



Accurate, efficient analysis of the Windows registry

Registry Decoder Digital Forensics Software

Digital forensics deals with the analysis of artifacts on all types of digital devices. One of the most prevalent analysis techniques performed is that of the registry hives contained in Microsoft Windows operating systems. Registry Decoder was developed with the purpose of providing a single tool for the acquisition, analysis, and reporting of registry contents. To learn the history of this project, please see the [history](http://www.digitalforensicsolutions.com/registrydecoder/content/history) (<http://www.digitalforensicsolutions.com/registrydecoder/content/history>) page.

Registry Decoder is a free and open source tool. The online acquisition component can be accessed at: <http://code.google.com/p/regdecoderlive/> (<http://code.google.com/p/regdecoderlive/>) and the offline analysis component accessed at: <http://code.google.com/p/registrydecoder/> (<http://code.google.com/p/registrydecoder/>).

Our first blog post (<http://dfsforensics.blogspot.com/2011/09/announcig-registry-decoder.html> (<http://dfsforensics.blogspot.com/2011/09/announcig-registry-decoder.html>)) announced Registry Decoder and listed all of its features. The second blog post (<http://dfsforensics.blogspot.com/2011/11/registry-decoder-11-released.html> (<http://dfsforensics.blogspot.com/2011/11/registry-decoder-11-released.html>)) announced the release of version 1.1 along with its new features and updates.

All functionality contained within the two components is exposed to a graphical user interface, and the tool aims to provide even novice investigators with powerful analysis capabilities. Another goal of Registry Decoder is to become the project in which all future registry-related research is performed in and developed for. If you are a researcher and interested in open problems within forensics registry research or are interested in contributing the project, please see our research page [here](http://www.digitalforensicsolutions.com/registrydecoder/content/research-and-contributions) (<http://www.digitalforensicsolutions.com/registrydecoder/content/research-and-contributions>) .

To follow the latest developments of Registry Decoder please follow our Twitter account [@dfsforensics](https://www.twitter.com/dfsforensics) (<https://www.twitter.com/dfsforensics>) .

