This repository Search Pull requests Issues Gist

volatilityfoundation / **volatility**

Watch 165 Star 946 Fork 198

Code Issues 37 Pull requests 5 Wiki Pulse Graphs

# Installation

gleeda edited this page 24 days ago · 19 revisions

**Table of Contents**

- Getting Volatility
- Installing Volatility
    - Dependencies
        - Recommended packages
        - Optional packages
- Upgrade Volatility

# Getting Volatility

You can get the source code by either downloading a stable release or cloning from github. To do the latter, type:

```
$ git clone https://github.com/volatilityfoundation/volatility.git
```

This will create a `volatility` folder that contains the source code and you can run Volatility directory from there.

# Installing Volatility

If you're using the standalone Windows, Linux, or Mac executable, no installation is necessary - just run it from a command prompt. No dependencies are required, because they're already packaged inside the exe.

If you're using the Pyinstaller (Windows-only) executable, double click and follow through with the installation instructions (which basically consists of clicking Next a few times and then Finish). You must already have a working Python 2.7. Also see below for the dependency libraries.

If you downloaded the zip or tar source code archive (Windows, Linux, OSX) there are two ways to "install" the code:

1) Extract the archive and run `setup.py` . This will take care of copying files to the right locations on your disk. Running `setup.py` is only necessary if you want to have access to the Volatility namespace from other Python scripts, for example if you plan on importing Volatility as a library. Pros: easy use as a library. Cons: more difficult to upgrade or uninstall.

**Pages** 30

Home

Getting Started

- FAQ
- Installation
- Linux
- Mac
- Android
- Basic Usage
- Windows 8 and 2012
- Pyinstaller Builds
- Unified Output

Command References

- Windows Core
- Windows GUI
- Windows Malware
- Linux
- Mac OSX

Development

- Windows Registry
- Address Spaces
- Style Guide

Miscellaneous

- Memory Samples
- Community Docs

Physical Address Spaces

- Firewire
- Crash Dumps
- Hibernation Files
- EWF Files
- LiME (Linux)
- VirtualBoxELF64
- VMWare Snapshot
- Hpak (FDPro)

**Clone this wiki locally**

https://github.com/volatili

Clone in Desktop

2) Extract the archive to a directory of your choice. When you want to use Volatility just do python `/path/to/directory/vol.py` . This is a cleaner method since no files are ever moved outside of your chosen directory, which makes it easier to upgrade to new versions when they're released. Also, you can easily have multiple versions of Volatility installed at the same time, by just keeping them in separate directories (like `/home/me/vol2.0` and `/home/me/vol2.1` ). Pros: clean, easy to run multiple versions, easy to upgrade or uninstall. Cons: more difficult to use as a library.

# Dependencies

This section does not apply to the standalone Windows executable, because the dependent libraries are already included in the exe. Also please note the majority of core Volatility functionality will work without any additional dependencies as well. You will only need to install packages if you plan on using specific plugins that leverage those packages (see recommended dependencies), or if you want to enhance your experience (see optional dependencies). Note: for Linux you may have to install a few other packages/libraries as prerequisites for the following recommended packages (Example: `apt-get install pcregrep libpcre++-dev python-dev -y` )

## Recommended packages

For the most comprehensive plugin support, you should install the following libraries. If you do not install these libraries, you may see a warning message to raise your awareness, but all plugins that do not rely on the missing libraries will still work properly.

- Distorm3 - Powerful Disassembler Library For x86/AMD64
  - Dependent plugins
    - apihooks
    - callbacks
    - impscan
    - kdbgscan, pslist, modules etc for Windows 8/2012 machines
    - the disassemble command in volshell, linux_volshell, and mac_volshell
- Yara - A malware identification and classification tool
  - Dependent plugins
    - yarascan, linux_yarascan, mac_yarascan
  - Note: get yara from the project's main website, do not install it with pip.
  - Note: if you are on Linux, you may have to issue the following command: `echo "/usr/local/lib" >> /etc/ld.so.conf && ldconfig`
- PyCrypto - The Python Cryptography Toolkit
  - Dependent plugins
    - lsadump
    - hashdump
  - Note: this requires `python-dev` to build (unless you get pre-built binaries)
- PIL - Python Imaging Library
  - Dependent plugins
    - screenshots
- OpenPyxl - Python library to read/write Excel 2007 xlsx/xlsm files
  - Dependent plugins
    - Any plugin that has been converted to unified format (with `--output=xlsx` option)
- ujson - Ultra fast JSON parsing library

  - Dependent plugins: anything using `--output=html`

## Optional packages

The following libraries are optional. If they're installed, Volatility will find and use them; otherwise an appropriate alternative method will be chosen.

- pytz for timezone conversion. Alternative: tzset (standard with Python)
- IPython for enhancing the volshell experience. Alternative: code (standard with Python)
- libforensic1394 for live analysis over firewire. Alternative: libraw1394

# Upgrade Volatility

If you used `setup.py` to install Volatility, the files will be placed in a few standard locations. For example:

```
$ sudo python setup.py install
....
byte-compiling /usr/local/lib/python2.6/dist-packages/volatility/fmtspec.py to fmtspec.py
byte-compiling /usr/local/lib/python2.6/dist-packages/volatility/utils.py to utils.pyc
running install_scripts
copying build/scripts-2.6/vol.py -> /usr/local/bin
changing mode of /usr/local/bin/vol.py to 755
running install_data
creating /usr/local/contrib/plugins
copying contrib/plugins/example.py -> /usr/local/contrib/plugins
copying contrib/plugins/psdispscan.py -> /usr/local/contrib/plugins
....
creating /usr/local/contrib/plugins/addrspaces
copying contrib/plugins/addrspaces/ewf.py -> /usr/local/contrib/plugins/addrspaces
copying contrib/plugins/addrspaces/ewf-python.py -> /usr/local/contrib/plugins/addrspaces
running install_egg_info
Writing /usr/local/lib/python2.6/dist-packages/volatility-2.1.egg-info
```

Unfortunately there is no uninstaller, and if you simply try to run `setup.py` for a new version of Volatility, you may end up with some mixed source files which will surely lead to trouble. So before you install a new version of Volatility, remove everything the previous `setup.py` created:

```
$ sudo rm -rf /usr/local/lib/python2.6/dist-packages/volatility
$ sudo rm `which vol.py`
$ sudo rm -rf /usr/local/contrib/plugins
```

Now you can run the `setup.py` for your new Volatility version. As stated above, please remember `setup.py` is only necessary if you plan on importing Volatility as a library from other Python scripts. If you just want to use Volatility, no installation is necessary (just extract the archive and run `vol.py` inside).

Volatility Foundation