

Launches a web page with information about creating .net regular expressions

Standard search

To conduct a standard search, simply enter one or more values in the 'Search for' box and click 'Search.' You can also press the Enter key twice on an empty line after entering a search term to perform the search.

68	Find								
0	Options Help								
	Standard								
	search for mui	i					Search in		
1	cad	he							
							Value data 🔲 Value slack		
							Search type		
						-	Simple Regular expression		
	History					-			
	riistor y						Literal Search		
					Rec	vuble	click a row in the Results grid to s		
			and have the stand and				-		
Dr			oup by that column						
	Hive Name	Hit Location	Last Write Time		Key Path				
٩	R <mark>B</mark> C	RBC	=		RBC				
•	1UsrClass.dat		2014-03-21 15:14:0	0	Local Setting				
	1UsrClass.dat	Key name	2014-09-09 03:09:5	51	Local Settings\Software\Microsoft\Windows\Shell\MuiCache				
	1UsrClass.dat	Key name	2014-03-21 15:14:0	0	Local Settings\MuiCache				
	1UsrClass.dat	Key name	2014-09-09 03:09:5	51	${\tt Local Settings} \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \$				
	1UsrClass.dat	Value name	2014-09-11 20:11:4	18	Local Setting	gs\Software	Microsoft\Windows\CurrentVersi		
	1UsrClass.dat	Value name	2013-12-04 19:21:4	1	Local Setting	gs\Software	Microsoft\Windows\Shell\Bags\		
	1UsrClass.dat	Value name	2013-12-04 19:21:4	1	Local Setting	gs\Software	Microsoft\Windows\Shell\Bags\		
	1UsrClass.dat	Value data	2014-09-11 21:24:2	22	Local Setting	gs\Software	Microsoft\Windows\Shell\BagMRU		
н	ive path: D:\Sy	nc\RegistryHi	ves\1UsrClass.dat	Sea	rch hits: 8	Search co	ompleted in 0.00469 seconds across		

The Literal checkbox controls whether the term searched for is looked for in binary data when searching in value data and/or slack. This is explained in more detail below.

If you entered a regular expression, change the radio button to 'Regular expression' so Registry Explorer knows to use RegEx when searching. The Help menu can be used to get additional help on building .net regular expressions. For additional resources on regular expressions, click <u>here</u> to view the regular expression searching section for RECmd.

The History drop down will contain a list of your recent searches

Last write timestamp search

To conduct a last write timestamp search, choose the date range to search for via the radio buttons and enter the required time stamp values, and then click Search (or press Enter).

66	Find										
Op	tions He	lp									
	Standard							Last write timesta	mp		
5	earch for					Search in		Earliest (UTC)			
								Latest (UTG)	2016-06-06 0	0.00.00 K	
						Key name	Value name	Latest (0) b)	2010-00-00 0	0.00.00 K	
						Value data	Value slack		Ø Before	Between	O After
						Search type					Search
											Search
					-	 Simple Regular exp 	ression				10
	listory				•						
	ill scor y					Literal	Search	NOTE: Unassociate	detected records	s are not searche	ed in this version
						Decults (Dec	ıble click a row i	in the scalts grid to			
						Results (Dou	IDIE CIICK a FOW I	in the Lesuits grid to	select the sea	ren nie in the n	nain window)
Dra	ig a column	header here to	group by that column								
	Hive Name		Hit Location	Last Write Time		Key Path					
٩					_						
-				9/19/2011 4:31:27 PM		-					
		-		9/19/2011 7:02:08 PM							
		-		9/19/2011 7:02:08 PM							
		-		2/1/2015 7:15:05 PM +		Local Settings Mu		7E			
		-		9/19/2011 4:31:27 PM							
		-		9/19/2011 4:31:27 PM				are down			
		-		9/19/2011 4:31:27 PM		_ .		windows Windows\CurrentVersion			
		-						Windows (CurrentVersion)			
		-				_ .		Windows (CurrentVersion)			
		-		0/10/2013 7:13:40 PM					(in a yinto un y		
Hi	ve path: D:	\Dropbox\Reg	jistryHives\UsrClass[DeletedBags.dat Sea	arch hits	: 41 Search co	mpleted in 0.002	240 seconds across 1 h	ive		

Note: Depending on the Date/Time format under Preferences you may see extra characters in the earliest and latest time stamp fields. These can be ignored.

Minimum value size search

When searching for values above a minimum size, the size of the value data's length is shown in the Value Data column as seen below.

	- • •
Minimum value size	
Minimum size (bytes)	2,048 Search
Base64 in values	
Minimum length	50 ‡ Search
this version	
	Value Data Length
	=
	327,870
	14,780
	10,343
Always on top	Export results

Base64 in values search

This works the same as a minimum value size, but validates the value's data contains a valid base64 encoded string.

Interacting with search results

Once a search is underway, results will show up in the Results grid at the bottom of the Find window.

68	Find											- • •
0	ptions He	elp										
	Standard							Last write t	imestamp		Minimum value size	
	Search for					Search in		Earliest (UTC)	·	Minimum size (bytes)	2,048 🛟
		cache				🗹 Key name	Value name	Latest (UTC)		•		Search
						Value data	Value slack		() B	efore 🔘 Betwee 🔘 After	Base64 in values	
						Search type				Search	Minimum length	50 🛟
					~	Simple Regular exp	pression					Search
	History				•	Literal	Search	NOTE: Una	ssociated delet	ed records are not searched in t	his version	
				Re	sults (Double d	click a row in th	e Results grid to	select the se	arch hit in th	e main window)		
							j			,		
Dr	-	header here to										
	Hive Name		Hit Location	Last Write Time	Key Path			Deleted		Hit Text	Value Data	
	RBC		R 8 C	=	RBC				RBC	RBC	R B C	<u>^</u>
•	UsrClassDe	eletedBags.dat	Key name	2011-09-19 19:02:08	Local Settings≬	MuiCache				mui		
	UsrClassDe	eletedBags.dat	Key name	2011-09-19 19:02:08	Local Settings≬	luiCache				cache		
	UsrClassDe	eletedBags.dat	Value name	2015-02-01 19:15:48	Local Settings\	Software (Microsof	t\Windows\Curren	tV	PromotedI	cache	{7820NR76-23R3-4229-82	P1-R41PO6
	1UsrClass.	dat	Key name	2014-03-21 15:14:00	Local Settings≬	luiCache				mui		E
	1UsrClass.	dat	Key name	2014-09-09 03:09:51	Local Settings\	Software\Microsof	t\Windows\Shell\M	ui		mui		
	1UsrClass.	dat	Key name	2014-03-21 15:14:00	Local Settings≬	luiCache				cache		
	1UsrClass.	dat	Key name	2014-09-09 03:09:51	Local Settings\S	Software (Microsof	t\Windows\Shell\M	ui		cache		
	1UsrClass.	dat	Value name	2014-09-11 20:11:48	Local Settings\	Software (Microsof	t\Windows\Curren	tv	PromotedI	cache	{7820NR76-23R3-4229-82	P1-R41PO6
	1UsrClass.	dat	Value name	2013-12-04 19:21:41	Local Settings\	Software Microsof	t\Windows\Shell\Ba	a	CachedOf	cache	0	
	1UsrClass.	dat	Value name	2013-12-04 19:21:41	Local Settings\S	Software Microsof	t\Windows\Shell\Ba	a	CachedOf	cache	1817893	-
Н	live path: D	:\Sync\Registr	yHives\UsrCla	assDeletedBags.dat	Search hits: 11	Search comp	leted in 0.00037 s	econds across	2 hives	Cancel search	Always on top E	Export results

In the above example, a simple search was done for the string 'mui' and 'cache' which resulted in 334 hits. The search results contains the hive the hit was found in, what type of hit it was (key name, value name, etc.), the hit text, and other relevant information.

The columns shown in the Results grid will change depending on what kind of search was done. When searching in value name and/or value data, two additional columns will be shown as seen below.

_								-	· · ·		
68	Find								[×
0	ptions He	lp									
ſ	Standard						Last write timestam	p			
	Search for	mui			Search in		Earliest (UTC)				-
		cache					Latest (UTC)				-
						alue name	Latest (OTC)				4
					Value data 🔲 V	alue slack		Ø Before	Between	After	
					Search type					Search	
										Search	
					 Simple Regular expression 	n					
	History				-						
	r listor y				Literal	Search	NOTE: Unas. ociated	dele and records a	re not searche	d in this versio	n
				Results (Double click a row in	the Results grid to sele	t the search	hit in the main wind	low,			
Dr	ag a column l	header here to	group by that	column	L.	}					
	Hive Name		Hit Location	Last Write Time	Hit Text	Key Path			Value Name	Value Data	
٩											-
•	UsrClassDel	letedBags.dat	Key name	9/19/2011 7:02:08 PM +00:00	mui	Local Settin	gs\MuiCache				
	UsrClassDel	letedBags.dat	Key name	9/19/2011 7:02:08 PM +00:00	cache	Local Settin	gs\MuiCache				
	UsrClassDel	letedBags.dat	Value name	2/1/2015 7:15:48 PM +00:00	cache	Local Settin	gs\Software <i>\</i> Microsoft\	Windows\Cur	PromotedI	{7820NR76.	/
	UsrClass (12	2).dat	Key name	8/18/2011 4:30:44 AM +00:00	mui	Local Settin	gs\MuiCache				-
н	ive path: D:	\Dropbox\Re	gistryHives\Us	rClassDeletedBags.dat Search	hits: 334 Search compl	eted in 0.5081	3 s Cancel search	Always on top		Export result	ts

When searching in value data and/or value slack, the Search for term will be found regardless of case or encoding (Western 1252 and/or Unicode to be exact). This makes it easy to find strings that have been encoded in binary data.

The way this works is to take the raw bytes that make up the value data and/or value slack and convert it to a string (again, in Western 1252 and Unicode), which is then searched using a regular expression. The regex will find the hit with exact capitalization, and the exact hit is then converted back to a byte string. This hit can then be reported back to the application and the data highlighted in context with the rest of the data, regardless of encoding or capitalization.

Find												
ptions Help												
Standard						Last write timesta	mp			Minimum value size		
Search for mui				Search in		Earliest (UTC)			*	Minimum size (bytes)	2,048 🛟	
cach	ie 🔪			Key name	Value name	Latest (UTC)			•			
				Value data	Value slack		Ø Before	Between Between	n 🔘 After			
				Search type					Search		Search	
			-	 Simple Regular explanation 	pression							
History			•	Literal	Search	NOTE: Unassociate	d deleted record	ls are not searc	hed in this version			
			Resi	ults (Double clie	k a row in the Re	sults grid to select	the search hit	in the main v	vindow)			
ag a column hea	der here to gr	oup by that column										
Hive Name	Hit Location	Last Write Time	Hit Text		Key Path			Value Name	Value Data			
												_
UsrClass (12	Value data	8/19/2011 1:20:12 AM +	43-00-61-00-63-00-6		Locar occurrigo porc						0-00-00-00-17-28-00-00-31-5	-
		8/19/2011 1:20:12 AM +				ware\Microsoft\Window		8			8-00-00-00-03-28-00-00-31-5	
•		8/19/2011 1:20:12 AM +				ware\Microsoft\Window		14	79-28-1F-00-29-28-0	05-DF-A3-23-1B-28-04-00-0	0-00-00-00-17-28-00-00-31-5	i3
UsrClass (12	Value data	8/19/2011 1:20:12 AM +	43-00-61-00-63-00-6	8-00-65-00	Local Settings\Soft	ware\Microsoft\Window	s\Shell\Bag	15	79-28-1F-00-29-28-0	05-DF-A3-23-1B-28-04-00-0	0-00-00-00-17-28-00-00-31-5	i3
ve path: D:\Dro	pbox\Regist	ryHives\ALL\UsrClass (12).	dat Search hits: 11	0 Search con	pleted in 0.38079	seconds across 3 hive	es		C	ancel search Always on	top Export re	sults

Here is an example of some search hits for 'cache' that were found in binary data:

Page 48 of 81 Last revised: 5/19/2017 8:36:46 AM If the Literal checkbox is checked, the additional search against the converted data is not done behind the scenes. This allows you to look for specific byte patterns without Registry Explorer converting binary data to strings.

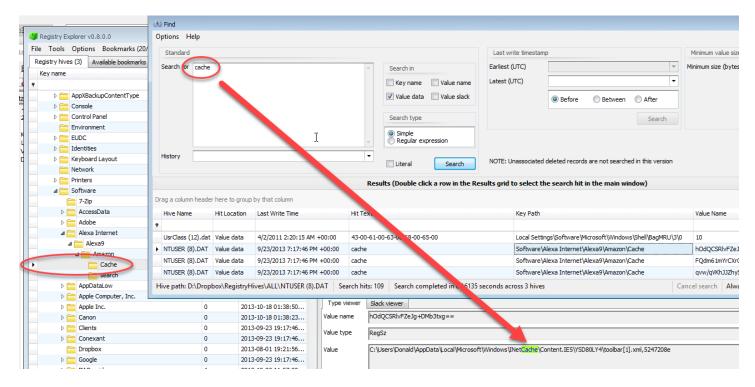
්ර Find				
Options Help				
Standard	Las	st write timestamp		Minimum value size
Search for las	 Search in 	iest (UTC)	Ŧ	Minimum size (bytes) 4,096
\cup		est (UTC)	▼	
	Value data Value slack			
	- Voide data - Voide sider	efore	Between 🔘 After	
	Search type		Search	Search
	Simple			
	Regular expression			
History	Literal Search NOT	E: Unassociated deleted records are n	not searched in this version	
	Results (Double click a row in the Results grid to	o select the search hit in the mai	n window)	
Drag a column header here to group by that column				
Hive Name Hit Location Last Write Time Key Pa	Path	 Hit Text 	Value Name	Value Data Slack
P				
NTUSER_Loveall Value slack 2008-01-31 04:32:24 + Control		6C-00-61-00-73-00	DisplayName	6C-00-61-00-73-00
NTUSER_Loveall Value slack 2008-01-31 04:32:36 + Softwa	tware \Microsoft \Windows \CurrentVersion \Themes \DefaultVi	sualStyleOff 4C-61-73	InstallVisualStyleSiz	re 03-00-4C-61-73-74
15				
Hive path: D:\Dropbox\RegistryHives\NTUSER_Loveall.DAT Sea	earch hits: 2 Search completed in 0.00053 seconds a	across 1 hive	Cancel searc	h Always on top Export results

Here is an example where the string 'las' was found in value slack:

In the screen shot above, notice the hit in value slack was found in two different encodings.

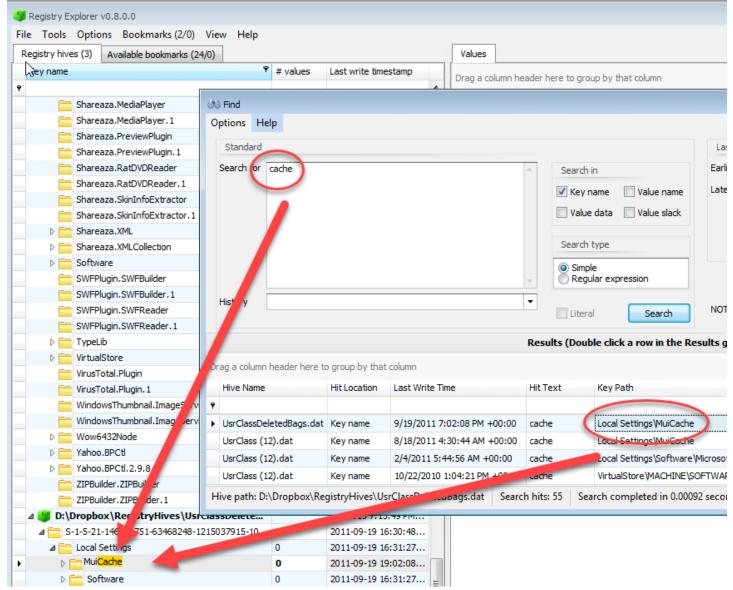
Viewing search results

To view the search hit in the main Registry Explorer window, simply double click on the result you wish to view. The Registry hive containing the hit will be selected along with the key where the hit was found. If the Hit location is in a value name or in value data, the corresponding value will be selected under the key.



For all simple searches, the search hit will be highlighted (or, in the case of a RegBinary hit, the bytes that make up the hit will be selected). A few more examples of this are shown below.

For key name hits, the matching part of the key name is highlighted.



For value data (when the value type is RegBinary) and value slack, the bytes that make up the search hit are selected in the hex viewer.

Last write times 2011-08-19 01: 2011-04-02 02: 2011-02-04 05: 2011-02-04 05: 2011-02-11 03: 2011-02-11 03: 2011-02-11 03: 2011-02-11 03: 2011-02-11 03:	Search for c	cache	7				A		earch in Key name		lue name	Earl	st write ti iest (UTC) est (UTC)				
2011-08-19 01: 2011-04-02 02: 2011-02-04 05: 2011-02-14 07: 2011-02-11 03: 2011-02-11 03: 2011-02-11 03: 2011-02-11 03: 2010-06-18 01:	Search for	cache	7				-		Key name			Earl	iest (UTC)				
2011-08-19 01: 2011-04-02 02: 2011-02-04 05: 2011-02-14 07: 2011-02-11 03: 2011-02-11 03: 2011-02-11 03: 2011-02-11 03: 2010-06-18 01:	Search for	cache	7				A		Key name			Earl	iest (UTC)				
2011-04-02 02: 2011-02-04 05: 2011-02-14 07: 2011-02-11 03: 2011-02-11 03: 2011-02-11 03: 2011-02-11 03: 2011-02-11 03:		cache	7				*		Key name								
2011-04-02 02: 2011-02-04 05: 2011-02-14 07: 2011-02-11 03: 2011-02-11 03: 2011-02-11 03: 2011-02-11 03: 2011-02-11 03:			7									Late	st (UTC)				
2011-04-02 02: 2011-02-04 05: 2011-02-14 07: 2011-02-11 03: 2011-02-11 03: 2011-02-11 03: 2011-02-11 03: 2011-02-11 03:														Ē			
2011-02-14 07: 2011-02-11 03: 2011-02-11 03: 2011-02-11 03: 2011-02-11 03: 2011-02-11 03: 2010-06-18 01:			Ν								lue slack						
2011-02-11 03: 2011-02-11 03: 2011-02-11 03: 2011-02-11 03: 2011-02-11 03:			N						Value dat		IUE SIGCK				Before	🔘 Be	tween
2011-02-11 03: 2011-02-11 03: 2011-02-11 03: 2010-06-18 01:									earch type								
2011-02-11 03: 2011-02-11 03: 2010-06-18 01:								3	earch type	-		_					
2011-02-11 03: 2010-06-18 01:	History							0	Simple								
2010-06-18 01:	History						Ψ.		Pegular e	expression	1						
							•						T. 11				
2011 02 11 02									Literal		arch	NO	E: Unass	ciated de	eleted record	is are not	searche
2011-02-11 03:	· · · · · · · · · · · · · · · · · · ·																
2011-02-11 03:			Re	esuits (D	uble click	a row in	the Resul	ts grid	to select	t the sea	irch hit ir	the.	n window	1)			
2011-02-04 03:	Drag a column h	header here	to group b	y that colu	mn												
2011-02-04 03:	Hive Name	Hitle	act Write T	īmo	Hit Te				Key Path				Mah	e Name	Value I	Data	
2011-02-04 03:		1110 20111	Last write i	ine	THE TE				Reyrau				Valu	envanie		Data	
2011-02-11 03:	Y								(Ē
2011-02-11 03:	UsrClass								İ			osoft\Win				-1F-00-29	
2011-02-04 03:	UsrClass	Value	8/19/2011 1	1:20:12	43-00-61-0	00-6 00-6	8-00-65-00)	Local Set	tings\Soft	ware Micr	osoft\Win	8		65-28-	-1F-00-15	~
2011-02-04 03:	UsrClass	Value	8/19/2011 1	1:20:12	43-00-61-0	0-63-0-6	8-00-65-00)	Local Set	tings\Soft	ware Micr	osoft\Win	14		79-28-	-1F-00-29	~
2011-02-11 03:	UsrClass	Value	8/19/2011 1	L:20:12	43-00-61-0	0-63-00-	8-00-65-00)	Local Set	tings\Soft	ware Micr	osoft\Win	15		79-28-	-1F-00-29	····
2011-02-11 03:	UsrClass	Value	8/19/2011 1	1:20:12	43-00-61-0	0-63-00-6	8 0-65-00)	Local Set	tings\Soft	ware Micr	osoft\Win	16		9D-28	-1F-00-40)
2011-02-11 03:	UsrClass	Value	8/19/2011 1	L:20:12	43-00-61-0	0-63-00-6	8-00 5-00)	Local Set	tings\Soft	ware Micr	osoft\Win	17		79-28	-1F-00-29	···· •
2011-02-11 03:	Live eath DA	Drankavil	De minter della				angela la su	100	Canada au	a namela 🗌 i	Canaalaa	angle A		• • • • • •			. like
2011-02-11 03:	The path: D:\	(propoox/i	registryHiv	es(ALL\U	si cidss (12	Juan S	carch ne 4	109	Search C	ompie	Cancer se	A	ways on	tob 📃	EX	ipon rest	
2011-02-11 03:	52:52	002000	00 00	00 00	00 00 0		0 00 0	200	00 00	00 00	00 00	00 00	00 00	00 00	00 00 0		
2011-02-11 03:																	
2011-02-11 03:																	
2011-02-11 03:			2A 00														B.Lt
2011-02-11 03:																	
2011-02-04 03:																	
2011-02-04 03:																	i.z.e.n t.o.l.i
2010-07-24 23:																	e@
2011-02-11 03:																	
2011-02-11 03:	52:51 CL	urrent offs	et: 10.13	8 (0x279A) Bytes	selected:	10 (0xA)									
	2011-02-11 03: 2011-02-11 03: 2011-02-11 03: 2011-02-11 03: 2011-02-11 03: 2011-02-11 03: 2011-02-11 03: 2011-02-11 03: 2011-02-11 03: 2011-02-04 03: 2011-02-04 03: 2010-07-24 23: 2011-02-11 03:	2011-02-11 03: UsrClass 2011-02-11 03: S2:52 2011-02-11 03: S2:52 2011-02-11 03: S2:52 2011-02-11 03: S2:51 2011-02-10 03: S2:51 2011-02-04 03:04:48 E 2011-02-04 03:04:48 2011-02-04 03:04:48 2011-02-11 03: S2:51 2011-02-11 03: S2:51 2011-02-10 3: S1:04:04:48 2011-02-10 3: S1:04:04:48 2011-02-10 3: S1:04:04:48 2011-02-11 03: S2:51 2011-02-11 03: S2:51	2011-02-11 03: UsrClass Value 2011-02-11 03: UsrClass Value 2011-02-11 03: UsrClass Value 2011-02-11 03: UsrClass Value 2011-02-11 03: Estension of the state stat	2011-02-11 03: UsrClass Value 8/19/2011 1 2011-02-11 03: 52:52 00002600 00 00 2011-02-11 03:52:51 00002706 00 00 000002706 2011-02-11 03:52:51 00002706 00 00 000002776 00 00 2011-02-11 03:52:51 00002770 00 00 000002776 00 00 2011-02-11 03:52:51 00002770 00 00 000002777 00 00 2011-02-11 03:52:51 00002772 06 9 000002772 06 9 00002772 00 9 00002772 06 9 000002772 06 9 0000278 6 D 0 00 00000278 6 D 00 00000278 6 D 00	2011-02-11 03: UsrClass Value 8/19/2011 1:20:12 2011-02-11 03: Esz: No0026D 00 00 00 00 2011-02-11 03: Esz: 000026D 00	2011-02-11 03: UsrClass Value 8/19/2011 1:20:12 43-00-61-6 2011-02-11 03:52:52 0000260 00<00.00	2011-02-11 03: UsrClass Value 8/19/2011 1:20:12 43-00-61-00-63-00-6 2011-02-11 03:52:52 000026D 00	2011-02-11 03: 2011-02-11 03	2011-02-11 03: 2011-02-11 03	2011-02-11 03: 2011-02-11 03	2011-02-11 03: UsrClass Value 8/19/2011 1:20:12 43-00-61-00-63-00-68-0.65-00 Local Settings (soft 2011-02-11 03: UsrClass Value 8/19/2011 1:20:12 43-00-61-00-63-00-68-00-55-00 Local Settings (soft 2011-02-11 03: UsrClass Value 8/19/2011 1:20:12 43-00-61-00-63-00-68-00-55-00 Local Settings (soft 2011-02-11 03: Escretch 1:00 Search h : 109 Search comple 2011-02-11 03: Escretch 0:000260 0:0	2011-02-11 03: 2011-02-11 03	2011-02-11 03: UsrClass Value 8/19/2011 1:20:12 43-00-61-00-63-00-68-00-65-00 Local Settings (software (Microsoft (Win. 2011-02-11 03: UsrClass Value 8/19/2011 1:20:12 43-00-61-00-63-00-68-00-65-00 Local Settings (software (Microsoft (Win. 2011-02-11 03: UsrClass Value 8/19/2011 1:20:12 43-00-61-00-63-00-68-00-68-00-68-00 Local Settings (software (Microsoft (Win. 2011-02-11 03: Sz:52: Divortions 00 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	2011-02-11 03: UsrClass Value 8/19/2011 1:20:12 43-00-61-00-63-00-68-00-65-00 Local Settings (software (Microsoft)(Win 16 2011-02-11 03: UsrClass Value 8/19/2011 1:20:12 43-00-61-00-63-00-68-00-65-00 Local Settings (software (Microsoft)(Win 17 2011-02-11 03: UsrClass Value 8/19/2011 1:20:12 43-00-61-00-63-00-68-00-68-00 5-00 Local Settings (software (Microsoft)(Win 17 2011-02-11 03: UsrClass Value 8/19/2011 1:20:12 43-00-61-00-63-00-68-00 5-00 Local Settings (software (Microsoft)(Win 17 2011-02-11 03: 52:52 0000260 00 <td>2011-02-11 03: 2011-02-11 03</td> <td>2011-02-11 03: UsrClass Value 8/19/2011 1:20:12 43-00-61-00-63-00-63-00-63-00-63-00 Local Settings (software Microsoft Win 16 90-28 2011-02-11 03: UsrClass Value 8/19/2011 1:20:12 43-00-61-00-63-00-63-00-68-00 Local Settings (software Microsoft Win 17 79-28 2011-02-11 03: UsrClass Value 8/19/2011 1:20:12 43-00-61-00-63-00-68-00 5-00 Local Settings (software Microsoft Win 17 79-28 2011-02-11 03: UsrClass Value 8/19/2011 1:20:12 43-00-61-00-63-00-68-00 5-00 Core of the of th</td> <td>2011-02-11 03: UsrClass Value 8/19/2011 1:20:12 43-00-61-00-63-00-65-00 Local Settings/Software/Wicrosoft/Win 16 9D-28-1F-00-4D 2011-02-11 03: UsrClass Value 8/19/2011 1:20:12 43-00-61-00-63-00-65-00 Local Settings/Software/Wicrosoft/Win 17 79-28-1F-00-29 2011-02-1103: UsrClass Value 8/19/2011 1:20:12 43-00-61-00-63-00-68-00 5-00 Local Settings/Software/Wicrosoft/Win 17 79-28-1F-00-29 2011-02-1103: UsrClass Value 8/19/2011 1:20:12 43-00-61-00-63-00-68-00 5-00 Local Settings/Software/Wicrosoft/Win 17 79-28-1F-00-29 2011-02-1103:52:52 D00026ED 00 00 00 00 00 00 00 00 00 00 00 00 00</td>	2011-02-11 03: 2011-02-11 03	2011-02-11 03: UsrClass Value 8/19/2011 1:20:12 43-00-61-00-63-00-63-00-63-00-63-00 Local Settings (software Microsoft Win 16 90-28 2011-02-11 03: UsrClass Value 8/19/2011 1:20:12 43-00-61-00-63-00-63-00-68-00 Local Settings (software Microsoft Win 17 79-28 2011-02-11 03: UsrClass Value 8/19/2011 1:20:12 43-00-61-00-63-00-68-00 5-00 Local Settings (software Microsoft Win 17 79-28 2011-02-11 03: UsrClass Value 8/19/2011 1:20:12 43-00-61-00-63-00-68-00 5-00 Core of the of th	2011-02-11 03: UsrClass Value 8/19/2011 1:20:12 43-00-61-00-63-00-65-00 Local Settings/Software/Wicrosoft/Win 16 9D-28-1F-00-4D 2011-02-11 03: UsrClass Value 8/19/2011 1:20:12 43-00-61-00-63-00-65-00 Local Settings/Software/Wicrosoft/Win 17 79-28-1F-00-29 2011-02-1103: UsrClass Value 8/19/2011 1:20:12 43-00-61-00-63-00-68-00 5-00 Local Settings/Software/Wicrosoft/Win 17 79-28-1F-00-29 2011-02-1103: UsrClass Value 8/19/2011 1:20:12 43-00-61-00-63-00-68-00 5-00 Local Settings/Software/Wicrosoft/Win 17 79-28-1F-00-29 2011-02-1103:52:52 D00026ED 00 00 00 00 00 00 00 00 00 00 00 00 00

										×
Options Help										
Standard							Last write tin	nestamp		
Search for oft					earch in		Earliest (UTC)			_
					Key name 📃 Va	lue name	Latest (UTC)			
				v	Value data 🔲 Va	lue slack		Ø Befo	re 💿 Betwee	en
					earch type					
				St	earch type	_				
) Simple) Regular expression					
			-							
History					Literal	Search	NOTE: Unasso	ciated deleted re	cords are not sea	rche
										_
	Results	s (Double click a rov. r	the Resu	ults grid	to select the sea	rch hit in th	e main window	v)		
Drag a column header here	to group by that	: column								
Hive Name	Hit Location	Last Write Time		Hit Text						
		CODE FITTE THILE		and i dive	Key Path			Value Name	Value Data	
٩				AL ILA	Key Path			Value Name	Value Data	*
P NTUSER (8).DAT	Value data	8/8/2013 7:03:37 PM ·	0:00	oft	Key Path Software Microsof	t\Internet Exp	plorer\Typed	Value Name url 18	Value Data http://go.mic	•
	Value data Value data		0:00 -00:00						http://go.mic	•
NTUSER (8).DAT		8/8/2013 7:03:37 PM ·		oft	Software (Microsof 2. ftware (Microsof	t MediaPlayer		url 18	http://go.mic	• 111
NTUSER (8).DAT NTUSER (8).DAT	Value data	8/8/2013 7:03:37 PM · 10/1/2013 6:51:41 PM	-00:00	oft oft	Software Microsof Software Microsof Software Microsof	t MediaPlayer	Preferences	url 18 ObfuscatedS	http://go.mic C:\Users\Do	• H
NTUSER (8).DAT NTUSER (8).DAT NTUSER (8).DAT	Value data Value data	8/8/2013 7:03:37 PM - 10/1/2013 6:51:41 PM 9/23/2013 7:17:46 PM	-00:00 -00:00	oft oft oft	Software Microsof Software Microsof Software Microsof	t\MediaPlayer t\Office\15.0 t\Office\15.0	Preferences Access\Se Common\I	url 18 ObfuscatedS Path	http://go.mic C:\Users\Do C:\Program F	•
NTUSER (8).DAT NTUSER (8).DAT NTUSER (8).DAT NTUSER (8).DAT	Value data Value data Value data	8/8/2013 7:03:37 PM - 10/1/2013 6:51:41 PM 9/23/2013 7:17:46 PM 10/23/2013 2:56:32 A	-00:00 -00:00 +00:00	oft oft oft oft	Software Microsof Software Microsof Software Microsof Software	t\MediaPlayer t\Office\15.0 t\Office\15.0 t\Office\15.0	\Preferences \Access\Se \Common\I \Common\I	url 18 ObfuscatedS Path FilePath	http://go.mic C:\Users\Do C:\Program F C:\Users\Do	•
NTUSER (8).DAT NTUSER (8).DAT NTUSER (8).DAT NTUSER (8).DAT NTUSER (8).DAT	Value data Value data Value data Value data Value data	8/8/2013 7:03:37 PM - 10/1/2013 6:51:41 PM 9/23/2013 7:17:46 PM 10/23/2013 2:56:32 A 10/23/2013 2:56:32 A 9/23/2013 7:17:46 PM	-00:00 -00:00 +00:00 +00:00	oft oft oft oft oft oft	Software Microsof Software Microsof Software Microsof Software Microsof Software Microsof	t\MediaPlayer t\Office\15.0 t\Office\15.0 t\Office\15.0	VPreferences Vaccess \Se Common \I Common \I	url 18 ObfuscatedS Path FilePath Url FilePath	http://go.mic C:\Jsers\Do C:\Program F C:\Jsers\Do https://offic	•
 NTUSER (8).DAT NTUSER (8).DAT NTUSER (8).DAT NTUSER (8).DAT NTUSER (8).DAT NTUSER (8).DAT 	Value data Value data Value data Value data Value data	8/8/2013 7:03:37 PM - 10/1/2013 6:51:41 PM 9/23/2013 7:17:46 PM 10/23/2013 2:56:32 A 10/23/2013 2:56:32 A 9/23/2013 7:17:46 PM	-00:00 -00:00 +00:00 +00:00 -00:00	oft oft oft oft oft oft	Software Wicrosof Software Wicrosof Software Wicrosof Software Wicrosof Software Wicrosof	t\MediaPlayer t\Office\15.0 t\Office\15.0 t\Office\15.0 . Office\15.0	VPreferences Vaccess \Se Common \I Common \I	url 18 ObfuscatedS Path FilePath Url FilePath	http://go.mic C:\Users\Do C:\Program F C:\Users\Do https://offic C:\Users\Do	•
NTUSER (8).DAT NTUSER (8).DAT NTUSER (8).DAT NTUSER (8).DAT NTUSER (8).DAT NTUSER (8).DAT Hive path: D:\Dropbox\Ru T:51	Value data Value data Value data Value data Value data egistryHives\Al	8/8/2013 7:03:37 PM - 10/1/2013 6:51:41 PM 9/23/2013 7:17:46 PM 10/23/2013 2:56:32 A 10/23/2013 2:56:32 A 9/23/2013 7:17:46 PM	-00:00 -00:00 +00:00 +00:00 -00:00 εarch hits	oft oft oft oft oft oft :: 1,388	Software Wicrosof Software Wicrosof Software Wicrosof Software Wicrosof Software Wicrosof Software Wicrosof Search comp	t\MediaPlayer t\Office\15.0 t\Office\15.0 t\Office\15.0 t\Office\15.0 Cance vearcl	\Preferences \Access\Se \Common\I \Common\I h Always on t	url 18 ObfuscatedS Path FilePath Url FilePath top	http://go.mic C:\Users\Do C:\Program F C:\Users\Do https://offic C:\Users\Do Export results	
NTUSER (8).DAT NTUSER (8).DAT NTUSER (8).DAT NTUSER (8).DAT NTUSER (8).DAT NTUSER (8).DAT Hive path: D:\Dropbox\R4	Value data Value data Value data Value data Value data egistryHives\Al	8/8/2013 7:03:37 PM - 10/1/2013 6:51:41 PM 9/23/2013 7:17:46 PM 10/23/2013 2:56:32 A 10/23/2013 2:56:32 A 9/23/2013 7:17:46 PM LL\NTUSER (8).DAT	-00:00 -00:00 +00:00 +00:00 -00:00 εarch hits	oft oft oft oft oft oft :: 1,388	Software Wicrosof Software Wicrosof Software Wicrosof Software Wicrosof Software Wicrosof Software Wicrosof Search comp	t\MediaPlayer t\Office\15.0 t\Office\15.0 t\Office\15.0 t\Office\15.0 Cance vearcl	\Preferences \Access\Se \Common\I \Common\I h Always on t	url 18 ObfuscatedS Path FilePath Url FilePath top	http://go.mic C:\Users\Do C:\Program F C:\Users\Do https://offic C:\Users\Do Export results	

For value name and non-RegBinary value data hits, all instances of the search term are highlighted.

Search tips

The fastest searches are against key names. Searching against value names will be slower than key names only. Searching value data/value slack is slower still. This is because every value of every key has to be looked at in order to search for value names or value data/slack across all loaded hives.

Do not let this stop you from searching against value names and data however. Even with these options selected, Registry Explorer can still search multiple hives very quickly (often under a second), but this depends on the number of keys and values in the loaded hives.

You can export the search results to Excel via the button in the lower right.

Technical details in depth

One unique feature of Registry Explorer is the ability to view the technical details of any key, its values, security information, etc. This feature bridges the gap between a hex editor and other viewers in that Registry Explorer can be used to validate itself as to its interpretation of Registry data.

To view the technical details of a key, select the key you are interested in, then right click and select 'Technical details' from the context menu. **F5** can also be used as a shortcut.

Technical	details i	for 'Lo	ocal S	Settin	gs\So	oftwa	re≬M	icroso	oft\W	indov	vs\Sh	ell\Ba	agMRI	ט'									×
NK record	Value	s :	Subke	eys	SK	record	1	Full d	etails	as te	ext	Hive	e deta	ails									
General in																		4	•		xes are relative. Add 0 ata in a hex editor)x1000 to find t	the
Size (Offse	et 0x00)						0x58	(88)											same u	ata in a nex cuitor		
Relative of	ffset							0x5BD	D0 (2	3504)												
Absolute o	ffset							0x6BI	D0 (2	7600)												
Signature	(Offset	0x04	1)					nk											_				
Last write	timesta	mp ((Offse	t 0x0	8)			2/1/2	015	7:15:	41 PN	1 +00	0:00										
Is free																							
⊿ Flags (Off:	set 0x0	6)						0x000	0000	20													
Flags p								Comp	resse	edNar	ne												
Name info	rmation																						
Name (Off	set 0x5	i0)						BagM	RU														
Name leng	th (Off	set 0	x4C)					0x6 (6)														
Maximum r	name le	ngth	(Offs	et Ox	38)			0x2 (2)														
Parent cel	l inform	ation																					
Parent cell	index (Offse	et Ox	14)				0x57	30 (2	2448))												
Value infor	rmation																						
Value cour	nt (Offs	et 0x	28)					0x4 (4)														
Value list c	ell inde:	x (Of	fset (0x2C)				0x5A	78 (2	3160)										click 'Parent cell index'	to load technic	al
Marian		I.		104				010	(10)										÷	details f	for this key's parent		
	00	01	02	03	04	05	06	07	08	09	0 A 0	0 B	0C	0D	0 E	0 F	10	11	1	2 13			
00000000	A8	FF	FF	FF	6E	6B	20	00	30	D0	6 B	78	53	3E	D0	01	00	00	0	00 00	ÿÿÿnk .0Đk:	x S > Ð	
00000014	BO	57	00	00	01	00	00	00	00	00	00	00	10	53	00	00	FF	FF	F	FFF	° W		
00000028	04	00	00	00	78	5A	00	00	E0	02	00	00	FF	FF	FF	FF	02	00	0	00 00	x Z à	. ÿÿÿÿ	
000003C	00	00	00	00	12	00	00	00	16	00	00	00	00	00	00	00	06	00	0	00 00			
00000050	42	61	67	4D	52	55	00	00													BagMRU		
																					-		
																			_				
C:\ProjectW	/orking	Fold	er\Re	egisti	yVie	werZ	\Usi	Class	Dele	tedB	ags.	dat									Bytes selected: 8	Offset: 0x8 (8)) ?

In the example above, the Technical details for the 'Local Settings\Software\Microsoft\Windows\Shell\BagMRU' key are shown. The bytes at the bottom of the details form are the bytes for the NK record as they are found in the Registry hive as viewed in a hex editor.

As different properties are selected, the highlighted bytes change to reflect the location in the raw data where that property lives. The Last write timestamp property is selected, as are the bytes that this property is derived from.

The selected bytes can be copied via **Ctrl+C.** Hold **Ctrl+Alt+C** to copy both the property name and the value to the clipboard.

If a key contains one or more values, the Values tab is visible and contains a list of all the key's values. Selecting a value will display the VK record's properties and raw data as we saw with the NK record above.

VK record	Values	ss	ubke	ys	SKir	ecore	i F	Full de	etails	as te	ext	Hive	e det	ails								
Values											Va	lue p	roper	rties								
										"		Gene	ral in	form	ation							
												Size ((Offse	et Ox	00)					0xFF	FFFFE0 (-32)	
4RUListEx				-						L		Relat	ive o	ffset						0x2E	EA8 (11944)	
lodeSlots												Absol	lute o	ffset	t					0x3E	EA8 (16040)	
										-	1	Signa	ture	(Offs	set 0>	(04)				vk		
												Is fre	e									
											⊿	_	-		x14)					0x1		
													ags p							Nam	ne is ASCII	
													e info									
															Offset		6)			0x1	(1)	
													-)x18)					0		
													infor									
															et 0>	(10)				0x3	(RegBinary)	
													is res		-						- ()	
															ffset	0x08)				6 (22)	
													(offs r info		-					Data	a at relative offset 0x2EC8 (11	976)
	1					_						Othe	rinto	rmat	ION							
/K record	Value	data	Va	alue s	lack																	
	00	01	02	03	04	05	06	07	08	09	0 A 0	0 B	0C	0 D	0 E	0 F	10	11	12	13		
0000000 0000014				F F 00									C8	2 E	00	00	03	00	00	00	àÿÿÿvkÈ c.0.e.d.u.	

At the bottom of the Values tab, the raw VK record is shown. A hex viewer for the value data and value slack (if the value has slack) is also shown. This allows you to see both the VK records and the data in one place. The value data/slack is the data that is available at the Data offset.

Technical	details for	'Local Settin	gs\Software	Microso	oft\Wir	ndows	Shell\₿	agMRI	U'						
NK record	Values	Subkeys	SK record	Full d	etails	as tex	t Hiv	e deta	ails						
Values						1	Value p	proper	ties						
0						1 6	Gene	eral in	form	ation					
1						1 -	Size	(Offse	et Ox	00)					0xFFFFFE0 (-32)
MRUListEx NodeSlots							Rela	tive of	ffset						0x2EA8 (11944)
Nouesious								lute o		•					0x3EA8 (16040)
							_	ature	(Offs	set 0x	(04)				vk
							Is fre								
						-	4 Flags 5	-		-					0x1 Name is ASCII
								ags pi e infor							Name is ASCII
								e leng			0.00	5)			0x1(1)
								e (Off				.,			0
								infor							
							Data	type	(offs	et 0x	(10)				0x3 (RegBinary)
							Data	is res	ident	t					
								lengt			0x08)			0x16 (22)
								(offs		-					Data at relative offset 0x2EC8 (11976)
			\sim				Othe	er info	rmat	ion					•
VK record	Value da	ta Value	slack												
	00 0	1 02 03	04 05 0	06 07	08	09 0	A OB	0C	0 D	0 E	0F	10	11	12	13
00000000	14 0	0 1F 50	E0 4F [00 20	EA	3A 6	9 10	A2	D8	08	00	2 B	30	30	9D 📕 PàOĐ ê:i. ¢ Ø +00.
00000014	00 0	0													
C:\ProjectW	/orkingFo	Ider\Regist	ryViewerZ\l	JsrClass	Delet	edBag	js.dat	1				1			Bytes selected: 0 Offset: 0x0 (0) ?

If a key contains subkeys, the Subkeys tab is visible and contains a list of the current key's subkeys. Double clicking on a subkey will open the Technical details report for that key in its own window.

NK record Valu	es Subkeys	SK record	Full details as text	Hive details	3			
		Double click	a row to open the	e Technical d	details view for the sele	cted subkey		
Drag a column head	der here to arou	p by that colu	mn					
-	-	ite Timestamp		0	ubkey Count	Value Count		Is Free
Key Name		ite limestamn		S	UDKEV COUNT			
inc y manie	Lust W	ree minestamp	,		abitery count	Volue Courte		
9	Lust	ree ninestanip	, 		abite) edunt	Value Count		
		15 7:14:41 PM				1	3	

Page 56 of 81 Last revised: 5/19/2017 8:36:46 AM

Keys found in the active Registry (in other words, not deleted) will have an SK record tab that contains the security key information for the NK record. The SK record tab works the same as the NK and VK tab in that the hex editor updates when properties are selected, etc.

Technical d	letails f	ior 'Lo	ocal S	etting	gs\So	oftwa	re (M	icroso	ft\W	indov	vs\Sh	ell\Ba	agMR	U'							
NK record	Values	s 5	Subke	eys	SKI	recor	d	Full d	etails	as te	ext	Hiv	e det	ails							
General inf	ormatio	n																-	n.		
Size (Offse	t 0x00)							0xD0	(208)											
Relative of	fset							0x2E) (73	6)											
Absolute of	ffset							0x12	EO (4	832)									•		
Signature (Offset	0x04	f)					sk													
Forward lin	k (Offs	et Ox	:08)					0x12	3 (29	6)											
Backward li	ink (Off	iset O	x0C)					0x1D	8 (47	2)											
Reference count (Offset 0x10)						(0x1E	(30)													
Descriptor		(Offs	et 0x	(14)				0xB8 (184)													
Descriptor	Descriptor data																				
Revision (Offset 0x18) 0x1 (1) Image: A control flags (Offset 0x1A) 0x00008004																					
⊿ Control	flags ((Offse	t Ox 1	1A)				0x00	00800	04											
_	s prese							SeDa	dPres	sent,	SeSe	lfRel	ative								
Offset t		-			•			0x80													
Offset t								0x9C)											
Offset t		-		-				0x0 (·												
Offset t	to SACL	. (Off	set 0)x28)				0x14	(20)												
DACL																		· .			
Devi	icion (o	ffeat	0~00	n				0v2(וכ												
	00	01	02	03	04	05	06	07	08	09	0 A	0 B	0C	0 D	0 E	0 F	10	11	12	13	
00000000	30	FF	FF	FF	73	6B	00	00	28	01	00	00	D8	01	00	00	1 E	00	00	00	0ÿÿÿsk(Ø
00000014	B8	00	00	00	01	00	04	80	80	00	00	00	9C	00	00	00	00	00	00	00	, · · · · · · · · · · · · · · · · · · ·
00000028	14	00	00	00	02		6C			00	00	00	00		24	00		00	0 F	00	· · · · · · · · · · \$. ?
000003C	01	05	00	00	00		00	05		00	00	00	47	19	B6	08		72		03	G. 1. Ør È.
00000050	DB	01		48		03		00				00	3F	00	0F	00	01	01		00	Û. I Hê ?
00000064	00	00		05		00					18	00	3F	00	0F	00	01	02		00	···· · · · · · · ⁷ · · · · · ·
00000078 0000008C	00	00	00	05 00	20			00	20	02 00	00	00	00	03 05	14	00	19	00		00	
0000008C	15	00	00	00	47		B6	05	D8	72	C8	00	DB	01	6C	48	E8	00		00	G. 11. ØrÈ. Û. IHè
000000A0	01	05	00	00		00	_			00				19		40 08	D8		C8		G. 1. Ør E. O. THE
00000000				48			_														Û. I H
C:\ProjectW	orking	Fold	er\Re	egistr	yVie	werZ	\Usi	Class	Dele	tedB	ags.	dat								B	ytes selected: 4 Offset: 0x10 (16) ?

The 'Full details as text' tab contains a textual representation of the selected key including the NK record, all VK records, and the SK record. This can be copied and pasted into reports as needed.

Finally, the Hive details tab contains information about the hive where the key was found. This includes the sequence numbers, timestamp, length, root key name, checksum, and so on.

Krecord Values Subkeys SK record Full deta	as text Hive details
General information	
Signature	regf
Sequence 1	0x15 (21)
Sequence 2	0x15 (21)
Timestamp	2/1/2015 7:15:49 PM +00:00
Version	1.3
Length	0x34000 (212,992)
Embedded file name	\Microsoft\Windows\UsrClass.dat
Root cell index	0x20 (32)
Root key name	S-1-5-21-146151751-63468248-1215037915-1000_Classes
CheckSum	0x8CB71E6C (-1934156180)
Calculated CheckSum	0x8CB71E6C (-1934156180)
CheckSum match	

Plugins

Plugins provide a means to process a key and/or value in the Registry. They are primarily intended for binary or otherwise obfuscated keys and values to be decoded to a more user friendly manner. The plugin architecture is open source and easy to implement.

Each release of Registry Explorer will contain all available plugins, but the hope is that others will also contribute to the Registry Explorer project, located at <u>https://github.com/EricZimmerman/RegistryPlugins</u>.

Plugins live under the main Registry Explorer directory in a subdirectory called 'Plugins' which can also contain other directories as needed. Plugins are named according to the format:

RegistryPlugin.*.dll

Where the * is a description of what the plugin is for. Any subdirectories under the Plugins directory are also checked for files matching the above specification.

When Registry Explorer is started, it looks for all files matching that pattern. It then verifies that each file found is indeed a plugin. If it is, the plugin is made available to Registry Explorer.

To view all available plugins, use the View | Plugins menu option. When this is selected, the following dialog is displayed:

Rugins		- • ×
7-Zip archive his Ares P2P informa ComDlg32 CIDSiz File Extensions First folder	ation zeMRU	E
ComDlg32 LastVi ComDlg32 LastVi ComDlg32 Opens ComDlg32 Opens Recent documen	sitedPidlMRU SaveMRU SavePidlMRU	······································
Plugin name	ComDlg32 LastVisitedMRU	
Author	Eric Zimmerman, saericzimmerman@gmail.com, 501-313-3778	
Key paths	Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\LastVisitedMRU	A
Value name		
Version	0.5	
Internal GUID	b2b33fad-e2e7-41e2-bc5b-292483df83ba	
Short description	Extracts executables and last visited directory from LastVisitedMRU key	* *
Long description	Extracts executables and last visited directory from LastVisitedMRU key	•
Plugins loaded:	15	

As different plugins are selected, the properties for the plugin are updated. In the above example we can see the name of the plugin and the exact key path (or paths) a plugin will handle.

Plugins can be tied to a key name or a key name and a value name. When a plugin processes particular value, that value name will be shown in the appropriate field.

The Internal GUID is an identifier Registry Explorer uses to make sure each plugin is unique. In this way you can have multiple plugins for a given key and things would still work properly (vs. basing uniqueness off of a name or similar).

The short and long descriptions are used to explain in more detail what a plugin is doing, why it is relevant, etc. The long description can also include even more details including links to blogs, etc.

Using plugins

There is no requirement on a user's part other than clicking on a given key and/or value. As Registry Explorer is used to navigate around a hive, Registry Explorer checks if any plugins have registered an interest in the selected key/value. If any plugins are found, the key is passed to the plugin for processing and the plugin then returns results to Registry Explorer which it then displays.

For example, say a user clicks on the SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\ClDSizeMRU key. This key's values look like this:

ag a column hea	ader here to grou	ip by that column
Value Name	 Value Type 	Data
54	RegBinary	46-00-54-00-48-00-20-00-49-00-6D-00-61-00-67-00-65-00-72-00-2E-00-65-00
55	RegBinary	62-00-69-00-74-00-6D-00-61-00-70-00-63-00-61-00-63-00-68-00-65-00-76-00
56	RegBinary	70-00-65-00-67-00-61-00-73-00-75-00-73-00-67-00-75-00-69-00-2E-00-65-00
57	RegBinary	70-00-6F-00-77-00-65-00-72-00-73-00-68-00-65-00-6C-00-6C-00-70-00-6C-00
58	RegBinary	70-00-75-00-74-00-74-00-79-00-67-00-65-00-6E-00-2E-00-65-00-78-00-65-00
59	RegBinary	76-00-6D-00-77-00-61-00-72-00-65-00-2E-00-65-00-78-00-65-00-00-00-00-00
6	RegBinary	7B-00-31-00-42-00-46-00-41-00-45-00-46-00-38-00-42-00-2D-00-31-00-37-00
60	RegBinary	53-00-65-00-74-00-75-00-70-00-48-00-6F-00-73-00-74-00-2E-00-45-00-78-00
61	RegBinary	53-00-68-00-65-00-6C-00-6C-00-42-00-61-00-67-00-73-00-45-00-78-00-70-00
62	RegBinary	4D-00-66-00-74-00-32-00-43-00-73-00-76-00-36-00-34-00-2E-00-65-00-78-00
63	RegBinary	4D-00-66-00-74-00-32-00-43-00-73-00-76-00-2E-00-65-00-78-00-65-00-00-00
7	RegBinary	65-00-78-00-70-00-6C-00-6F-00-72-00-65-00-72-00-2E-00-65-00-78-00-65-00
8	RegBinary	64-00-65-00-76-00-65-00-6E-00-76-00-2E-00-65-00-78-00-65-00-00-00-00-00-00-00-00-00-00-00-00-00
9	RegBinary	6E-00-61-00-76-00-69-00-63-00-61-00-74-00-2E-00-65-00-78-00-65-00-00-00
MRUListEx	RegBinary	16-00-00-00-05-00-00-00-00-00-00-3E-00-00-3F-00-00-00-2A-00-00-00

There are many RegBinary values and an MRUListEx value that tracks the order each of the values. Clicking on a value would display all of the binary data in the hex viewer, like this:

	۲	21		R	46	-00-6	9-00	-6C-0	0-6	-00	14-00								3	72-	-00-6	D-00								
L	_	22		R						~	15-00								3	88-	07-0	0-00								Ŧ
	1	Гуре	viev	ver	Slad	ck vie	wer	1																						
ſ					00	01	02	03	04	05	06	07	08	09	0A	0 B	0C	0 D	0 E	0F	10	11	12	13						^
L	0	0000	0000)	46	00	69	00	6C	00	65	00	44	00	61	00	74	00	65	00	2 E	00	65	00	F.i.l.e.	. D. a	a.t	. e	. e.	
L	0	0000	014	Ļ	78	00	65	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	x. e					
L	0	0000	028	3	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00						
l	0	0000	030	2	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00						
l	0	0000	050)	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00						
l	0	0000)064	Ļ	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00						
l	0	0000	078	3	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00						
l	0	0000	080	2	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00						
l	0	0000)0A0)	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00						
l	0	0000)0B4	Ļ	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00						
	0	0000	300	3	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00						
ŀ	0	0000	NULX	r i	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00						~
	C	urrer	nt o	ffset:	() (Ox())	Byte	es sel	ecte	d:	0 (0)	d)													Data	inte	rprete	er 👘	?

A Unicode string can be seen in the data, but it is difficult to see all of the data at once. This is where the plugin steps in and presents a much easier to use presentation of the values under this key. After a plugin processes a key, a new tab is displayed next to the Values tab at the top of the right side of Registry Explorer:

ag a column header here to group by that column			
Executable	MRU 🔺	Opened On	
{50D526C4-E50C-4138-A032-29EB9DE9EC35}	0	5/3/2016 4:41:26 PM +00:00	
PickerHost.exe	1		E
EditPadPro7.exe	2		
Mft2Csv64.exe	3		
Mft2Csv.exe	4		
{33BE88C0-71D4-49E5-9891-64DB26171AF2}	5		
ShellBagsExplorer.exe	6		
xwforensics.exe	7		
{1BFAEF8B-17E3-4D03-BAD2-68853E050708}	8		
snagiteditor.exe	9		
chrome.exe	10		
{21EB7BD4-C127-401D-9751-5D221AEF0307}	11		
postbox.exe	12		
vlc.exe	13		

Each value is processed and the results are displayed in a grid which can then be sorted on, filtered, or exported as needed

For plugins that handle a key and a value, like the AppCompatCache plugin, the results of the plugin are displayed on a tab next to the Type viewer at the bottom part of the interface (below the values tab).

As an example, the 7-Zip archive history value is a NULL terminated list of archives opened in 7-Zip.

Type viewer																
	00	01	02	03	04	05	06	07	08	09	0A	OB	0C	0 D	0 E	
0000000	44	00	ЗA	00	5C	00	44	00	72	00	6Fl	20	70	00	62	D.:.∖.D.r.o.p.b
000000F	00	6F	00	78	00	5C	00	21	00	4 B	00	72	00	6F	00	. o. x. \. ! . K. r. o.
0000001E	6C	00	6C	00	5C	00	45	00	78	00	70	00	65	00	6 E	I.I.∖.E.x.p.e.n
0000002D	00	73	00	65	00	20	00	72	00	65	00	70	00	6F	00	.s.er.e.p.o.
000003C	72	00	74	00	73	00	5C	00	41	00	70	00	72	00	69	r.t.s.\.A.p.r.i
0000004B	00	6C	00	20	00	32	00	33	00	20	00	32	00	30	00	.12.32.0.
0000005A	31	00	36	00	5C	00	41	00	70	00	72	00	69	00	6C	1.6.∖.A.p.r.i.I
00000069	00	20	00	32	00	33	00	20	00	32	00	30	00	31	00	2. 3 2. 0. 1.
00000078	36		2 E	00		00	69	00	70	00	00	00	44		3A	6z.i.pD.:
00000087	00			6D	00	49	00	2 E	00	65	00	78	00	65	00	. \. m Ie. x. e.
00000096	00	00	43		3A				55		73	00	65		72	C.:.\.U.s.e.r
000000A5	00	73	00	5C	00	65		5C		44			00	73	00	. s. \. e. \. D. e. s.
000000B4	6 B	00	74		6F	00	70	00		00	46		_	00	4 F	k. t. o. p. \. F. R. O
000000C3	00	4D		20	00	68	00	69	00	74	00	73	00	20	00	. M h. i. t. s
000000D2	53	00	51	00	4C	00	2E		37	00	7A		00	00	43	S. Q. L 7. z C
000000E1	00	3A	00	5C	00	54	00	65	00	6D	00	70	00	5C		.:.\.T.e.mp.\.
000000F0	6F	00	73	00	54	00	72	00	69	00	61	00	67	00	65	o.s.T.r.i.a.g.e
000000FF	00	32	00	5 F	00	63	00	75	00	73	00	74	00	6F	00	. 2 c. u. s. t. o.
0000010E	6D	00	2 E	00	65	00	78	00	65	00	00	00				me.x.e
Current offset	t: (0 (Oxl	0)	Byte	s sel	ecte	d:	0 (O	x0)							Data interpreter ?

When this value is selected, the 7-Zip plugin processes the value and returns a much nicer list, like this:

Registry h	nives (2) Available bookmarks (29/0)				Values				
Key nan	ne	# values	Last write timestamp)rag a column head	der here to ara	oup by that column		
7			*		-	-			
⊿	SOFTWARE	1	2016-05-03 16:20:54		Value Name 🔺	Value Type	Data	Value Type Raw	Value Slack
	⊿ 💳 7-Zip	2	2015-12-30 19:25:46	1					
	⊿ Compression	5		•	ArcHistory	RegBinary	44-00-3A-00-5C-00		3 00-00
	⊿ Options	0	2016-04-29 16:26:17		Archiver	RegSz	zip		1 2C-39-29-0
	💳 7z	6	2016-04-29 16:26:17		EncryptHeade	RegDword	0		4
	iii zip	4	2016-04-29 16:26:17		Level	RegDword	5		4
	D 🔚 FM	10	2016-04-27 21:25:25		ShowPassword	+ gDword	1		4
	AccessData	0	2016-02-28 18:58:06						
	Angryziber	0	2016-01-04 23:11:08						
	AppDataLow	0	2015-11-17 20:06:41	1E	Type viewer 7-	-Zip archive his	tory		
	D Einary Fortress Software	0	2015-11-17 21:37:35	1Ľ.			1 1 1 1		
	🛛 🚞 Canneverbe Limited 🛛 🔓	0	2016-02-29 23:20:20)rag a column head	der here to gro	oup by that column		
	D 🔚 Citrix	0	2016-04-11 20:28:09		Archive Name				
	Clients	0	2015-11-18 15:09:11	9					
	CodeValue Ltd	0	2015-11-24 18:35:05		D:\Dropbox\!Kro	oll\Expense rep	ports\April 23 2016\April	23 2016.zip	
	Common	1	2015-11-17 21:38:00	TE	D:\mI.exe				
	ConEmu	11	2016-05-03 16:20:54		C: Users \e Des	kton/FROM hit	s SOL . 77)	
	Developer Express	0	2015-12-01 14:58:20		C:\Temp\osTriad		-		
	DevExpress	0	2015-11-25 20:48:49		- C: (remp los mag	gez_custom.e	xe		
	DJI Interprises	0	2015-12-30 16:50:59						
	Dropbox	0	2015-11-17 21:42:31						
	DropboxUpdate	0	2015-11-17 21:42:07						

Page 62 of 81 Last revised: 5/19/2017 8:36:46 AM The data returned can now be filtered, sorted, and exported as we saw earlier.

Some plugins can return a vast amount of information which can make displaying it all in a grid overwhelming. In these cases, Registry Explorer will, by default, hide the details from the plugin view (but this column can easily be unhidden if you like). As an example, let's look at the LastVisitedPidlMRULegacy plugin. When this key is selected, all values are processed and the results are displayed as we saw before. This plugin has a property named 'Details' which contains just that, a very detailed listing of information extracted from a value. When a value is selected a new tab is shown next to the Type viewer tab that contains the details of the selected value, like this:

	# values	Last write timestamp	Drag a column h	eader here to grou	up by that column		
ComDlg32	0	2015-11-18 00:21:50	Value Name	Mru Position	Executable	Absolute Path	Opened On
CIDSizeMRU	65	2016-05-03 16:41:26	?				
	79	2016-05-05 16:41:28	0	2	MozBackup.exe	Unmapped GUID:	
FirstFolder	17	2016-05-02 16:08:09				e31ea727-12ed-4702-820c-4b6445f28e1a	
ast//isitedDidMDU	26	2016-05-03 16:41:26	4	4	phpDesigner.exe	My Computer \U:	
LastVisitedPidlMRULeg		2010 03 03 10. 11.20	▶ 5	0	Wireshark.exe	dc\Host PCAP	4/29/2016 5:48:52 PM +00:00
OpenSavePidIMRU	0	2016-04-26 01:01:28	1	3	WinHex.exe	My	
Desktop	0	2015-11-17 20:08:26				Computer\C:\Temp\testdump\a52b0784bd6674	
Discardable	0	2015-11-17 20:06:41	Total rows: 6				Export
ExtractionWizard	1	2015-11-17 20:56:42	Turner	ComDie 22 LootVis	sitedPidlMRU selected ro	u datala	
FileExts	0	2016-04-29 16:34:25	Type viewer Type: Directory,		atedPlaimRO selected ro	w details	
HideDesktopIcons	0	2015-11-17 20:08:26	rype. Directory,	value, uc			
LogonStats	1	2015-11-17 20:06:41	Extension blocks)4)		
LowRegistry	0	2015-11-17 20:06:41	Long name: dc				
Map Network Drive MRU	4	2015-12-09 02:09:04		016 4:31:10 PM +(
MenuOrder	0	2015-11-17 20:06:41		9/2016 4:31:10 PM ence #: 86129/116			
MMStuckRects3	3	2015-11-17 21:38:03	File system hint:	NTFS			
Modules	0	2015-11-17 20:09:34					
MountPoints2	0	2016-05-02 16:02:11	Short name: dc				
OperationStatusManager	2	2016-03-21 20:18:31	Modified: 2/19/2	016 4:31:10 PM +	00:00		
Package Installation	1	2015-11-17 21:16:25					
RecentDocs	150	2016-05-03 16:45:21	Type: Directory,	Value: Host PCAP			
Ribbon	2	2015-11-17 20:09:12	Extension blocks				
RunMRU	0	2015-11-17 20:57:02	Long name: Host	Block 0 (Beef00) PCAP	14)		
SearchPlatform	0	2015-11-17 20:06:35	Created: 2/19/2	016 4:33:00 PM +0			
Shell Folders	31	2015-11-17 20:06:41		9/2016 4:33:00 PM ence #: 401605/10			
Shutdown	1	2016-04-25 17:08:12	File system hint:				
StartPage	3	2015-11-17 20:06:43					
StartupApproved	0	2015-11-17 21:46:36	Short name: HOS				
StreamMRU	3	2016-04-12 00:32:55 👻	Modified: 2/19/2	016 4:33:00 PM +	00:00		

This particular plugin decodes all of the shell items found in the binary data and places this decoded data into the Details property. This is what is displayed when a value is selected.

When exporting plugin results for plugins that have a Details property, this column will be exported as well, like

this:

Wo	rkbook View	5	Show	Zoom		Window	
4	• :	× 🗸	f _x				
A	В	С	D	E		F	
	eMru Position	Executable	Absolute Path	Opened Or		Details	
5	0	Wireshark.exe	dc\Host PCAP	4/29/2016 5:48:52	Extr Lon Cre Las: MFT File Sho Moo Typ Extr Lon Cre Las Las HFT File Sho	be: Directory, Value: dc tension blocks found: 1 	

The Details column seen in the Excel sheet above is the same that is available after unhiding the details column in Registry Explorer.

Creating plugins

To create a new plugin, download the RegistryPlugins project from Github, open the project in Visual Studio, and create a new project that follows the correct naming convention similar to what we saw earlier, RegistryPlugin.<something>. Once the project is created, add a reference to the RegistryPluginBase project as this project will contain the base types and classes needed for a plugin. Once this is done, the actual coding can begin. By default a generic class is created in the new project. Rename this to something more meaningful. This main class will contain the "brains" of the plugin. Next, add a new class to the project and call it ValuesOut. While you can name this class anything, most other plugins use this same convention.

The ValuesOut class defines the objects the plugin will return for display in Registry Explorer. For example, the 7-Zip plugins ValuesOut class looks like this:



The important things to remember is to add read only properties and define a constructor that allows for setting up the object. By doing this way we ensure our objects are immutable.

With the ValuesOut class done, we can code the primary class. Using the 7-Zip project as a reference again, lets take a look at the top section of the class:

```
namespace RegistryPlugin._7_ZipHistory
 —
           1 reference | Eric Zimmerman, 6 days ago | 1 author, 2 changes
! 🖻
           public class SevenZip : IRegistryPluginGrid
           Ł
               private readonly BindingList<ValuesOut> values;
               O references | Eric Zimmerman, 7 days ago | 1 author, 1 change
               public SevenZip()
 Ē
                    _values = new BindingList<ValuesOut>();
                    Errors = new List<string>();
                }
                16 references | Eric Zimmerman, 7 days ago | 1 author, 1 change
                public string InternalGuid => "6b1296a2-d3fb-441f-89c1-fd3706855acc";
                16 references | Eric Zimmerman, 7 days ago | 1 author, 1 change
                public List<string> KeyPaths => new List<string>(new[]
                {
                    @"Software\7-Zip\Compression"
               });
                17 references | Eric Zimmerman, 7 days ago | 1 author, 1 change
                public string ValueName => "ArcHistory";
                34 references | Eric Zimmerman, 7 days ago | 1 author, 1 change
                public string AlertMessage { get; private set; }
                16 references | Eric Zimmerman, 7 days ago | 1 author, 1 change
                public RegistryPluginType.PluginType PluginType => RegistryPluginType.PluginType.Grid;
                16 references | Eric Zimmerman, 7 days ago | 1 author, 1 change
                public string Author => "Eric Zimmerman";
                16 references | Eric Zimmerman, 7 days ago | 1 author, 1 change
                public string Email => "saericzimmerman@gmail.com";
                16 references | Eric Zimmerman, 7 days ago | 1 author, 1 change
                public string Phone => "501-313-3778";
                16 references | Eric Zimmerman, 7 days ago | 1 author, 1 change
                public string PluginName => "7-Zip archive history";
                21 references | Eric Zimmerman, 7 days ago | 1 author, 1 change
                                                                                                              Τ
                public string ShortDescription =>
                    "Extracts archive history from ArcHistory key"
                    ;
                16 references | Eric Zimmerman, 7 days ago | 1 author, 1 change
                public string LongDescription => ShortDescription;
               16 references | Eric Zimmerman, 7 days ago | 1 author, 1 change
                public double Version => 0.5;
               85 references | Eric Zimmerman, 7 days ago | 1 author, 1 change
               public List<string> Errors { get; }
```

1

i.

÷

1

1

ł

ł.

1

4

1

1

After the class name we can see a reference to an Interface, IRegistryPluginGrid. This interface contains the 'rules' the class must follow as it relates to properties. The interface definition looks like this:

```
namespace RegistryPluginBase.Interfaces
Ξ
   {
       16 references | EricZimmerman, 317 days ago | 1 author, 2 changes
       public interface IRegistryPluginGrid : IRegistryPluginBase
Ė
       {
           /// <summary>
           /// Gets the values after processing by a plugin.
           /// </summary>
           /// <remarks>The underlying class should extend ProcessedValue</remarks>
           /// <value>The values.</value>
           45 references | EricZimmerman, 318 days ago | 1 author, 1 change
           IBindingList Values { get; }
       }
   }
```

Which in turn references another interface, IRegistryPluginBase, that looks like this:

1 reference | Eric Zimmerman, 308 days ago | 2 authors, 5 changes public interface IRegistryPluginBase /// <summary> /// Gets the internal unique identifier. /// </summary> /// <remarks> 111 Set this to a static GUID value in plugin's constructor. This is used to make sure pluging aren't loaded more 111 than once. /// </remarks> /// <value>The internal unique identifier.</value> 16 references | Eric Zimmerman, 308 days ago | 2 authors, 2 changes string InternalGuid { get; } /// <summary> 111 The path to the key this plugin handles. /// </summary> /// <remarks>Do not include the root key in the key path</remarks> /// <value>The key path.</value> 16 references | Eric Zimmerman, 310 days ago | 1 author, 1 change List<string> KeyPaths { get; } /// <summary> /// The value name this plugin handles /// </summary> /// <value>The name of the value.</value> 17 references | EricZimmerman, 318 days ago | 1 author, 1 change string ValueName { get; } /// <summary> /// Gets the alert message. /// </summary> /// <remarks>Optional message to display to user (an interesting value, missing info, etc)</remarks> /// <value>The alert message.</value> 34 references | Eric Zimmerman, 308 days ago | 2 authors, 2 changes string AlertMessage { get; } 16 references | EricZimmerman, 317 days ago | 1 author, 2 changes RegistryPluginType.PluginType PluginType { get; } 16 references | EricZimmerman, 317 days ago | 1 author, 1 change string Author { get; } 16 references | EricZimmerman, 317 days ago | 1 author, 1 change string Email { get; } 16 references | EricZimmerman, 317 days ago | 1 author, 1 change string Phone { get; } 16 references | EricZimmerman, 317 days ago | 1 author, 1 change string PluginName { get; } 21 references | EricZimmerman, 317 days ago | 1 author, 1 change string ShortDescription { get; 16 references | EricZimmerman, 317 days ago | 1 author, 1 change string LongDescription { get; } 16 references | EricZimmerman, 317 days ago | 1 author, 1 change double Version { get; } 85 references | EricZimmerman, 317 days ago | 1 author, 1 change List<string> Errors { get; } /// <summary> Process raw values into plugin specific format 111 /// </summary> /// <remarks>This method should populate the 'Values' property for pluging implementing this interface</remarks> /// <param name="key">The key where inValues originated. Also contains all subkeys, values, etc</param> 25 references | Eric Zimmerman, 308 days ago | 1 author, 1 change void ProcessValues(RegistryKey key);

}

These interfaces define what properties must exist in a class that implements a given interface.

Looking back at our SevenZip class, we can see several of the properties from the interface definitions along with a few other fields and variables. First, we see a read-only collection named _values which will hold each of our ValueOut

Page 68 of 81 Last revised: 5/19/2017 8:36:46 AM

objects we create. Next is the constructor which initializes the class. The internal GUID is nothing more than a unique GUID that can be generated via the C# Interactive window (or any other means using Guid.NewGuid.ToString() method).

The next two properties define the key that this plugin is interested in and optionally, a value. This particular plugin does contain a value name and as such, a combination of the key name and value name is used.

The PluginType defines the how the resulting data from the plugin will be displayed. As of 0.8.0.0, Grid is the only valid option.

The Author, Email, and Phone properties contain information about who made the plugin and how to get a hold of them.

The PluginName, descriptions, and Version properties are next and are self-explanatory.

The Errors collection will contain a list of any errors encountered by the plugin as it processes a key and/or value.

The remaining part of the class looks like this:

```
85 references | Eric Zimmerman, / days ago | 1 author, 1 change
    public List<string> Errors { get; }
    25 references | Eric Zimmerman, 6 days ago | 1 author, 2 changes
    public void ProcessValues(RegistryKey key)
         values.Clear();
        Errors.Clear();
        try
        ł
             var arcHist = key.Values.SingleOrDefault(t => t.ValueName == "ArcHistory");
            if (arcHist != null)
                 var arcs = Encoding.Unicode.GetString(arcHist.ValueDataRaw).Split('\0');
                                                                 T
                 foreach (var arc in arcs)
                 {
                     if (arc.Trim().Length == 0)
                     {
                         continue;
                     }
                     var v = new ValuesOut(arc);
                     Values.Add(v);
                 }
            }
        }
        catch (Exception ex)
        {
             Errors.Add($"Error processing 7-Zip archive history: {ex.Message}");
        }
        if (Errors.Count > 0)
        {
            AlertMessage = "Errors detected. See Errors information in lower right corner of plugin window";
        }
    }
    public IBindingList Values => _values;
}
```

The ProcessValues function is called by Registry Explorer when it is determined a given key should be processed by a plugin. This is where a key should be looked at and processed into ValuesOut objects. It is very important to properly handle any possible errors by use or Try/Catch blocks. This keeps the plugin from crashing and allows for reporting errors to a user in a consistent manner.

The AlertMessage can be anything a plugin author wishes and will be displayed in Registry Explorer below the grid containing plugin results.

The Values property at the bottom is the property Registry Explorer will use to display the data returned by the plugin.

Creating plugins is very simple in that it is some basic plumbing code (name, email, key path, etc.) and a single function to process things. While this example showed a simple plugin, there are other, more complicated examples in the Github project you can use as templates for new plugins.

RECmd

RECmd is a command line tool used to access offline Registry hives. It includes many of the same features as Registry Explorer including searching, looking at keys and values, and exporting data.

RECmd uses the same back end as Registry Explorer to process Registry hives. RECmd is open source and the source code is available <u>here</u>.

Getting started

Running RECmd.exe without any arguments displays a list of command line options as shown below.

λ .\RECmd.exe	If you encounter an exception when running this application, see	15 3:05 PM
RECmd version 0.7.0.0		15 1:10 PM
Authors Enis Zimmung (acces		15 12:21 PM
Author: Eric Zimmerman (saeri https://github.com/EricZimmer		15 10:14 AM r
Note: Enclose all strings con	taining spaces (and all RegEx) with double quotes	
Hive Literal Recover Recursive RegEx Sort SuppressData	Hive to search. If present,sd andss search value will not be interpreted as ASCII or Unicode byte string If present, recover deleted keys/values Dump keys/values recursively (ignored ifValueName used). This option provides FULL details If present, treat <string> insk,sv,sd, andss as a regular expression If present, sort the output If present, do not show data when usingsd orss</string>	
KeyName ValueName SaveToName	Key name. All values under this key will be dumped Value name. Only this value will be dumped Saves ValueName value data in binary form to file	
StartDate EndDate MinSize sk sv sv sd ss	Start date to look for last write timestamps (UTC). If EndDate is not supplied, last writes AF End date to look for last write timestamps (UTC). If StartDate is not supplied, last writes BE Find values with data size >= MinSize (specified in bytes) Search for <string> in key names. Search for <string> in value names Search for <string> in value record's value data Search for <string> in value record's value slack</string></string></string></string>	
RECmd.exeHive "D: RECmd.exeHive "D: RECmd.exeHive "D:	\Temp\UsrClass 1.dat"sk URLRecover \temp\UsrClass 1.dat"StartDate "11/13/2014 15:35:01" \temp\UsrClass 1.dat"RegExsv "(App Display)Name" \temp\UsrClass 1.dat"StartDate "05/20/2014 19:00:00"EndDate "05/20/2014 23:59:59" \temp\UsrClass 1.dat"StartDate "05/20/2014 07:00:00 AM"EndDate "05/20/2014 07:59:59 PM"	

There are three groups of command line options for RECmd.

General

This category includes the Hive and Recover switches. Hive is always required.

- **Hive**: The full path to the hive to process. If the path contains spaces, include them in double quotes.
- Literal: If present, the --sd and --ss search value is not interpreted as ASCII and Unicode strings
- **Recover**: If present, recover deleted keys and values
- **Recursive**: If present, dump keys and values recursively from the key specified by KeyName. This option provides much more detail about keys and values.
- **RegEx**: If present, treat <string> in --sk, --sv, --sd, and -ss as a regular expression
- Sort: If present, sort the output in a meaningful way based on the type of data requested.

Page 71 of 81 Last revised: 5/19/2017 8:36:46 AM

Query

If either the key or value has spaces in them, be sure to enclose them in quotes.

When passing in key names, the root key name is optional. This is because most of the time you will not even know the root key name in order to be able to include it.

To get default values, use a value name of "(default)".

- **KeyName**: The key name to look for. If used without ValueName, displays all subkeys and values.
- ValueName: Display only the value specified
- SaveToName: Saves ValueName value data in binary form to a file

Search

This is a particularly useful feature to locate data across hives in key names, value names, and perhaps most importantly, in value data.

Searching is broken down into four types, by last write timestamp, value data minimum size, simple string searches (and regular expression (RegEx) based searches when –RegEx is present).

- StartDate: The earliest date to look for in Registry key last write timestamps. Timestamp should be in UTC.
- EndDate: The latest date to look for in Registry key last write timestamps. Timestamp should be in UTC.
- MinSize: Find values with value data size greater than or equal to the specified size (in bytes).
- sk: Search for <string> in key names
- sv: Search for <string> in value names
- **sd**: Search for <string> in value record's value data. The value data will be converted to its equivalent in ASCII and Unicode and also searched/compared to <string> unless the --Literal switch is used
- **ss**: Search for <string> in value record's value slack. The value slack will be converted to its equivalent in ASCII and Unicode and also searched/compared to <string> unless the --Literal switch is used

Simple searches

The two letter search options starting with 's' are string search options. These options look for matches via 'contains' logic rather than 'begins with' or similar. For example, if you search for 'cache', the following keys would match if they existed in the Registry hive:

- Muicache
- Cache items
- UnCAcHeD

Simple searches are not case sensitive.

To search for binary data in value data, simply string the hex characters you want to find together, separated by dashes (04-00-EF-BE for example).

```
D:\temp\RegistryExplorer\RECmd
  .\RECmd.exe --Hive "D:\temp\re\ALL\UsrClassDeletedBags.dat" --sd "04-00-EF-BE"
RECmd version 0.7.0.0
Author: Eric Zimmerman (saericzimmerman@gmail.com)
https://github.com/EricZimmerman/RECmd
Note: Enclose all strings containing spaces (and all RegEx) with double quotes
Processing hive 'D:\temp\re\ALL\UsrClassDeletedBags.dat'
Initial processing complete. Building tree...
Found root node! Getting subkeys...
Hive processing complete!
Flushing record lists...
Root key name: S-1-5-21-146151751-63468248-1215037915-1000 Classes
Key: Local Settings\Software\Microsoft\Windows\Shell\BagMRU\0\0, Value: 0, Data: 74-00-31
0-00-00-00-00-33-3F-D9-83-11-00-55-73-65-72-73-00-60-00-08-00-<mark>04-00-EF-BE</mark>-EE-3A-85-1A-33-3
73-00-65-00-72-00-73-00-00-00-40-00-73-00-68-00-65-00-6C-00-6C-00-33-00-32-00-2E-00-64-00-
C-00-6C-00-2C-00-2D-00-32-00-31-00-38-00-31-00-33-00-00-00-14-00-00-00
Found 1 value data hit
Search took 0.050 seconds
```

This allows you to find signatures for common data structures ANYWHERE in the Registry. The binary signature used above is that of a BEEF0004 extension block, commonly used in ShellBags. It contains information such as MAC dates/times, MFT info, etc.

When using the sd and ss switches, the value data or slack will be converted to its equivalent ASCII and Unicode representation from the raw bytes. For example, if you searched for Ask, three searches would actually happen:

- 1. For the Ask string itself
- 2. Raw data converted to ASCII string. A case insensitive search against this string is performed. If found, the position of the hit is used to extract the exact string that was hit on. This string is then converted back to bytes and reported as a hit.
- 3. Raw data converted to Unicode string. The rest happens as in step 2.

This allows string searches to find data regardless of encoding or case. If data is found in encoded form, the exact bytes making up the hit are highlighted. These bytes may differ from the searched for string if the capitalization was different.

If the --Literal switch is used with sd or ss, then only the first search is done behind the scenes. This allows you to look for specific byte patterns without RECmd interpreting raw data or slack to ASCII or Unicode.

Page 73 of 81 Last revised: 5/19/2017 8:36:46 AM

Regular expression searches

When the --RegEx switch is present, the search term used is treated as a regular expression. Regular expression searches offer much more powerful capabilities to find things at the cost of having to follow a more complex set of rules when building search terms. Another tradeoff is that it can be slower depending on how complicated your RegEx is.

Enclose the RegEx in quotes to make sure the shell does not try to interpret anything in there.

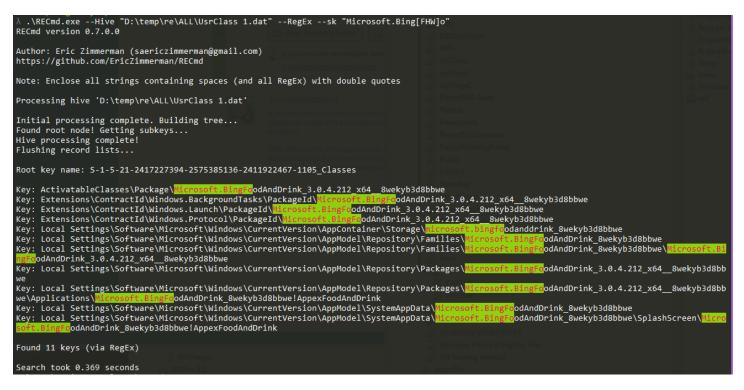
As with simple searches, regular expression based searches are case insensitive.

Regular Expression examples

Finding keys

To find all keys that contain 'Microsoft.Bing' followed by an F, H, or a W, then an o, use the following search:

RECmd.exe --Hive "D:\temp\re\UsrClass 1.dat" --RegEx --sk "Microsoft.Bing[FHW]o"



Finding values

To find all values with names that contain either 'AppName' or 'DisplayName', use the following search:

RECmd.exe --Hive "D:\temp\re\UsrClass 1.dat" --RegEx --sv "(App|Display)Name"

320 results were found in 0.380 seconds, but due to the length of the output, only the first few are shown below.

λ .\RECmd.exeHive "D:\temp\re\ALL\UsrClass 1.dat"RegExsv "(App Display)Nam RECmd version 0.7.0.0	ne", JeffRich
Author: Eric Zimmerman (saericzimmerman@gmail.com)	MD5 collision
https://github.com/EricZimmerman/RECmd	MP3
	osTClass
Note: Enclose all strings containing spaces (and all RegEx) with double quotes	osTriage1
Processing hive 'D:\temp\re\ALL\UsrClass 1.dat'	osTriage2
	PhotoDNA Code
Initial processing complete. Building tree Found root node! Getting subkeys	Photos
Hive processing complete!	Powerpoint
Flushing record lists	
Root key name: 5-1-5-21-2417227394-2575385136-2411922467-1105_Classes	ProjectWorkingFolder
<pre>Key: Extensions\ContractId\Windows.AppointmentsProvider.AddAppointment\PackageId\mi 3d8bbwe\ActivatableClassId\Microsoft.WindowsLive.Calendar.AppX8aw8zprmge6rpnpcf2pbb Key: Extensions\ContractId\Windows.AppointmentsProvider.RemoveAppointment\PackageId kyb3d8bbwe\ActivatableClassId\Microsoft.WindowsLive.Calendar.AppXMdsmbnj96vbbsrtjy2 Key: Extensions\ContractId\Windows.AppointmentsProvider.ReplaceAppointment\PackageId ekyb3d8bbwe\ActivatableClassId\Microsoft.WindowsLive.Calendar.AppXKaqyc69sy6we8d3wg Key: Extensions\ContractId\Windows.AppointmentsProvider.ShowTimeFrame\PackageId\micr d8bbwe\ActivatableClassId\Microsoft.WindowsLive.Calendar.AppXtp1qs1d9f5y8jbjjmhsq3c Key: Extensions\ContractId\Windows.BackgroundTasks\PackageId\Microsoft.BingFinance_ AppXt2b0qt8jwqketvnyx02s765gyw55jaq6.mca, Value: DisplayName Key: Extensions\ContractId\Windows.BackgroundTasks\PackageId\Microsoft.BingFinance_ rking.BackgroundTransfer.Internal.BackgroundTasks\PackageId\Microsoft.BingFinance_ rking.BackgroundTransfer.Internal.NetworkChangeTask.ClassId.1, Value: DisplayName Key: Extensions\ContractId\Windows.BackgroundTasks\PackageId\Microsoft.BingFinance_ rking.ContentPrefetcher.Internal.ContentPrefetcherTask.ClassId.1, Value: DisplayName</pre>	<pre>>5xb4tm2kwee.wwa, Value: DisplayName Nmicrosoft.windowscommunicationsapps_17.5.96 Bk3k47cv542vte.wwa, Value: DisplayName d\microsoft.windowscommunicationsapps_17.5.9 gez35dkc33h4dhmw.wwa, Value: DisplayName rosoft.windowscommunicationsapps_17.5.9600.2 g4kqg3fsqr.wwa, Value: DisplayName 3.0.4.212_x648wekyb3d8bbwe\ActivatableClas ame 3.0.4.212_x648wekyb3d8bbwe\ActivatableClas ame 3.0.4.212_x648wekyb3d8bbwe\ActivatableClas 3.0.4.212_x648wekyb3d8bbwe\ActivatableClas 3.0.4.212_x648wekyb3d8bbwe\ActivatableClas</pre>

Finding data

To find all values whose data contains 'URL:bing' followed by either an m, h, or s, use the following search:

RECmd.exe --Hive "D:\temp\re\UsrClass 1.dat" --RegEx --sd "URL:bing[mhs]"

```
λ .\RECmd.exe --Hive "D:\temp\re\ALL\UsrClass 1.dat" --RegEx --sd "URL:bing[mhs]"
RECmd version 0.7.0.0
Author: Eric Zimmerman (saericzimmerman@gmail.com)
https://github.com/EricZimmerman/RECmd
Note: Enclose all strings containing spaces (and all RegEx) with double quotes
Processing hive 'D:\temp\re\ALL\UsrClass 1.dat'
Initial processing complete. Building tree...
Found root node! Getting subkeys...
Hive processing complete!
Flushing record lists...
Root key name: S-1-5-21-2417227394-2575385136-2411922467-1105_Classes
Key: binghealthnfitness, Value: (default), Data: URL:binghealthnfitness
Key: bingmaps, Value: (default), Data: URL:bingmaps
Key: bingsports, Value: (default), Data: URL:bingsports
Found 3 value data hits (via RegEx)
Search took 0.494 seconds
```

For more examples, run RECmd.exe without any command line arguments.

All regular expressions must of course be valid .net regular expressions. Different flavors of RegEx providers allow for different syntax, so be sure to use the proper syntax.

RegEx tutorials for .net.

https://msdn.microsoft.com/en-us/library/az24scfc%28v=vs.110%29.aspx

http://regexhero.net/reference/

https://msdn.microsoft.com/en-us/library/hs600312%28v=vs.110%29.aspx

http://www.codeproject.com/Articles/9099/The-Minute-Regex-Tutorial

http://www.systemtextregularexpressions.com/help

RegExBuddy is an awesome tool for building and testing RegEx against data sets.

Page 76 of 81 Last revised: 5/19/2017 8:36:46 AM

Version changes

Version 0.9.0.0

NEW: Added Raw Value property to non-RegBinary values that contains the bytes that make up the value. This is useful for copying out into other programs like DCode, etc.

NEW: Plugins added for Known networks (SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList), WordWheelQuery, TypedURLs (including TypedURLsTime), Services, Terminal services client (RDP history), DHCPNetworkHint, NEW: Added Options | Convert selected | To ROT-13 in Find window. This allows for searching for things ROT-13 encoded like UserAssist, etc without having to rely on a plugin NEW: Added '# subkeys' column to Registry Hives and Available bookmarks trees NEW: Added 'Selected hive' to left side of status bar that tracks the name of the hive currently selected. Double clicking copies full path of hive to clipboard NEW: More bookmarks NEW: Add indicator for 'Deleted' in search results NEW: Added 'Data interpreter' option to Values context menu. This allows you to view and decode the raw value data in a wide variety of formats (integer to EPOCH date, etc.) NEW: Much better filtering options in trees and grid including Excel like filtering **NEW: Updated controls** NEW: Holding CTRL while right clicking a node in Registry hives tree will automatically expand all child nodes (saves time over using context menu) NEW: Project support added. You can now create projects based on currently loaded hives and reload projects as needed

NEW: Add File | Unload all hives option

NEW: More data interpreter conversions

CHANGE: Allow for cell selection vs entire rows in Values grid

CHANGE: Allow for scrollbar on tree so all columns can be seen

CHANGE: User created bookmarks now show up in the Available bookmarks tab in Blue (bold) font to differentiate them from Common bookmarks

CHANGE: Absolute path to active Registry hive is now prepended to Key path on Copy via context menu in trees and to Value summary in Values grid

CHANGE: Add group membership and password hints to SAM plugin

FIX: Plugins updated based on test data

FIX: Save Datetime format and load it on subsequent starts

FIX: Bug fixes

Version 0.8.1.0

NEW: Change to .net 4.6

NEW: Added exporting of values to Excel, TSV, PDF, and HTML via key context menu (under Export | Values). Data is exported exactly as shown in Values grid (this lets you hide columns, reorder, sort, etc. before export) NEW: Plugin support added.

NEW: Added View | Plugins to explore available plugins

NEW: Added Base64 to data interpreter under Strings section

NEW: Added Tools | Preferences

NEW: Option to show (and therefore export) RegBinary values as Base64 strings (enabled in Tools | Preferences)

Page 77 of 81 Last revised: 5/19/2017 8:36:46 AM

NEW: Option to show (and therefore export) value slack as Base64 strings (enabled in Tools | Preferences)

NEW: Option to set custom date/time format for timestamps

NEW: For RegUnknown value type, show the actual value of the Registry Type in hex and decimal.

NEW: Ability to double click offset in hex viewers to jump to the offset in either decimal or hex

NEW: When a plugin is added for a key or value, make it the active tab

NEW: Hex viewer allows for selecting bytes and copying as hex, ANSI string (Windows 1252 code page), or Unicode string

NEW: When exporting value data, offer exporting in binary or string format

NEW: Allow for searching for many terms at once vs one at a time in Find dialog

NEW: Change messages count background color to yellow when there are warning messages and red when there are error messages. This color will be cleared when the Messages window is viewed.

CHANGE: Disable Bookmarks menu when on Available bookmarks tab

CHANGE: Clear any active filters before selecting bookmarked key

CHANGE: Set focus to last used search type on Find form

CHANGE: Sort bookmarks by name

CHANGE: Load hives when they do not have an nk record with a HiveRootEntry flag set. When this happens, an alternate method is used to find the root key

CHANGE: Put the newest search history items at the top of the list

CHANGE: Don't trust Header length when looking for hbins as sometimes Header length is wrong

CHANGE: Values grid filters use 'contains' vs 'starts with' as default

FIX: Add missing tooltip to Literal checkbox on Find form

FIX: Update hex position in hex type viewer when moving up and down rows vs only left and right

FIX: Correct issue when selecting hits in Find panel if the Registry keys tree was sorted when a virtual key existed (Associated Registry keys for example)

FIX: Handle rare issue when building virtual keys for 'Associated deleted records' where there is an active key and a recovered deleted key with the same name

FIX: Lots of tweaks and miscellaneous fixes

Version 0.7.1.0

RECmd changes

New: Added --Dir switch. This recursively searches for hives in a given directory and searches each of them

Registry Explorer changes

New: Registry Explorer can now function as a "default application" in that you can associate RE with *.dat and then double click hives. This also allows for setting up RE in other apps like X-Ways as an external viewer, dragging and dropping hives onto RE shortcut/executable, etc.

New: Added Check for updates to About menu

Version 0.7.0.0

As of 0.7.0.0, Registry Explorer and RECmd are included together.

RECmd changes

NEW: Added –Literal switch. When present, --sd and --ss switches will not be interpreted NEW: Added --ss switch for searching Value slack space

Page 78 of 81 Last revised: 5/19/2017 8:36:46 AM

NEW: Search terms are now highlighted in search results. Edit nlog.config to adjust colors for foreground and background

NEW: Added --RegEx switch. When present, treat <string> in --sk, --sv, --sd, and --ss as a regular expression NEW: If nlog.config is missing, add default config and warn user

CHANGE: Switches are NOT case sensitive any more CHANGE: Remove RegEx specific switches (See --RegEx above) CHANGE: Tweak command line option descriptions CHANGE: Updated nlog

See <u>here</u> for changes in version 0.6.1.0.

Registry Explorer changes

This version is pretty much a complete rewrite under the hood. This was done to address performance issues due to initial (bad) design decisions.

Hive processing is fully asynchronous, but very large hives can take a few seconds to display once the hive is loaded. This is due to the need to load all

NEW: Full support for searching including key names, value names, and value data, both with simple searches and RegEx. Searching based on last write timestamps is supported as well

NEW: Fully asynchronous loading of hives which keeps the GUI responsive, even when loading 100+ MB hives (I am looking at you SOFTWARE hive)

NEW: Tech details hex editors now update with offset and selection length when bytes are selected

NEW: Added value context menu to copy value summary (a combination of name, type, and data), name, type, data, and slack to clipboard

NEW: Add value context menu to export data and slack to a file

NEW: Settings for things persist

NEW: Search strings are remembered and autopopulate when typing on the Find form. Use the Tools menu to clear NEW: Added Convert | To hex ASCII and To hex Unicode to Find. This allows you to look for encoded strings in value data without having to manually convert strings to hex

NEW: Allow deleting of user created bookmarks in Bookmark Manager via Ctrl-Delete

NEW: Added context menu to Available bookmarks (Copy, expand/collapse, tech details) that work the same as the 'Registry hives' context menu options

NEW: Added 'Jump to key' context menu item on Available bookmarks tab that will select the hive's key on the 'Registry hives' tab

NEW: More hot keys added to main/context menus

NEW: Added 'Root key name' to Tech details | Hive details properties and strip root key from Tech details window title to save space

NEW: Added Export 'Registry hive' menu to File menu. This exports the tree exactly as it is shown to the selected format NEW: Enable/disable expand/collapse subkey options depending on the expanded state of the selected key

NEW: Save positions of vertical and horizontal splitters

NEW: Trees and grids all save settings (sorting, filtering, conditional formatting rules) between sessions NEW: Save size of main form

NEW: Improved hex editor control for RegBinary keys. Added offset, selection length, and data interpreter

NEW: Added 'Show associated deleted records' and 'Show unassociated deleted records' to Options menu

NEW: Added 'Slack viewer' tab for values that have slack space

NEW: Added 'Show parent keys when filtering' to options menu. Turning this OFF shows only the keys that match the filter. When ON, parent keys to keys matching the filter are also shown

Page 79 of 81 Last revised: 5/19/2017 8:36:46 AM

NEW: Added a Total messages counter to lower status bar (far right) that indicates the total number of messages available on the Messages form

NEW: Added skinning support. Active skin can be changed from the Options menu

NEW: Added icon for Registry hive in the Registry hives tree to visually separate it from keys

NEW: Make hive name bold to make it stand out from keys

NEW: Tech details info can be copied via Ctrl+C (just the value) or Ctrl+Alt+C (Name: Value)

NEW: All hex viewers now support Ctrl+C to copy selected bytes to clipboard

NEW: Search for minimum value sizes added

NEW: Search in value slack added

CHANGE: Allow resizing of window below 800x600

CHANGE: Drag and dropping of hives supported on any of the 3 main sections of Registry Explorer

CHANGE: Status bars adjusted. Added options to hold Shift when double clicking in order to copy different parts of the key/value

CHANGE: Add vertical scroll bar to Technical details hex editors

CHANGE: Rename tree context menus from 'child nodes' to 'subkeys'

CHANGE: Hide Messages form by default since things load and process faster when its hidden

CHANGE: Icon for existing key placeholder in Associated deleted records updated

CHANGE: Icon for Associated deleted records updated

CHANGE: Made legend icons bigger

CHANGE: Bookmarks manager now allows editing/deleted both common and user created bookmarks

FIX: Bug fixes in Registry parser (yay unit tests)

FIX: Show SK record in Technical details form

Version 0.2.0.0

NEW: Added new tab in upper left, Available bookmarks, that shows all available bookmarks across all loaded Registry hives

NEW: Added 'Technical details' option to context menu. Use this to view all the down and dirty details about a key including its bytes, its security key, subkeys, values, etc. This provides an easy to use way to explore and validate Registry tools

NEW: Added several hotkeys for commonly used key context menu items

NEW: Allow exporting of keys either individually or recursively to .reg format via the context menu

NEW: Add 'Collapse all hives' button to status bar.

NEW: Added more bookmarks

CHANGE: Prevent illegal file name characters in category names (\, /, |, and so on). Any illegal characters will be replaced with an underscore

CHANGE: Nlog logging added

CHANGE: Registry parsing is now ~150% faster and memory usage reduced by 40-80%

CHANGE: Prevent the same hive from being loaded more than once

CHANGE: Expand the top level node after loading a hive

CHANGE: Hide or unhide all matching keys in all open hives vs only the active hive

FIX: When removing keys from auto hide list, remove any hidden keys in the tree that match as well

FIX: Actually export the timestamp when exporting Messages

FIX: GUI polish

Appendix A – Contributors

The following people have contributed in one way or another during the development and refinement of SBE

- SA/FE Devon P. Ackerman <u>devon.ackerman@ic.fbi.gov</u>, <u>sadevonackerman@gmail.com</u>
- David Cowen @HECFBlog
- Dan Pullega @4n6k
- Jerod Alexander @jerod
- Willi Ballenthin @williballenthin

Appendix B – Additional resources

- <u>http://binaryforay.blogspot.com/</u>: Contains detailed postings on the internal workings of the Registry
- <u>https://github.com/EricZimmerman/Registry</u>: Source code for the back-end parser used in Registry Explorer
- <u>https://github.com/EricZimmerman/RECmd</u>: Source code for RECmd
- <u>https://github.com/EricZimmerman/RegistryPlugins</u>: Source code for all Registry Explorer plugins