PASSMARK® SOFTWARE

Volatility Workbench Configuration File Specification

Document Edition: 1.0
Date: 23 June 2017
Web site: www.passmark.com & www.osforensics.com

PASSMARK® SOFTWARE

Introduction

This document describes an enhancement to the Volatility memory forensics tool.

Many of the commands used with Volatility require one or more parameters to be passed into the tool on the command line. Typically, these are “Profile name”, the “KDBG address” and sometimes a process id. Collecting this initial data can be a time consuming business, especially with large memory images. Each time a memory image is created or reloaded this data needs to be collected again. As far as we know there is no standard way to store this data once it is collected.

We hope to address this by proposing the use of configuration files. Configuration files are “.cfg” files within the same directory as the memory dump file. These files are created by the dumping software (for example OSForensics V5) and helps to speed up the analysis process in Volatility. This is achieved by saving the image profile which is known at the time of creating the image.

The first time an image file is opened by the Volatility Workbench, it searches within the image to find the KDBG address and process list and will append this information to the configuration file. Therefore, when a memory image is re-loaded, this saves a lot of time by eliminating the steps to acquire the KDBG address and process list.

File path and encoding details

The configuration file should be in the image directory and with the same name as the memory image file. e.g. if the image file is “mem.img”, then the configuration file should be “mem.cfg”.
File Extension: .cfg
Encoding: UTF-8 with BOM (byte sequence 0xEF,0xBB,0xBF)

An example of the file contents is shown below:
Example:

```
PROFILE=Win2003SP0x86
KDBG=0x805693d0
PROCESS=System,4
PROCESS=smss.exe,356
PROCESS=csrss.exe,412
PROCESS=winlogon.exe,436
…
```

PASSMARK® SOFTWARE

Parameters Description

Profile

Volatility needs to know what type of system your memory dump came from, so it knows which data structures, algorithms, and symbols to use. If you want to see a list of supported profile names, do the following:

```
$ python vol.py –info
```

This parameter will be automatically filled if you generate the memory dump using OSForensics tool.

KDBG (optional)

The KDBG is a structure maintained by the Windows kernel for debugging purposes. It contains a list of the running processes and loaded kernel modules. The KDBG address is optional and can be identified by running kdbgscan plugin of the Volatility tool or performing Get Process List from the Volatility Workbench tool.
The Volatility Workbench will add this parameter to the configuration file once it finished getting the process list.

PROCESS (optional)

You can specify the process list by including PROCESS=[process name],[process address] for each process in the memory image file. This parameter is optional and can be identified by running pslist plugin of the Volatility tool or performing Get Process List from within the Volatility Workbench tool.
The Volatility Workbench will add this parameter to the configuration file once it obtained the process list.

Use of the .CFG file

At the moment the command line version of Volatility (V2.6) doesn't use the configuration file. But the graphical user interface, Volatility Workbench, does make use of the file.

References

Volatility foundation
http://www.volatilityfoundation.org/

OSForensics
http://www.osforensics.com/osforensics.html

Volatility Workbench
http://www.osforensics.com/tools/volatility-workbench.html

License