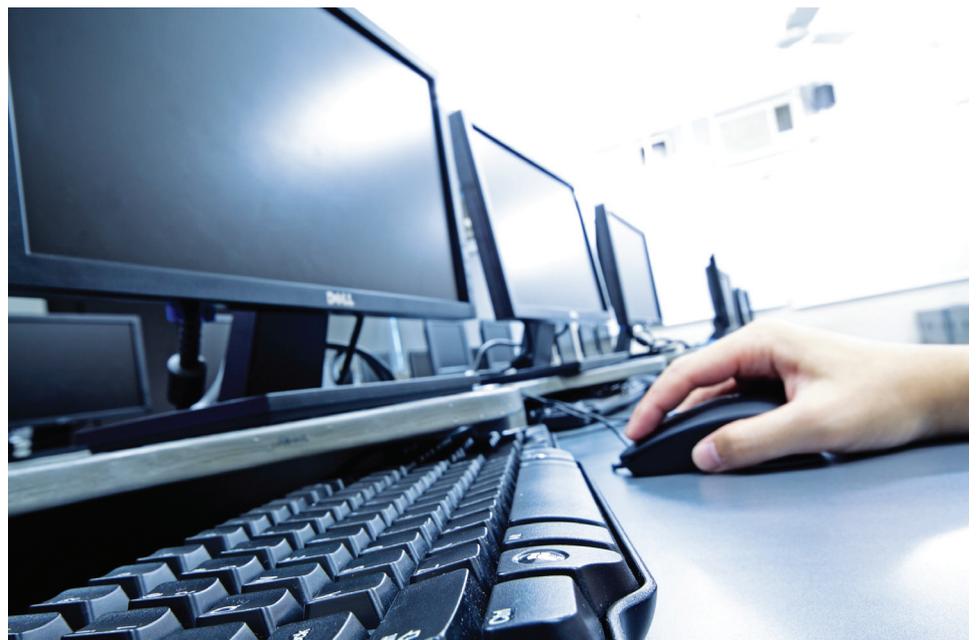


Registry Decoder

Version R2 (Live) & 1.2 (Offline)

EVALUATION REPORT

August 2012





NIJ Electronic Crime Technology Center of Excellence
550 Marshall St., Suite B
Phillipsburg, NJ 08865
www.ECTCoE.org

NIJ ECTCOE TESTING AND EVALUATION PROJECT STAFF

Robert J. O'Leary, CFCE; DFCP
Russell Yawn, CFCE
Chester Hosmer
Mark Davis, Ph.D.

Michael Terminelli, ACE
Randy Becker, CFCE
Jacob Fonseca

Victor Fay-Wolfe, Ph.D.
Kristen McCooey, CCE; ACE
Laurie Ann O'Leary

Table of Contents

Introduction	1
Overview	3
Product Information	3
Test Bed Configuration	5
Evaluation and Testing of Registry Decoder	7
Download and Configuration	7
Test – Registry Decoder Live.....	7
Test – Registry Decoder Offline on Image Files	12
Test – Copied Registry Files.....	14
Test – File Copied Using EnCase®	15
Conclusion	17

This report is current at the time of writing. Please be sure to check the vendor website for the latest version and updates.

Introduction

The National Institute of Justice (NIJ) Electronic Crime Technology Center of Excellence (ECTCoE) has been assigned the responsibility of conducting electronic crime and digital evidence tool, technology and training testing and evaluations in support of the NIJ Research, Development, Testing and Evaluation (RDT&E) process.

The NIJ RDT&E process helps ensure that NIJ's research portfolios are aligned to best address the technology needs of the criminal justice community. The rigorous process has five phases:

- **Phase I: Determine technology needs principally in partnership with the Law Enforcement and Corrections Technology Advisory Council (LECTAC) and the appropriate Technology Working Group (TWG).** NIJ identifies criminal justice practitioners' functional requirements for new tools and technologies. (For more information on LECTAC and the TWGs, visit <http://www.justnet.org>.)
- **Phase II: Develop technology program plans to address those needs.** NIJ creates a multiyear research program to address the needs identified in Phase I. One of the first steps is to determine whether products that meet those needs currently exist or whether they must be developed. If a solution is already available, Phases II and III are not necessary, and NIJ moves directly to demonstration, testing and evaluation in Phase IV. If solutions do not currently exist, they are solicited through annual, competitively awarded science and technology solicitations and TWG members help review the applications.
- **Phase III: Develop solutions.** Appropriate solicitations are developed and grantees are selected through an open, competitive, peer-reviewed

process. After grants are awarded, the grantee and the NIJ program manager then work collaboratively to develop the solutions.

- **Phase IV: Demonstrate, test, evaluate and adopt potential solutions into practice.** A potential solution is tested to determine how well it addresses the intended functional requirement. NIJ then works with first-adopting agencies to facilitate the introduction of the solution into practice. After adoption, the solution's impact on practice is evaluated. During the testing and evaluation process, performance standards and guides are developed (as appropriate) to ensure safety and effectiveness; not all new solutions will require the publication of new standards or guides.
- **Phase V: Build capacity and conduct outreach to ensure that the new tool or technology benefits practitioners.** NIJ publishes guides and standards and provides technology assistance to second adopters.¹

The High Priority Criminal Justice Technology Needs are organized into five functional areas:

- Protecting the Public.
- Ensuring Officer Safety.
- Confirming the Guilty and Protecting the Innocent.
- Improving the Efficiency of Justice.
- Enabling Informed Decision-Making.

The NIJ ECTCoE tool, technology and training evaluation and testing reports support the NIJ RDT&E process, which addresses high priority needs for criminal justice technology.

¹ *National Institute of Justice High-Priority Criminal Justice Technology Needs*, March 2009 NCJ 225375.

Overview

Product Information

From the Registry Decoder Website:

Registry Decoder is a tool that automates the acquisition and analysis of registry files. There are two components of this tool: an online tool that collects files from a running machine, and an offline tool that performs some preprocessing and then allows analysis. This document contains the official instructions for the online component. For information about the offline component, please see:

<http://www.registrydecoder.com> or

<http://code.google.com/p/registrydecoder/>.

The current version of Registry Decoder Live (RDL) is able to acquire the current registry files, as well as the historical registry files from the 32- and 64-bit versions of Windows XP, Vista and Windows 7.

To acquire the currently in-use registry files, RDL leverages the Sleuth Kit to read them from underneath the file system, thereby bypassing locking mechanisms.

Historical files are gathered on XP through the System Restore facility and on Vista and Windows 7 through interaction with the Volume Shadow Service. The acquisition of historical data ensures that as much evidence as possible is acquired for analysis.

Test Bed Configuration

The following four computers were used as a test bed to the evaluation of the Registry Decoder program. These four computers represent what most likely would be encountered by a computer forensic examiner.

- A Samsung laptop computer running Windows 7 on a 600 gigabyte hard drive. Below are the details of this computer.

Windows edition	
Windows 7 Home Premium	
Copyright © 2009 Microsoft Corporation. All rights reserved.	
Service Pack 1	
System	
Manufacturer:	Samsung Electronics
Processor:	Intel(R) Core(TM) i5 CPU M 460 @ 2.53GHz 2.53 GHz
Installed memory (RAM):	4.00 GB (3.79 GB usable)
System type:	64-bit Operating System
Pen and Touch:	No Pen or Touch Input is available for this Display

- A shop-built desktop computer running Windows 7 on a 1 terabyte hard drive. Below are the details of this computer.

Windows edition	
Windows 7 Professional	
Copyright © 2009 Microsoft Corporation. All rights reserved.	
System	
Processor:	AMD Phenom(tm) II X4 925 Processor 2.80 GHz
Installed memory (RAM):	8.00 GB (3.37 GB usable)
System type:	32-bit Operating System
Pen and Touch:	No Pen or Touch Input is available for this Display

- A Dell laptop computer running Windows XP Media Center on an 80 gigabyte hard drive. Below are the details of this computer.



System:

Microsoft Windows XP
Media Center Edition
Version 2002
Service Pack 3

Manufactured and supported by:



Dell Inspiron MXC061
Intel(R) Core(TM)2 CPU
T 7200 @ 2.00GHz
1.99 GHz, 1.99 GB of RAM
Physical Address Extension

- A shop-built desktop computer running Windows XP Professional on a 1 terabyte hard drive. Below are the details of this computer.



System:

Microsoft Windows XP
Professional
Version 2002
Service Pack 3

Computer:

AMD Athlon(tm) 64 X2 Dual
Core Processor 3800+
2.01 GHz, 2.00 GB of RAM
Physical Address Extension

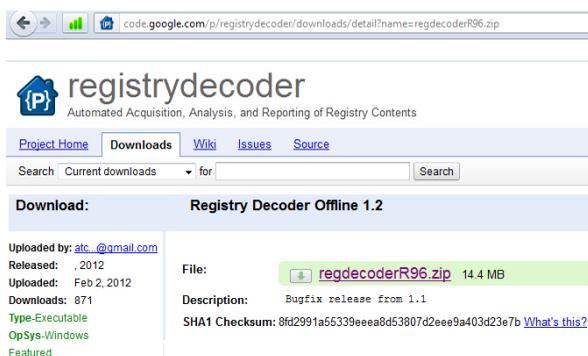
Evaluation and Testing of Registry Decoder

Download and Configuration

On 4/5/2012, the below-listed files were downloaded from the website <http://code.google.com/p/regdecoderlive/downloads/> and used for testing live acquisition of the Registry.



On 4/5/2012, the below-listed file was downloaded from the website <http://code.google.com/p/registrydecoder/downloads/> and used for testing the offline analysis program.



Test – Registry Decoder Live

The live version of Registry Decoder (REGDECODER-LIVE.EXE) was copied to a USB thumb drive. This

thumb drive was then inserted into each of the above-mentioned computers. Note that a new folder was created on the thumb drive before inserting into the target computer. Registry Decoder was configured to acquire both current and backup copies of the registries.

Registry Decoder successfully acquired registries from all of the computers. The only issue encountered was on the Dell laptop. Registry Decoder produced an error message and stopped working when both current and backup registries were selected; however, acquisition was successful when only the current registry was selected.

Inspection of the target system after Registry Decoder's live acquisition program was run revealed several files related to the Registry Decoder program that had been created and deleted, and other files whose last access dates were updated. This disk and file activity is expected when running a live program, and even inserting the thumb drive into the computer causes system files to be accessed and updated. Close analysis of the file activity that occurred while running Registry Decoder Live revealed that no user-created data was affected.

It appears that the amount of data written to disk during the running of Registry Decoder amounted to approximately 29 megabytes. This amount of data is written to unallocated disk space on the target system, possibly overwriting previously deleted, and maybe recoverable, data.

The above-mentioned issues are going to be present anytime a 'live' forensic program is going to be used. The examiner needs to weigh the pros and cons of conducting any type of live data acquisition or any other live triage tool. The smaller the footprint a live tool leaves on a system, the better, and the footprint of Registry Decoder can be considered small when

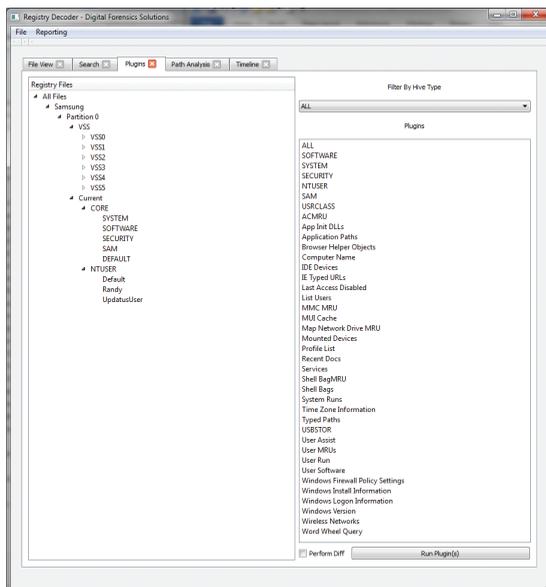
compared to the potential value of the evidence that may be located.

If an investigator decides against using the Registry Decoder Live program, there is still the option of shutting the system down, obtaining a forensic image of the system, and then using the Registry Decoder Offline program to extract the registry information from the forensic image.

Test – Registry Decoder Offline

This test uses the information gathered in the above live acquisition. To perform this test, the following steps were performed:

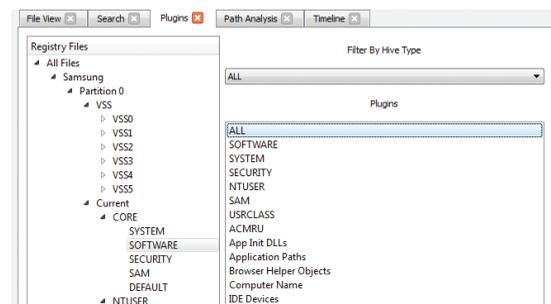
1. The offline version of Registry Decoder (REGDECODER.EXE) was run from the computer designated to conduct analysis.
2. The image below depicts using the ‘Plugins’ feature of the program. Note the expanded Registry Tree and the number of backup registries reported via the Volume Shadow Copy Services (VSS). In this case, there are six backup copies (numbered 0 through 5), as well as the current registry. Note that when using dd image files as a source, only one backup registry is acquired.



3. Once the above-shown registry hives were presented, analysis of various registry keys was quite easy. Registry Decoder has ‘plugins’ that can be selected and allow the user to decide which keys to analyze and the depth of the analysis. The various plugins are shown below.

- | | |
|------------------------|----------------------------------|
| ALL | Profile List |
| SOFTWARE | Recent Docs |
| SYSTEM | Services |
| SECURITY | Shell BagMRU |
| NTUSER | Shell Bags |
| SAM | System Runs |
| USRCLASS | Time Zone Information |
| ACMRU | Typed Paths |
| App Init DLLs | USBSTOR |
| Application Paths | User Assist |
| Browser Helper Objects | User MRUs |
| Computer Name | User Run |
| IDE Devices | User Software |
| IE Typed URLs | Windows Firewall Policy Settings |
| Last Access Disabled | Windows Install Information |
| List Users | Windows Logon Information |
| MMC MRU | Windows Version |
| MUI Cache | Wireless Networks |
| Map Network Drive MRU | Word Wheel Query |
| Mounted Devices | |

4. The availability of the plugins allows the user to choose different levels of examinations to be conducted. In this example, it was chosen to apply “ALL” plugins to the CURRENT\CORE\ SOFTWARE key.



5. The results of running the All-Software plugin are multiple tabs across the top of the window; each tab being a particular registry key.



The reported keys [the tabs] were:

- App Init DLLS.
- Application Paths.
- Browser Helper Objects.
- Profile List.
- System Runs.
- Windows Install Information.
- Windows Logon Information.
- Windows Version.
- Wireless Networks.

6. Obtaining information from a particular registry key is done by clicking on one of the tabs. Shown below is what was presented when clicking on the “Windows Version” tab. Note that the Windows Version could have been obtained by choosing only the “Windows Version” plugin and not selecting the ‘All’ option.

1	InstallDate	2010/11/06 13:46:47.000000
2	ProductName	Windows 7 Home Premium
3	CSDVersion	Service Pack 1

7. Choosing all plugins for the CURRENT\CORE\SYSTEM registry hive provided key information on the following:

- Windows Firewall Policy Settings.
- IDE Devices.
- Last Access Disabled.
- Mounted Devices.
- Services.
- Time Zone Information.
- USBSTOR.

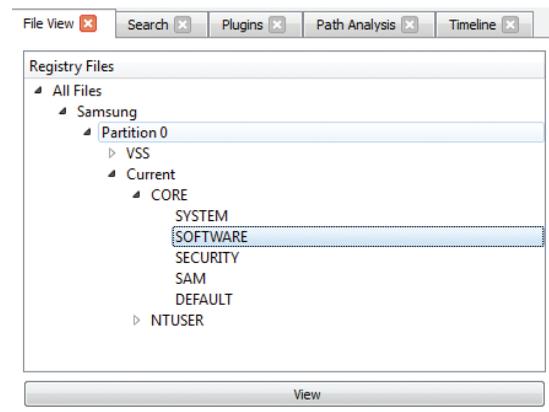
8. Registry Decoder provides a means to browse the Registry Hive. See the following excerpt from the program documentation:

Hive browsing performs functions similar to tools such as regedit or Access Data’s Registry Viewer®. To browse a file, simply choose it within the presented evidence tree and click “View.”

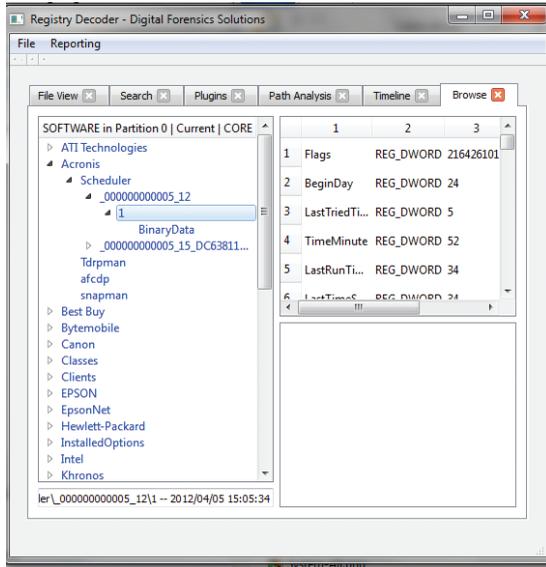
The automatically generated Browse tab presents an interface similar to that of other registry hive browsers. The left pane shows the hive keys as a tree. When a key is chosen, its full path within the registry and last written time are placed in the label at the bottom of the form. Data from this form can be copy/pasted, but not edited. The right panes show the keys, names and data for the chosen key. These columns can be sorted. When a value is clicked in the right page, a hexdump of its contents will be shown in the bottom right table.

To instantly check if a path exists in a file, and jump to it if it exists, right click in any place on the tree and enter the path you wish to check. If it exists, the tree will be repositioned at that location. DO NOT include the “root” of the tree when searching, such as “\$\$\$PROTO.HIV” for XP hives.

9. Shown below is preparing to ‘Browse’ the contents of the Current\Software hive, and once these options are selected, the ‘View’ button is clicked.



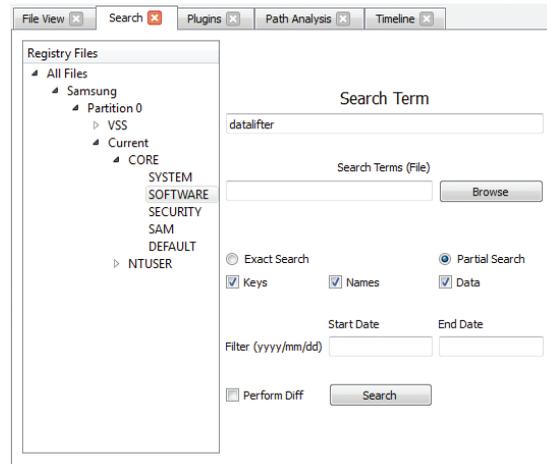
10. After clicking the ‘View’ button, a new tab “Browse” appeared. Shown below is the presentation after opening one of the keys. This is an easy method for browsing the registry hive.



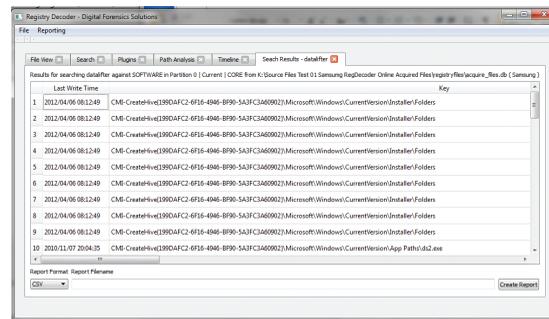
11. Registry Decoder provides a means to search within the Registry. See the following excerpt from the program documentation:

This tab allows for searching of data contained within the analyzed hives. Files can be selected using the same methods as the Hive View. Individual search terms may be entered in the input box under “Search Term,” or a newline delimited file of search terms may be uploaded using the “Browse” button.

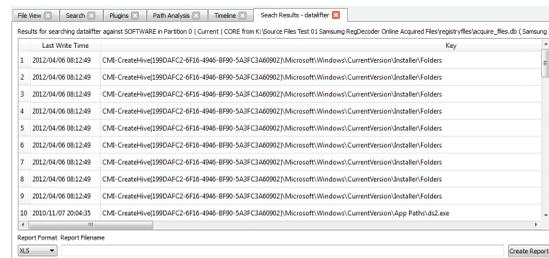
12. Shown below is preparing to ‘Search’ the contents of the Current\Software hive for the string “data-lifter.” It was known ahead of time that there were programs associated with this name installed on the system, so this character string was chosen to see what results would be returned.



13. After clicking the ‘Search’ button, a new tab, “Search Results – datalifter,” appeared. Shown below is the presentation after clicking on this newly created tab. Each one of these keys has data associated with the various Datalifter programs that were installed on this computer.



14. There is a feature that allows for ‘saving out’ this information into a file. Note at the bottom left of the previous image a dropdown button that allows for the choice of a report format: CSV, HTML, PDF or XLS. In this test the XLS format was chosen as well as the path and file name for the report.



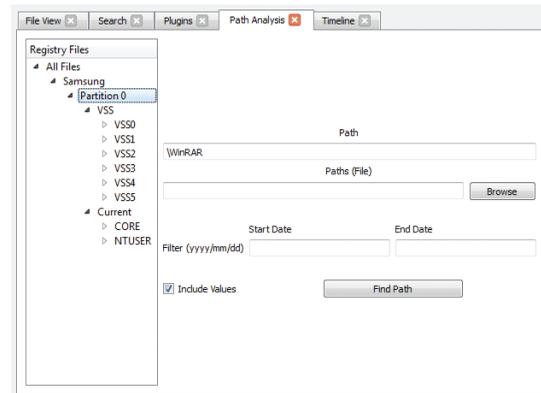
15. After the 'Create Report' button was clicked, a message window popped open stating "Report Successfully Created." Reviewing the XLS file revealed the data was present and an investigator could then conduct whatever analysis of the data that was necessary.
16. Registry Decoder provides a means to conduct path-based analysis. See the following excerpt from the program documentation:

The path analysis form allows for determining if specific path(s) are within investigated registry files. It also allows exporting of information about paths along with their name/value pairs. This information is very useful in a number of situations, such as:

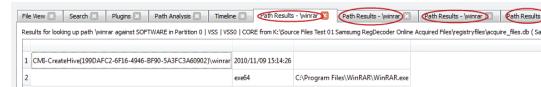
- Showing that malware was or wasn't installed.
- Showing if certain applications were installed and their corresponding parameters.
- Exporting and analyzing data not covered by a plugin.

To use this form, simply choose the registry files of interest and enter either a path to search or a newline-separated file with a list of paths. Results can be filtered by the key's last write time through using either the Start Date and/or End Date fields. The "Include Values" checkbox controls whether or not key/value pairs are included in the results and report.

17. Shown below is the dialog window for starting a 'Path Analysis' looking for evidence of the WinRAR program. Note that it was known ahead of time that the WinRAR program was installed on this system and that the application path included "\WinRAR" (without the quotes and not case sensitive). It was chosen to start the path analysis at Partition 0 so all backups and the current registry hives will be searched, and no date range limits were used.



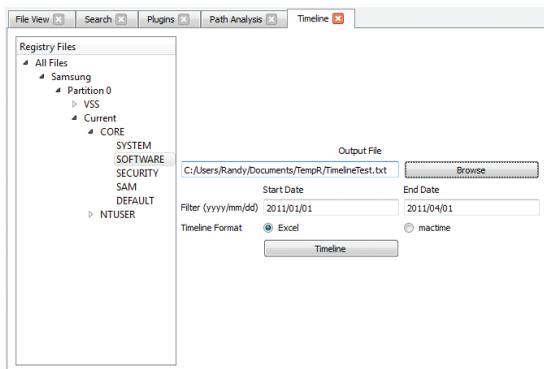
18. Shown below is just a partial listing of the results. A new tab was presented for each search hit and not shown in the image below is that there were a total of seven tabs, one for each backup and one for the current registry. Note the first tab reports an associated key found in VSS0. From an investigator's point of view, had the WinRAR program been installed at some point between the first backup registry and the current registry, then that could have been determined.



19. Registry Decoder provides a means to conduct timeline analysis. See the following excerpt from the program documentation:

The Timeline tabs allows for timelining of hives based on the last write time of keys. Keys can be filtered by using the Start Date and/or End Date fields. This analysis does not generate a result and instead writes directly to an output file as regtime.pl by Harlan Carvey. The output file can be then be used in conjunction with the Sleuthkit suite of timelining tools.

20. Shown below is getting ready to 'Timeline' the contents of the Current\Software key for the date range 1/1/2011 to 4/1/2011. Note that the Excel timeline format option was chosen.



21. The created file was then imported into Excel. A large number of entries, 1,447, were pulled from this key for the time period requested. This data would allow an investigator to analyze activity, as maintained by the Registry, on the computer during this time period.

Test – Registry Decoder Offline on Image Files

In real-world examinations, a computer forensic examiner works with previously acquired forensic evidence files (forensic images) that can be in various formats. Most likely these forensic images are in a dd format or E01 format that is used by Guidance Software's Encase™ program. These forensic images can consist of a single file or they can be broken into segments.

There are other ways to obtain the Registry information from a computer, such as, using AccessData's FTK Imager™ to obtain the 'protected files' from a live system, or using a forensic program, such as Forensic Toolkit™ (FTK), Encase™, or X-Ways Forensics™ to 'copy out' of the forensic image the files that represent the Registry.

This portion of the testing focuses on the following types of noncompressed forensic images:

- DD Image files (both single & segmented).
- Encase E01 files (both single & segmented).

DD image files

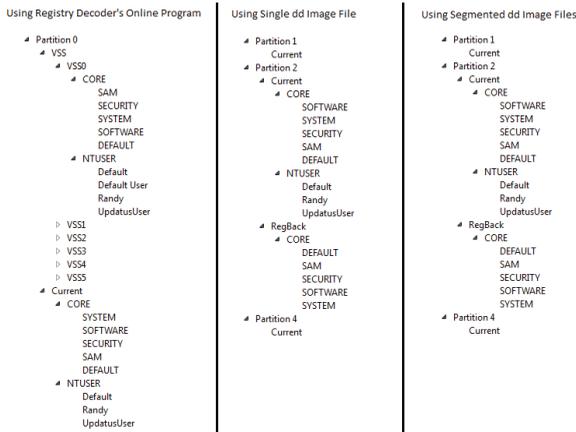
A popular image file format that many computer forensic programs can recognize is the dd format, also known as a bit-stream image. Registry decoder is advertised as being able to recognize dd images and acquire from them the registry information. Prior to this testing, both a single dd image file and a set of segmented dd image files were obtained from the above-mentioned Samsung laptop computer using AccessData's FTK Imager™ version 3.0 program. The segmented dd image consisted of 407 files.

For this test, Registry Decoder's option to 'create a new case' using both the single dd image file and the segmented dd images were performed. The results were the same when using both the single and segmented dd image files.

When selecting the dd images as the source, Registry Decoder allows the user to select either current, backup or both registries to extract from the dd image files. In this test both were selected.

Shown below is a comparison of the Registry Trees that Registry Decoder presented when using the different source files: (1) data acquired using Registry Decoder's live program, (2) single dd Image file and (3) segmented dd Image files. The dd images provided the current and one backup registry, but when using the data acquired by Registry Decoder's live program, provided were the current and six backup registries: Volume Shadow Services (VSS) zero through five.

Analysis of the below-listed registry hives (all from the same computer) provided similar and expected results.



Name	Size
registryfiles	
caseinfo.db	2 KB
caseobj.pickle	80,568 KB
evidence_database.db	7 KB
namedata.db	2,800 KB
stringtable.db	90,100 KB
treenodes.db	14,924 KB

Encase E01 image files

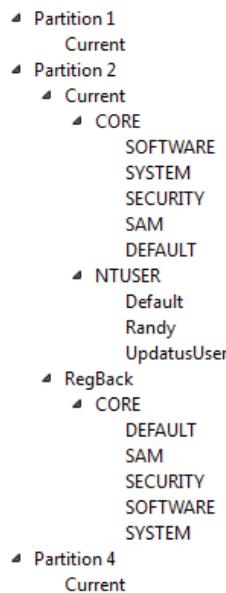
Another popular image file format that many computer forensic programs can recognize is Guidance Software’s Encase™ E01 format. Registry Decoder is advertised as being able to recognize E01 images and acquire from them the registry information. Prior to this testing, both a single E01 file and segmented E01 image files were obtained from the above-mentioned Samsung laptop computer using AccessData’s FTK Imager™ version 3.0 program. The segmented E01 image consisted of 408 files.

For this test, Registry Decoder’s option to ‘create a new case’ using both the single E01 image file and the segmented E01 images were performed.

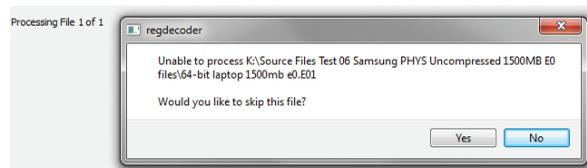
When using Registry Decoder to ‘create a new case’ using a single E01 image file, the processing appeared to be going well until a pop-up window appeared with an error message. The only option to close the pop-up window also closed the program.

It was noted that the folders assigned by Registry Decoder to hold the extracted data did in fact appear to contain data.

Since this folder/file structure appeared to contain quite a bit, Registry Decoder was run again, but this time requested to ‘Load an Existing Case,’ and it was pointed at the above case folder. The case loaded and the below-shown Registry Hive Tree was provided, and the data contained therein was consistent with the registry information.



When using Registry Decoder to ‘create a new case’ using segmented E01 image files, the program presented a pop-up window soon after starting with a message that the first file could not be processed. The result was Registry Decoder not being able to process segmented E01 image files.



The vendor was contacted about the problems encountered with the E01 image files, and they advised there were known issues with the E01 image files and that they were working on a fix. They also advised that Guidance Software is soon to change the format of the E01 files, and that format is not yet known.

Test – Copied Registry Files

There are additional methods to obtain Registry files from a computer, such as:

- Use FTK Imager™ to obtain the ‘Protected Files’ from a live system.
- Use the forensic tool such as Encase™, FTK™ or X-Ways Forensics™ to locate and copy out the files that make up the Registry.
- Using protected files obtained with AccessData’s© FTK Imager program.

This test used AccessData’s FTK Imager version™ 3.0 program to copy out the protected files from the Samsung laptop, a live acquisition process. The files that were obtained in this process are shown below. Note that FTK Imager did not obtain the backup registry files but did acquire the following Registry Hives:

- Users.
- All Users.
- Default.
- Default User.
- Public.
- Randy.
- UpdatusUser.
- Default.
- SAM.
- SECURITY.
- SOFTWARE.
- SYSTEM.

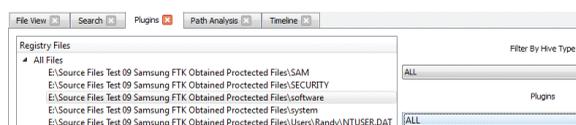
For the purpose of this testing, only the following registry files were selected for analysis by Registry Decoder’s offline program:

- Users\Randy\ NTUSER.DAT.
- SAM.
- SECURITY.
- SOFTWARE
- SYSTEM.

Registry Decoder presented the following registry files. Note the paths and file names were chosen by the evaluators.

```
Registry Files
├─ All Files
│   E:\Source Files Test 09 Samsung FTK Obtained Protected Files\SAM
│   E:\Source Files Test 09 Samsung FTK Obtained Protected Files\SECURITY
│   E:\Source Files Test 09 Samsung FTK Obtained Protected Files\software
│   E:\Source Files Test 09 Samsung FTK Obtained Protected Files\system
│   E:\Source Files Test 09 Samsung FTK Obtained Protected Files\Users\Randy\NTUSER.DAT
```

Registry Decoder allows for selecting only one, multiple or all of the above-mentioned files. Shown below is preparing to search all plugins for just the “Software” hive.



Noted were the same results as mentioned above when using the source files obtained with Registry Decoder’s live program and when using the dd image files; the same tabs with registry key information. (Tabs listed below.)

- App Init DLLS.
- Application Paths.
- Browser Helper Objects.
- Profile List.
- System Runs.
- Windows Install Information.

- Windows Logon Information.
- Windows Version.
- Wireless Networks.

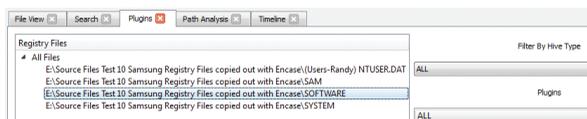
Test – File Copied Using EnCase[®]

This test was done by using the Encase[®] program to load the E0 image files for the Samsung laptop and then copy out the image from the following registry files for the user “Randy” and from the folder “windows\system32\config”:

- Randy\NTUSER.DAT.
- SAM.
- SOFTWARE.
- SYSTEM.

RegDecoder identified the following registry files. Note the paths and file names were chosen by the evaluators.

Registry Decoder allows for selecting only one, multiple or all of the above-mentioned files. Shown below is preparing to search all plugins for just the “Software” hive.



Noted were the same results as mentioned above when using the source files obtained with Registry Decoder’s live program and when using the dd image files; the same tabs with registry key information. (Tabs listed below.)

- App Init DLLS.
- Application Paths.
- Browser Helper Objects.
- Profile List.
- System Runs.
- Windows Install Information.
- Windows Logon Information.
- Windows Version.
- Wireless Networks.

Conclusion

The Registry Decoder program will fit nicely into a computer forensic examiner's toolbox. Registry Decoder provides a simple and easy method for acquiring current and backup copies of the registry hives from a running system, and it provided an easy, menu-driven and scalable (by choosing one or multiple menu options) method of examining a registry hives.

The Registry Decoder Program is not only a tool for examining a Windows registry hive from a computer system, but it also has the capability to examine multiple registries hives; registries from different computers. This capability to add registry hives from multiple computer systems allows an investigator to conduct registry searches, analysis and comparisons across all the computer systems.

The process used during the live acquisition testing was done by inserting a thumb drive (preconfigured with the live acquisition program and an empty folder for placing the acquired data) into an available USB port in the target system and running the live acquisition program. The data collected and placed onto the thumb drive can be copied to another location for analysis by Registry Decoder's offline program.

Registry Decoder's live acquisition program was tested against the following computer/operating systems:

- Windows 7 64-bit OS on a 32-bit processor.
- Windows 7 32-bit OS on a 64-bit processor.
- Window XP Professional.
- Windows XP Media Edition.

All tests were successful except when using the Windows XP Media system. In that case, Registry Decoder would not run when both options to acquire current and backup registries were selected. However,

when only the option to acquire the current registry was selected, the acquisition successfully completed.

Registry Decoder's offline program can read data from the following sources.

- The data obtained by its live acquisition program.
- Previously acquired forensic images of computer systems, i.e., dd image files.
 - Note that there were problems when using Encase E01 files as a source. The developer is aware of this problem and is working on a fix, but at the time of this testing the fix was not available.
- From files collected from a live system using AccessData's FTK Imager™ program.
- From files that make up the registry hives that were 'copied out' of a forensic image using a forensic program such as AccessData's Forensic Toolkit™ program or Guidance Software's Encase™ program.

Running Registry Decoder's Offline program using the data acquired with the Registry Decoder's live program provided access to more backup registries than using dd image files. Multiple backups of the registry were extracted from the data obtained by the live program, and only one backup extracted from the dd image files. From an investigator's point of view, having access to many backup registries could be useful when determining a particular chain of events regarding a particular issue.

Registry Decoder's Offline program provides the following options after loading the above-mentioned source files. Note that these option worked successfully and are discussed in detail in this report.

- Hive Browsing.
- Searching.

- Path Based Analysis.

- Timeline (choosing start and end dates).

Registry Decoder reported processing over 100,000 registry keys while processing the registry hive. Normally, a forensic examiner is going to be interested in certain keys to extract evidence pertinent to an investigation. Registry Decoder provides a means to search any portion of the hives (SYSTEM, SOFTWARE, NTUSER, etc.) for noncase-sensitive keywords. The ability to search for keywords is a real time saver.

Registry Decoder provides a means to print [export] the results of its processing. These results can be in CSV, HTML, PDF or XLS format. This feature could allow an examiner to provide registry information as an investigative case exhibit, or if processing multiple machines, to address link analysis type of issues.

Registry Decoder uses a ‘plug-in feature’ approach to allow an investigator to pull desired information from the registry with only a few mouse clicks. For example, it took just a few mouse clicks on easy-to-read menu options to obtain information from the “USBSTOR” subkey, historic information that a forensic examiner would be interested in. There are many important data of interest from a forensic examiner’s point of view that can easily be obtained with these minimal mouse clicks using the program’s plugins, such as, but not limited to:

- From the Software Key.

- Application Path (historic and current information).
- Profile Lists (user accounts).

- System Runs (startup programs).

- Windows Install Information (Registered Organization, Registered Owner and Product Name).

- Windows Version (install date and the OS version).

- Wireless Networks (historic information on wireless networks the computer has connected to).

- From the System Key.

- Recent IDE devices connected to the computer.

- Time zone setting.

- Recent USB devices mounted to the system.

- From the Core SAM Key.

- List Users (a list of user accounts).

- From the NTUSER Key (note that the following items may be different for each user account).

- IE Typed URLs.

- User MRUs.

- Recent Docs.

- User Assist (Program run as well as listing location of the program when run).

- User Run (Start up programs).

- User Software.

- Word Wheel Query (Keywords searched for by the user).