Windows Forensic Analysis

Dedicated to incident response and computer forensic analysis topics, with respect to Windows 2000, XP, 2003, and Vista operating systems

Registry Analysis

Registry analysis has long been an overlooked and underutilized tool in the forensic examiner's toolkit. Some think it's too difficult, too time consuming, and that the cost of having to figure out what to look for and how to extract it is simply not worth what you get back in return.

What if you could change that? What if you could fire up a tool that would automatically extract the information you needed? What if there was an application available that would marry up a Registry Viewer with a spreadsheet or checklist of pertinent Registry keys and values, *and* handle the translation of binary and other non-ASCII (i.e., binary encoded, ROT-13 encrypted, etc.) data? What if you could select a file and push a button, and within seconds have an easy-to-read report of Registry keys and values at your fingertips and ready for inclusion into your report?

Note: The RegRipper is ***NOT*** intended for use on live hive files. RegRipper is intended for use on hive files extracted from acquired images, or hive files accessed by mounting the image as a file system, as with Mount Image Pro. If you do not currently have any hive files available for "testing", consider downloading FTK Imager from AccessData's site and using that to extract a hive file or two from your live system.

Just such a tool is now available. Read on.

What is the RegRipper?

The Registry Ripper, or RegRipper for short, is *not* a Registry hive file viewer. There are plenty of Registry viewers out there already, some from commercial forensic analysis application vendors (Technology Pathways, EnCase, AccessData) and others available for free (RegEdit.exe, the Registry File Viewer). Who needs another one?

The RegRipper is an open-source application for extracting, correlating, and displaying specific information from Registry hive files from the Windows NT (2000, XP, 2003, Vista) family of operating systems. Not all information within Registry hive files is pertinent or even of interest to forensic examiners. However, some information is extremely valuable to the forensic examiner…recently accessed files and applications, application most-recently-used (MRU) lists, etc. RegRipper extracts this information, along with timestamp information from Registry keys (as well as values whose data contains timestamp information) and displays it in a text file for easy viewing, as well as inclusion into reports.

RegRipper provides a GUI interface for extracting specific information from a Registry hive file, defined through the use of plugins. The extracted information is printed in a text-based report file (for easy viewing, analysis, and inclusion into reports), and the RegRipper also generates a log file of its own activities. The location of the report file can be defined by the user, and the log file is created in the same

directory as the RegRipper EXE and DLL files.

Note: This document describes the Basic edition of RegRipper. The Advanced edition will include a separate text file containing timstamped information, which will be able to be imported into Excel, or parsed and imported into other applications, such as the Simile Timeline[1] application available from MIT. The Advanced version will also have other capabilities, as well.

The RegRipper consists of an EXE file, a DLL, and a plugins directory, as illustrated in figure 1.

Figure 1

As is further illustrated in figure 1, the Perl source code for RegRipper is also included, along with the Perl runtime DLL and the EXE file.

Note: The EXE and DLL file must be located in the same directory. The "plugins" directory must be in the same directory as the other two files, as well.

The plugins directory contains the plugins file and the plugins themselves, as illustrated in figure 2.

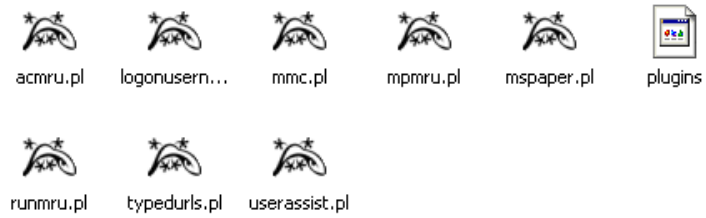

Figure 2

Note: The plugins illustrated in figure 2 are not a complete list of plugins, only a representative sample.

The plugins directory is hard-coded into the RegRipper application. The plugins file contains a listing of each plugin to be run, listed in the order that the examiner wishes the plugins to run. The examiner can easily modify the plugins file, as it is a flat text file containing the names of each plugin to be run on one line. RegRipper parses the plugins file, skipping blank lines and any line beginning with "#" (in Perl, this indicates a comment line). Example content of the plugins file appears as follows:

```
logonusername
acmru
runmru
typedurls
userassist
```

The above listing from a plugins file tells the RegRipper to run the logonusername.pl plugin, followed by the acmru.pl, runmru.pl, typedurls.pl and userassist.pl plugins. The output from each of these plugins is printed to the report file.

Again, the order and number of plugins to be run is configurable by the examiner. The plugins will be run regardless of the sequence in which they are listed, but they must be listed in the

[1] http://simile.mit.edu/timeline/

plugins file, and they must be a Perl script with a .pl extension.

Note: All plugin files must be located in the plugins directory along with the plugins file itself. Again, the examiner can control the plugins run against the selected hive file simply by manually editing the plugins file itself.

Running RegRipper

RegRipper can be launched in the same manner as any other Windows application. The examiner can begin by simply double-clicking the rr.exe file icon in Windows Explorer. Launching the GUI, the examiner will see the initial interface with two selection text fields and a report text field, as illustrated in figure 3.

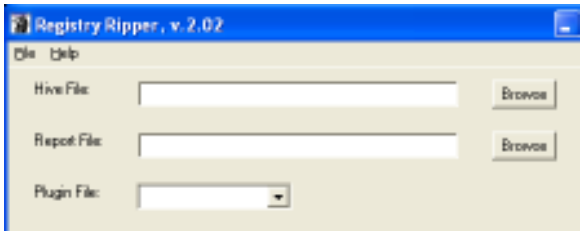

Figure 3

The first text field in the RegRipper GUI is labeled "Hive File", and is the text field in which the examiner must identify the Registry hive file to be parsed. The examiner can select a specific hive file to parse by either typing the complete path to the file into the text field, or by clicking on the first "Browse" button, navigating to the appropriate location, and selecting the file in question. The examiner must then enter the location for the report file into the second text field, or click on the second "Browse" button to select an output directory for the report file, as well as a file name, as illustrated in figure 4.

Figure 4

Note that in figure 4, a file extension is not required. The examiner simply enters the name of the report file, without any extension (.txt, etc.). The file extension is auto-populated by RegRipper. As with the "Hive File" text field, the examiner can also either type or paste in the path and filename for the report file.

Note: Once the examiner has selected a location for the report file, RegRipper will automatically use that same location and file name (changing the extension to ".log") for the log file of its own activities. As such, if the examiner opts to save the report file as a file named "Case006-B", RegRipper will automatically append the ".txt" extension for the report file, and then create "Case006-B.log" as the log file.

Many of the plugins currently deployed with RegRipper are intended for use with NTUSER.DAT files, user Registry hive files located in the user's profile directory on a Windows system. However, other plugins are also available for the System, Software, and Security hive files. The "Plugin File"

ComboBox allows the examiner to select which plugin file to be run against the selected hive file, as illustrated in Figure 5.

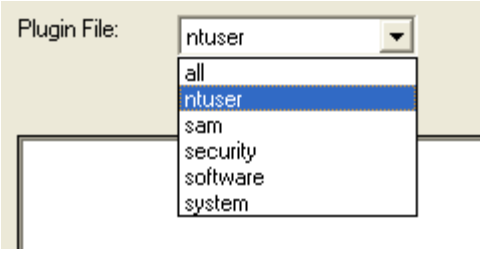

Figure 5

Once all fields have been populated, the examiner simply clicks the "Rip It!" button and RegRipper loads and runs each plugin, in order, and each plugin extracts specific information from the Registry hive file and writes it to the report file. Again, RegRipper maintains a log of its own activity, which uses the same file name as the report file, in the same path, except with the ".log" extension. Figure 6 illustrates the RegRipper after it has completed all of its plugins.

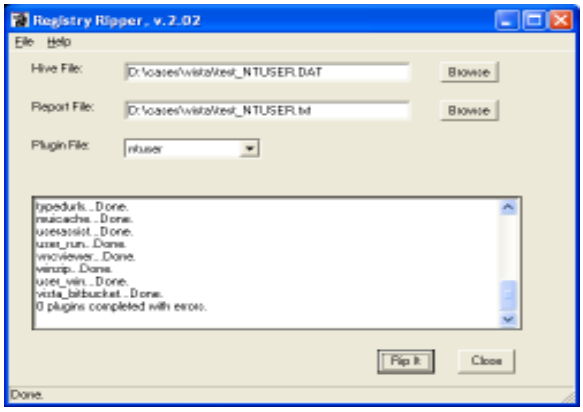

Figure 6

An excerpt from the report file generated by RegRipper appears a follows:

```
---------------------------------------
ACMru - Search Assistant
Software\Microsoft\Search Assistant\ACMru
LastWrite Time Mon Sep 26 23:02:08 2005
(UTC)
5603 [Mon Sep 26 23:32:56 2005 (UTC)]
   000 -> port*
   001 -> sol.exe
   002 -> hacker*
   003 -> hack*
   004 -> lad*

5604 [Mon Sep 26 23:33:30 2005 (UTC)]
   000 -> disk
   001 -> ha*

---------------------------------------
RunMru
Software\Microsoft\Windows\CurrentVersion
\Explorer\RunMRU
LastWrite Time Mon Sep 26 23:37:29 2005
(UTC)
MRUList = aedcb
a  iexplore\1
b  notepad\1
c  cmd\1
d  regedit\1
e  d:\bintext\1
---------------------------------------
TypedURLs
Software\Microsoft\Internet
Explorer\TypedURLs
LastWrite Time Mon Sep 26 23:16:24 2005
(UTC)
 url1 -> http://www.google.com/
 url2 -> http://movies.yahoo.com/
 url3 -> http://www.sysinternals.com/
 url4 -> http://www.heysoft.de/
 url5 -> http://www.careerbuilder.com/
 url6 -> http://www.monster.com/
 url7                                    ->
http://www.microsoft.com/isapi/redir.dll?prd=
ie&pver=6&ar=msnhome
---------------------------------------
Media Player - RecentFileList
Software\Microsoft\MediaPlayer\Player\Rec
entFileList
LastWrite Time Mon Sep 26 23:22:59 2005
(UTC)
 File0      ->      C:\Documents      and
Settings\jdoe\My      Documents\Morpheus
Shared\Downloads\
          Shania Twain - Man! I Feel Like A
Woman.mpg
 File1      ->      C:\Documents      and
Settings\jdoe\My      Documents\Morpheus
Shared\Downloads\
          Toby Keith - Stays In Mexico.mp3
```

The RegRipper utilizes plugins that automatically parse the UserAssist keys, MUICache values, etc. There is no limit to the information that the RegRipper can extract from a Registry hive file, or how it can be displayed and presented. Plugins can be written to extract specific values from a hive file, as well as correlate multiple values from multiple locations with a hive file.

Note: All timestamps displayed by RegRipper are in Universal Coordinated Time, or UTC format.

Plugins Files

The plugins files used by RegRipper are simply configuration files that tell RegRipper which plugins to run and in which order. These files co-exist within the same directory as the plugins themselves and do not have an extension. Lines of the plugin file that are to be skipped (i.e., comments, etc.) need only to start with "#"…RegRipper will ignore the rest of the line.

When the examiner launches RegRipper, the tool accesses the plugins directory and locates all files in the directory that do not have an extension. This list of files is then used to populate the plugins list combobox, as illustrated in figure 5 above. The examiner can create custom plugins files for various cases or types of cases, looking for specific items or Registry entries. Leaving these plugins files in the plugins directory will cause them to be added to the list of possible plugins files to be run whenever RegRipper is launched. RegRipper makes no modifications to the Registry on the examiner's system and does not maintain a list of plugins that have been available or run.

Creating your own plugin file is as easy as opening Notepad or any other text editor. Simply open any of the available plugins files in the editor of your choice to view the contents…the structure of the file is extremely simple and straightforward. The following section that discusses rip.exe can be used to collect information regarding available plugins.

Rip.exe

Rip.exe is an extremely useful command line interface (CLI) utility that ships with RegRipper. Rip allows the examiner to:

- List all available plugins, each with brief descriptive information (flat text or .csv format)
- Run a single plugin against a hive file
- Run a plugin file against a hive file
- Determine the type of hive file (experimental)

All of rip.exe's output goes to STDOUT, or the console. No report or log file is created when using rip.exe. To see all of rip.exe's syntax options, as well as examples, simply type any of the following at the command prompt:

```
C:\>rip
C:\>rip –h
C:\>rip /?
```

Note: To use rip.exe to create your own plugin file, type the following command at the command prompt:

```
C:\>rip –l –c > plugins.csv
```

When the command completes, open the resulting .csv file in Excel. The output has four columns, giving the plugin name, version, hive file, and a brief

description. Sort the results based on the "Hive" column, providing a list of plugins based on the hives for which each is intended. Highlight the desired plugins in "Plugin" column, cut them, and then paste them into a plugin file (opened in Notepad or any other text editor). Be sure to add comments (lines that start with "#") to the plugin file in order to note information about who created the plugin file, when it was created, etc.

What's to come in RegRipper?

Future versions of RegRipper will include the following functionality:

- More plugins!
- Descriptions, references, and analysis tips built into the plugins themselves, to be included in the report file
- Output of time-based information for timeline analysis (with utilities to import that data into other formats, such as Excel, Timeline, etc.)
- Greater support for hive files from 64-bit Windows XP/2003, as well as Vista and Windows 2008

Questions, comments, and requests for plugins should be directed to the author, H. Carvey at keydet89 [at] yahoo [dot] com. If specific plugins are requested, please consider providing sample hive files for testing.