D32 Tracking Computer Use With the Windows™ Registry Dataset (WiReD)

Douglas White, MS, National Institute of Standards and Ttechnology, 100 Bureau Drive Stop 8970, Gaithersburg, MD 20899-8970*

After attending this presentation, attendees will have a basic understanding of issues involving Windows™ Registry forensic investigation.

This presentation will impact the forensic community by presenting a rigorous procedure and data set to support investigation of Microsoft Windows(tm) computer systems.

The NIST Windows Registry Dataset (WiReD) contains the changes to the Windows™ Registry caused by application installation, de- installation, execution or other Registry modifying operations. The applications are chosen to be of interest to computer forensic examiners.

WiReD is currently an experimental prototype. NIST is soliciting feedback from the computer forensics community to improve and extend its usefulness.

There are two tools associated with the WiReD effort which will be discussed. One tool generates a XML-based difference between two Microsoft RegEdit-generated Registry patch files. The other tool creates the WiReD dataset from difference files generated from the XML. The tools are currently implemented in Ruby (1.8.4) and were tested in Mac OS X 10.4 (Tiger). Portability to other BSD-style operating systems will be discussed. Documentation for the tools and associated libraries will be provided.

Future directions of the WiReD prototype will be outlined. Limitations of using RegEdit to generate Registry dumps and handling problematic Registry entries will be discussed. The task and prioritization of identifying, acquiring and processing software for inclusion in the dataset will be discussed.

It is envisioned that the current prototype as only a small step in a much larger scheme that includes an XML database for managing the Registry difference files. This will allow for the efficient query and manipulation of acquired Registry data. Another goal is acquisition and cryptographic hashing of all files installed or modified by an application of interest. Expansion of Registry modification detection to beyond just application installation to include all phases of an application's life cycle on a given machine is the long term forensic information we seek.

Microsoft Windows, Registry, Registry Forensics

 ** Presenting Author*