

# volatility-runner

---

volatility-runner is a command line application designed to speed up memory forensics using the volatility framework, primarily for instances where the user has multiple memory dumps to analyse.

The purpose of the application is to provide the plugins that are required to be run, the paths to the memory dumps and the memory dump profile, **vr** will then run each plugin in sequence against each of the supplied memory dump files.

The application is controlled by yaml config file; an example of which is shown below:

```
volatility_path: "/opt/volatility/vol.py"
output_path: "/home/woany/mem/output"
use_summary_dir: true

plugins:
  - name: pslist
    summarise: true
  - name: shimcachemem
    summarise: true
  - name: pstree
    summarise: true
  - name: psxview
    summarise: true
  - name: cmdline

data:
  - ram_path: "C:\\dumps\\one.dmp"
    profile: Win7SP1x64_23418
  - ram_path: "C:\\dumps\\two.dmp"
    profile: Win7SP1x64_23418
  - ram_path: "C:\\dumps\\three.dmp"
    profile: Win10x64_10586
```

The **use\_summary\_dir** value creates a sub-directory to the location where the memory dump is located. The sub-directory is used to create the summary.md file

Each of the plugin values has a **summarise** value, which controls whether the data from the plugin is included in the summary. For example **filehandles** might create too much noise and so would have a **false** value set.

The config file supplied with the binary contains the core plugins set, with appropriate summarise (IMHO) values.

**It is important to know that backslashes must be escaped e.g. double slash else you will get an error such as:**

```
Error loading config: Error unmarshalling the hunt file: yaml: line 7: found unknown escape character
```

When running **vr** will keep the user informed as to what is running like so:

```
Running plugin 'pslist' against RAM dump 'one.dmp' @ 2017-06-23T12:11:09+01:00
Running plugin 'pslist' against RAM dump 'two.dmp' @ 2017-06-23T12:11:15+01:00
Running plugin 'pslist' against RAM dump 'three.dmp' @ 2017-06-23T12:11:20+01:00
Running plugin 'netscan' against RAM dump 'one.dmp' @ 2017-06-23T12:11:43+01:00
Running plugin 'netscan' against RAM dump 'two.dmp' @ 2017-06-23T12:11:43+01:00
Running plugin 'netscan' against RAM dump 'three.dmp' @ 2017-06-23T12:11:43+01:00
Running plugin 'svcscan' against RAM dump 'one.dmp' @ 2017-06-23T12:11:43+01:00
Running plugin 'svcscan' against RAM dump 'two.dmp' @ 2017-06-23T12:11:43+01:00
Running plugin 'svcscan' against RAM dump 'three.dmp' @ 2017-06-23T12:11:43+01:00
```