NUIX WORKBENCH REGRIPPER EXTENSION

Streamline your forensic investigation workflows

RegRipper is an open source tool that extracts forensic data from a target computer's Windows Registry, a valuable source of forensic evidence. This document provides detailed instructions on installing the RegRipper extension for Nuix Workbench. Using this extension, users can eliminate several steps from the digital forensic investigation and incident response workflows.

PREPARATION

Before you begin, complete the following steps.

1. Visit https://github.com/keydet89/RegRipper2.8 and download RegRipper to your local system
2. Extract the RegRipper archive to a folder
3. Visit https://github.com/NuixSDK/Reg-Ripper/releases and download the RegRipper extension for Workbench archive
4. Extract the three files in the archive to the Nuix Scripts folder. This is usually found at C:\Users\user\AppData\Roaming\Nuix\Scripts. However, your installation of Nuix might vary.

nuix

SETUP

This Workbench extension essentially "shells out" to RegRipper, launching it as an external tool and running it against exported hive files. It does so by using RegRipper's ability to run a "profile" of plugins; that is, rather than running a single plugin, you can run a series of plugins called a "profile." In RegRipper, a profile is a file with no file extension that contains a list of plugins to run.

As such, the default HiveProfileMap.json file that ships with the archive may not be suitable, and should be replaced with the following:

```
{
        "ntuser.dat": "ntuser",
        "default":"ntuser",
        "usrclass.dat": "usrclass",
        "security": "security",
        "software": "software",
        "sam": "sam",
        "system": "system",
        "amcache.hve": "amcache"
}
```

The contents of this file provide the hive-to-profile mapping used by the extensions script, and some of the profiles may not exist, or may need to be modified based on the needs of the individual examiner, in order to achieve optimal results.

For example, in the last line above you will notice a file named "amcache" was created in the RegRipper plugins folder. This file includes two lines: amcache, and del. Once the file is saved, it becomes a RegRipper profile and when used in conjunction with the RegRipper extension for Workbench, tells RegRipper to automatically run the "amcache.pl" and "del.pl" plugins against the AmCache.hve file.

> *Caution*
>
> The extension uses a mime-type search to locate the files in question, and as such, there can be issues. For example, on a Windows 10 test image, the user's USRCLASS.DAT file existed, but contained all zeros. On that same system, as well as on a Windows 2016 test image, the Registry hive files in the RegBack folder (i.e., "C:\Windows\system32\config\RegBack") existed but were zero bytes in size.
>
> Both of these conditions will result in the "hive" (quotes were used, as a file with all zeros, or a zero byte file, would not be considered a "hive" file) files not being exported or parsed.

REGISTRY HIVES

The extension attempts to locate, export, and parse the following Registry hive files:

1. C:\Windows\system32\config: SAM, Security, Software, System, Default
2. C:\Windows\system32\config\RegBack: SAM, Security, Software, System, Default
3. C:\Windows\system32\config\systemprofile; NTUSER.DAT
4. Every user profile (C:\Users\user, "C:\Documents and Settings\user"); NTUSER.DAT,
    a. Windows Vista and above: C:\Users\user\AppData\Roaming\Microsoft\Windows\USRCLASS.DAT (if it exists)
    b. Windows XP/2003: C:\Documents and Settings\user\Local Settings\Application Data\Microsoft\Windows\USRCLASS.DAT
3. C:\Windows\ServiceProfiles\LocalService, NetworkService; NTUSER.DAT,
    a. C:\Windows\ServiceProfiles\[LocalService‖NetworkService]\AppData\Roaming\Microsoft\Windows\USRCLASS.DAT (if it exists)
2. C:\Windows\AppCompat\Programs\Amcache.hve

USAGE

To run the extension, open a case, select Scripts in the tool bar, and choose the RegRipper script, as illustrated in Figure 1.

Once the extension dialog opens, fill in the text fields with the appropriate information, as illustrated in Figure 2. Note that you can select File from the menu bar, and save or load the settings.

Once the proper entries are made in the text fields, click "Ok" to launch the script. Allow the script to run; it will automatically search out and attempt to export and parse all of the previously identified hive files.

Once the script completes, all RegRipper output files are located in the "Output Path" folder, along with a "summary_report.csv" file that provides information regarding which files were exported from the Nuix case and sent to RegRipper for parsing.

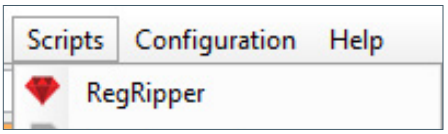

Figure 1: RegRipper extension script

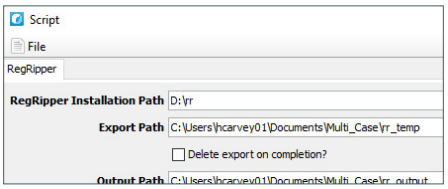

Figure 2: Extension text fields

LESS CLICKS - FASTER RESULTS

Your investigations are complicated and lengthy enough. Over the course of many investigations or analysis of multiple devices within a single investigation, the mouse clicks and seconds spent switching between applications add up.

The RegRipper extension for the Nuix Workbench trims away some of that back-and-forth by automating some of those steps, making it more efficient to collect and import the Windows Registry evidence that you need to successfully complete your investigations.

TO FIND OUT MORE ABOUT HOW NUIX CAN HELP YOUR ORGANIZATION, VISIT

nuix.com/problems-we-solve

ABOUT NUIX

Nuix understands the DNA of data at enormous scale. Our software pinpoints the critical information organizations need to anticipate, detect, and act on cybersecurity, risk, and compliance threats. Our intuitive platform identifies hidden connections between people, objects, locations, and events—providing real-time clarity, control, and efficiency to uncover the key facts and their context. **www.nuix.com**.

North America

USA: +1 877 470 6849

EMEA

UK: +44 203 934 1600

APAC

Australia: +1 877 470 6849