

# Registry Decoder

Instructions for Online Acquisition Component

Version 1.0

Date: 09/03/11

## 1. **Table of Contents**

2.	Introduction .....	3
3.	Obtaining Registry Decoder .....	3
4.	Obtaining Files from a Target Machine.....	3
5.	Current Limitations .....	4
	XP .....	4
	Vista/7 .....	4
	Server 2003/2008 .....	4
6.	Installation .....	4
7.	Reporting Bugs .....	4
8.	Contacting the Developers.....	5
9.	Future Developments .....	5

## 2. Introduction

Registry Decoder is a tool that attempts to automate 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 the pre-processing and analysis. This document contains the official instructions for the online component. For information about the offline component, please see <http://www.registrydecoder.com> and <http://code.google.com/p/registrydecoder/>.

The current version of Registry Decoder's online acquisition component is able to acquire the current registry set as well 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, Registry Decoder creates a System Restore Point on the target machine. This 'freezes' and generates a read-only backup of the current registry files. The acquisition component then locates these files and safely copies to external storage.

Historical files are gathered on XP through the System Restore facility and historical files are gathered 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.

Please read the following sections for detailed instructions on how to safely acquire files from a running machine with Registry Decoder.

## 3. Obtaining Registry Decoder

To obtain the offline analysis component of Registry Decoder, please see the instructions at: <http://code.google.com/p/regdecoderlive>.

This repository includes both the source code of the project as well as pyinstaller-based binaries, which can be run on any Windows machine that Registry Decoder supports.

## 4. Obtaining Files from a Target Machine

During a real investigation, it is recommended that investigators download the pyinstaller executable for the operating system architecture they are targeting (32 or 64 bit) and place this on a CD or USB drive. The executable can then be run directly from this medium without having to install software on the target machine.

The acquisition component is very simple and contains only one form. Investigators simply need to provide a description of the case, an empty directory in which to copy acquired files, and indicate which registry files should be acquired.

Note: For forensics soundness and to support best practices, the target directory should be either on an external drive or a network share. Writing to a drive on computer under investigation is strongly discouraged, but not specifically disallowed by the acquisition component.

Once the acquisition options are chosen, simply click the analysis button and wait for acquisition to complete. Acquired registry files will be written to the chosen output directory, along with a logfile that lists the selected options and acquired files as well as a SQLite database with information on each hive obtained. This directory can then be imported into the offline analysis tool.

**NOTE: For Vista/Windows 7 systems, the tool MUST be run with full administrator privileges (e.g. right click on the executable, choose 'Run as Administrator', and click 'Yes' on the UAC prompt) or the tool will be unable to collect any registry files.**

## 5. Current Limitations

### XP

Since the online acquisition tool relies on the System Restore facility to acquire registry files, we are unable to recover these files on systems with the facility disabled. Backup files may still be acquired though.

### Vista/7

Although strongly discouraged by Microsoft, it is possible to turn the Volume Shadow Service off on Vista/Windows 7 machines. If the Volume Shadow Service is disabled, Registry Decoder will be unable to acquire all possible registry files.

### Server 2003/2008

The server versions of Windows do not support System Restore Points, but they do support the Volume Shadow Service. We are currently exploring methods to acquire registry files from machines running these operating systems. The current version does not support acquisition from Server 2003/2008.

## 6. Installation

Although we strongly recommend using the supplied Pyinstaller binary for acquisition during real forensics scenarios, the online component has only minimal dependencies:

1. Python version 2.6 or 2.7
2. Python WMI (<http://timgolden.me.uk/python/wmi/index.html>)

Please note that due to WMI design, Python and the WMI library must be installed to match the architecture (32 or 64) of the target machine.

## 7. Reporting Bugs

To report a bug in the online acquisition component, please use our bug tracker at:

<http://code.google.com/p/regdecoderlive/issues/list>

or send email to [registrydecoder@digdeeply.com](mailto:registrydecoder@digdeeply.com).

## 8. **Contacting the Developers**

To contact the developers of Registry Decoder, please email [registrydecoder@digdeeply.com](mailto:registrydecoder@digdeeply.com).

## 9. **Future Developments**

To see the ongoing developments of Registry Decoder and the roadmap of future features please visit the project tracker at:

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