# TotalRecall v 1.0

## Prerequisites

TotalRecall requires the following programs. Most of these are included in Remnux, a free Image available for download at <http://zeltser.com/remnux/>. This has been tested on Remnux v3.

* Yara
* VirusTotal API Key (<https://www.virustotal.com>)
  + This gets placed in the investigation file, search for API KEY
* Volatility (2.3\_alpha)
* ClamAV

### To Install other Volatility Versions

The program uses Volatility 2.3, which is not yet available, but the code is available to testing. It must therefore be downloaded for TotalRecall is to be used. Be sure you are in the directory you want these to be in. The default for TotalRecall is “/home/remnux”

cd /home/remnux

svn co <http://volatility.googlecode.com/svn>

If you decide to use another location for these, the variable ‘volatilityPath’ must be changed in the code. This route was chosen as it ensures everyone is running TotalRecall on the same version of Volatility, as there are varying versions on REMNux, each having different output.

Please note that since we are using a beta version, there WILL be errors like this:

\*\*\* Failed to import volatility.plugins.zeusscan1 (AttributeError: 'module' object has no attribute 'ImpScan')

Don’t worry, this is normal!

## Usage

The minimum requirements to run TotalRecall are the PATH, FILENAME, and PROFILE parameters.

usage: WORKING\_Volatility9.py [-h] -d PATH -f FILENAME -p PROFILE

[-v VOLATILITY] [-i] [-t]

Grabs information from a memory dump

optional arguments:

-h, --help show this help message and exit

-d PATH, --directory PATH

Directory to save the output of the commands to.

-f FILENAME, --filename FILENAME

The memory dump you wish to analyse.

-p PROFILE, --profile PROFILE

The profile of the memory dump being analysed

-v VOLATILITY, --volatility VOLATILITY

The full path to vol.py, default is to usr/bin/vol.py

-i, --investigation Enable investigation of dumped items with yara, Cymru, and clamav

-t, --timeline Attempt to pull timeline artefacts

By default, TotalRecall runs the following Volatility plugins. They are saved in the location specified by the “-d” parameter.

* Pslist
* Psscan
* Apihooks
* Callbacks
* Connscan
* Dlllist
* Driverscan
* Ldrmodules
* Modules
* Ssdt
* Sockscan
* Dlldump
* Vaddump
* Procexedump
* Moddump
* malfind

### -p (PROFILE)

The profile of the memory dump. This means you must run ‘imageinfo’ FIRST before running the script!

vol.py imageinfo –f <memory dump>

This will produce the profile of the memory dump.

### -i (INVESTIGATION)

The investigation plugin at this time does the following:

* Runs ClamAV against every file dumped from dlldump, vaddump, procexedump, moddump, and malfind (saved as clamAVScan.txt)
* Run YARA against against every file dumped from dlldump, vaddump, procexedump, moddump, and malfind (saved as YaraHits.txt)
* These outputs are parsed for hits, sorted, and uniq’d to remove duplicates and their hashes are submitted to VirusTotal (saved as VirusTotalResults.txt)
* The hashes are also submitted to TeamCyrmu (saved as Cymru\_results.txt). The output of the results can be interpreted by reading the MHR page at http://www.team-cymru.org/Services/MHR/

The plugin requires the VirusTotal (VT) API key, you can add your key in the function VirusTotalSubmission on line 48. The key can be acquired by joining the VirusTotal community at https://www.virustotal.com.

parameters = {"resource": hashValue,

"apikey": "<VT\_API\_Key>"}

Please note the investigation module is limited to **4 hash submissions a minute**, due to the restrictions in VirusTotal.

### -t (TIMELINE)

The timeline plugin at the time runs the following Volatility commands:

* Userassist
* Shellbags
* Shimcache
* Iehistory
* Mftparser
* Timeliner *<- \*This can take a long time\**
* Evtlogs (works on Win2k3/XP only)

### -v (VOLATILITY)

By default, Volatility is running from “/usr/local/bin”. If you have Volatility running from a different location, you can specify it from the command line using this parameter.

## Accessing the Database

The database is an sqlite3 database located in the dump directory (“-d”). TheDB name is the hash of the memory dump. The database is easily viewed and searched using the SQLite Manager plugin for firefox (<https://addons.mozilla.org/en-US/firefox/addon/sqlite-manager/>). Currently all investigation plugins are added to the database and a combination of timeliner, mftparser, and shellbags make up the timeline table.

## Time to Complete

These times are based on a VM with 2GB RAM and the memory dump being approximately 512 MB. Time to complete will vary based on RAM on host plus the size of the memory dump being analyzed.

* No additional switches: 9 minutes
* With the investigation switch: 1hr 9 minutes (approx. 35 minutes spent up uploading hashes to VirusTotal)
* With the timeline switch: > 2 hours

## Tips

* The more yara rules you create- the better detection!
* Update clamAV before running the investigation script
* Try to give your analysis machine as much RAM as possible