ARSENAL RECON

REGISTRY RECON

Quick Start Guide

ATTENTION!

BEFORE INSTALLING REGISTRY RECON

You will need administrator rights on a Windows 7 or 8 system with Microsoft Visual C++ 2010 Redistributable and .NET Framework 4 packages installed.

INGESTING EVIDENCE

Disk Images

To search a disk image for Registry data (whether active, backed up, or deleted) go to the ***Evidence Menu, Add, Mount Forensic Image***, select an EnCase, DD, or VHD disk image, then ***Open***. Your evidence is now mounted and highlighted. Click ***Add***, give the evidence a name, click ***Ok*** to proceed, and your mounted evidence will be ingested.

Contents of a Directory

To ingest Registry hives which you have already exported from a disk image or elsewhere, go to the ***Evidence Menu, Add***, and select the ***Directory*** tab. Click the ***Include*** button to select a folder containing Registry hives to ingest. Registry hives found in subfolders will be ingested as well.

NAVIGATING REGISTRY RECON

In the ***Recon Registries pane***, the root of each item is the name you have assigned to each piece of evidence. Under your evidence name are the Registries associated with each unique Windows installation found in your evidence. Red values were not found in active Windows installations.

The ***Key History pane*** shows all occurrences of keys selected in the Recon Registries pane. Clicking the triangle at the left of a row shows more instances of that key and where it was found.

The ***Recon View pane*** is populated from the Recon Registries or Key History panes. Clicking the triangle at the left of a row shows the Value Instances pane. The ***Value Instances pane*** first displays all times associated with a value's parent key. Clicking the triangle at the left of a particular time will show all the locations the value at that time was found.

A variety of copy and spreadsheet-friendly export options are available by ***right-clicking*** in any pane. Data from the Key History and Value Instances panes can be verified by using information in the ***Source Path*** column.

OPENING PREVIOUSLY INGESTED EVIDENCE

Evidence successfully ingested by Registry Recon is saved in the database specified under the ***Tools Menu, Configuration***. To open previously ingested evidence, go to the ***Evidence Menu, Browse***, and select the name of your evidence.

TROUBLESHOOTING

Log files for processed evidence can be found, by default, under ***Program Files (x86)\Arsenal Recon\Registry Recon\OutputData***.

Please consult the User Manual included with the latest release of Registry Recon for further details.
Thank you for using Registry Recon!

Follow @ArsenalRecon

ARSENAL RECON

COMPUTER FORENSICS TOOLS BY COMPUTER FORENSICS EXPERTS