



info@volatilesystems.com
Register

[Home](#) [Company](#) [Services](#) [Resources](#) [Training](#) [Partners](#) [Blogs](#) [Login](#)

The Volatility Framework: Volatile memory artifact extraction utility framework

Overview

The Volatility Framework is a completely open collection of tools, implemented in Python under the GNU General Public License, for the extraction of digital artifacts from volatile memory (RAM) samples. The extraction techniques are performed completely independent of the system being investigated but offer unprecedented visibility into the runtime state of the system. The framework is intended to introduce people to the techniques and complexities associated with extracting digital artifacts from volatile memory samples and provide a platform for further work into this exciting area of research.

The Volatility Framework demonstrates our commitment to and belief in the importance of **open source digital investigation tools**. Volatile Systems is committed to the belief that the technical procedures used to extract digital evidence should be open to peer analysis and review. We also believe this is in the best interest of the digital investigation community, as it helps increase the communal knowledge about systems we are forced to investigate. Similarly, we do not believe the availability of these tools should be restricted and therefore encourage people to modify, extend, and make derivative works, as permitted by the GPL.

Capabilities

The Volatility Framework currently provides the following extraction capabilities for memory samples

- Image date and time
- Running processes
- Open network sockets
- Open network connections
- DLLs loaded for each process
- Open files for each process
- Open registry handles for each process
- A process' addressable memory
- OS kernel modules
- Mapping physical offsets to virtual addresses (strings to process)
- Virtual Address Descriptor information
- Scanning examples: processes, threads, sockets, connections, modules
- Extract executables from memory samples
- Transparently supports a variety of sample formats (ie, Crash dump, Hibernation, DD)
- Automated conversion between formats

Supported Samples

The Volatility Framework can extract digital artifacts from volatile memory samples captured from:

- 32bit Windows XP Service Pack 2 and 3
- 32bit Windows 2003 Server Service Pack 0, 1, 2
- 32bit Windows Vista Service Pack 0, 1, 2
- 32bit Windows 2008 Server Service Pack 1, 2 (there is no SP0)
- 32bit Windows 7 Service Pack 0, 1

Example Data

If you want to give Volatility a try, you can download one of the samples listed within the **Volatility FAQ**.

Download

Volatility-2.0: **tar.gz / zip / standalone EXE / EXE (python installed) / md5 / sha1**
Volatility-1.3_Beta: **tar.gz zip md5 sha1 gpg tar.gz gpg zip gpg_key**
Volatility-1.1.2: **tar.gz zip md5 sha1 gpg tar.gz gpg zip gpg_key**
Volatility-1.1.1: **tar.gz md5 sha1 gpg gpg_key**

Mailing List

Register for the mailing lists at the following URL:

<http://lists.volatilesystems.com/mailman/listinfo>

Contribute

We are always looking for people who are willing to actively contribute to the project. If you are waiting for a particular feature to be released, remember it will get finished a lot quicker with your assistance. If you are interested in finding out ways you can contribute to the project, please contact us at the vol-dev mailing list.

Documentation

Documentation about Volatility usage and development can be found on the **Volatility Wiki**.

Bug Reports

Bug reports should be submitted to the Volatility Developers Mailing List (vol-dev), the **Volatility Issue Tracker**, or on IRC: #volatility @ freenode.

Training

If you are interested in understanding how you can leverage Volatility to augment your current digital investigations or how to build your own Volatility modules consider our hands-on training opportunities: <https://www.volatilesystems.com/default/education>

© 2006-2011 Volatile Systems, LLC