Jason Rodriguez

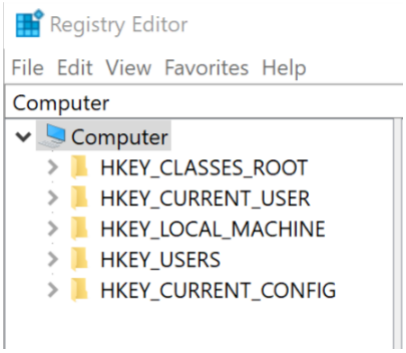
Windows registry Analysis

July 29, 2018

General Overview

> The Windows Registry usually referred to as just *the registry*, is a collection of databases of configuration settings in Microsoft Windows operating system. The Windows Registry is used to store much of the information and settings for software programs, hardware devices, user preferences, operating system configurations, and much more.

Before placing any data into the registry, an application needs to divide the data into two categories: computer-specific data and user-specific data

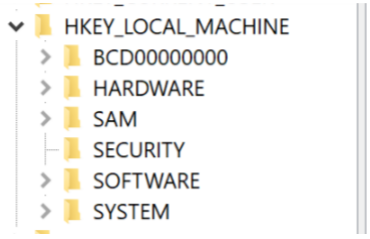


In-depth research

A Hive is a logical group of keys, subkeys, and values in the registry that has a set of supporting files containing backups of its data. For example, each time a new user logs on to a computer, a new hive is created for that user with a separate file for the user profile.

HKEY_LOCAL_MACHINE is a particular hive that contains most of the configuration information for the software you have installed, also for the Windows operating system itself. In addition to software configuration data, this hive also contains valuable information about currently detected hardware and device drivers and information about the computer's boot configuration.

They are subkeys in HKEY_LOCAL_MACHNE for example:



This is a Windows 10 Pro

The keys under your HKEY_LOCAL_MACHINE might look different on your computer, it all depends on what Windows version your computer is running.

The software subkey is one of the most commonly used keys, it is organized alphabetically by the software vendor, and this is where each program writes data to the registry so that the application gets opened in another time.

Windows Registry backup files are saved as REG files (REG files are a registration file used by the Windows Registry).

The information on the hives is critical for any forensic conducting an investigation, for example, knowing the last write time of any key can allow a forensic to infer the date or time an event occurred. A forensic can have a better understanding of what type of user is it by just by looking at the RunMRUkey. The RunMRUkey is the most recently used.

Tools

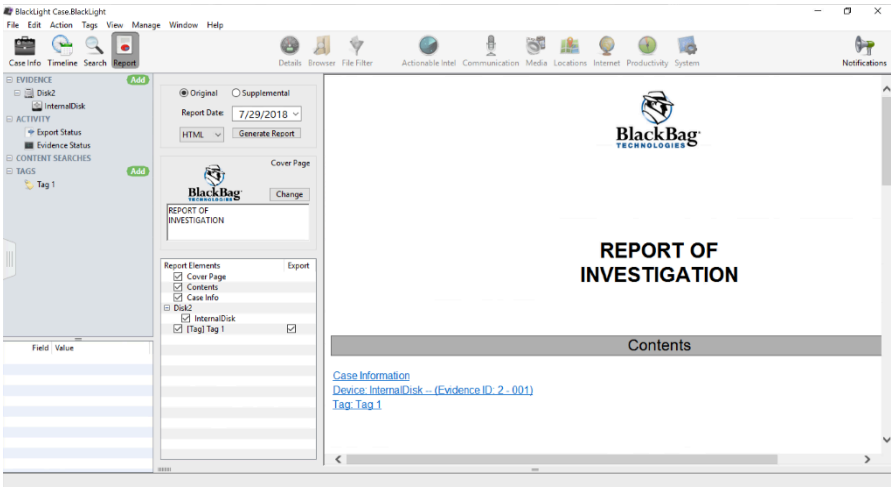
1. **Blacklight** by BlackBag technologies. Available for Windows, Mac OSX, Android, and Apple IOS.

BlackLight's Actionable Intel view allows examiners to view various data points that can be attributed to a user's actions. Traces of potentially important user activity from many disparate locations are organized for practical, efficient examination. Elements include:

- Windows Registry artifacts - recently executed files and programs, link files, jump lists, Prefetch and SuperFetch data
- Device connection data for all devices previously connected to the system, including USB device connection dates/times and the associated user account
- iOS device backups
- Recent file downloads
- Trash (for Mac OS X volumes) and Recycle Bin (for Windows volumes)

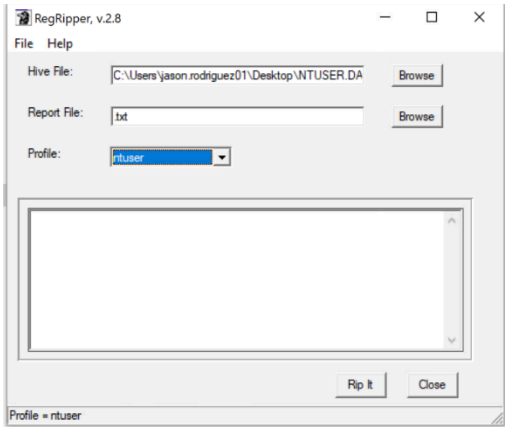
- Current and deleted user account info

Blacklight can report data in any format currently use such as: .pdf, .html, .docx, and .txt.



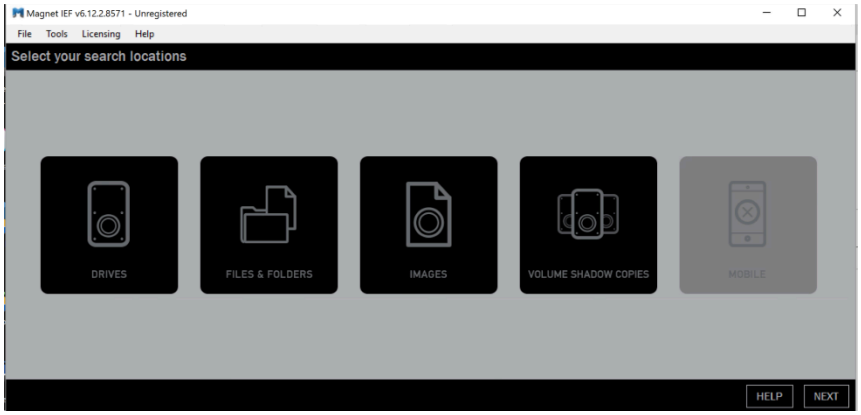
Blacklight makes reporting flexible, may export large data sets. You can even (blur) sensitive data if such report may be shared to non-authorized third parties.

2. **RegRipper** develop by Harlan Carvey. Available only for Windows. It is Windows Registry data extraction and correlation tool. RegRipper bypass the Win32API. This module is used to locate and access Registry key nodes within the hive files, also value



nodes and their data.

3. **Magnet IEF** by Magnet Forensics. Magnet is available for Windows, Mac OSX, Apple IOS, and Android. A single IEF search intelligently parses and carves for hundreds of different types of digital forensic artifacts found in allocated and unallocated space on computers.



Reference:

Fisher, T. (2018, January 8). What Is the Windows Registry & What's It Used For? Retrieved from https://www.lifewire.com/windows-registry-2625992

Forensic Tool Functionalities. (n.d.). Retrieved from https://toolcatalog.nist.gov/populated_taxonomy/index.php?all_tools=refine&ff_id=10&1[]=1&2[]=any&3[]=any&5[]=any&4[]=any&6[]=any&7[]=any

BlackLight | Native Mac, Windows, Android, iPad and iPhone Forensic Analysis Software by BlackBag Technologies. (n.d.). Retrieved from https://www.blackbagtech.com/blacklight.html#Features

Magnet IEF. (n.d.). Retrieved from https://www.magnetforensics.com/magnet-ief/

Shaver's, B. (2015, December 6). RegRipper. Retrieved from https://brettshavers.com/index.php/component/easyblog/entry/regripper