GVOL USER GUIDE V 1.1

EG-CERT

Malware Analysis Team

CONTENTS

1] Revision History

Version	Date	Authors	Organization
1.0	September 8, 2015	Mohamad Shawkey	EG-CERT
1.1	October 1,2015	May Medhat	“Malware Analysis Team”

2] EXECUTIVE SUMMARY

GVOL is a lightweight GUI application written in Java designed to automate the usage of Volatility toolkit for the purpose of malware analysis. The application includes various Volatility plugins with their predefined options. In addition to that, users can create batch files to run multiple plugins at once to scan a memory image. Moreover, GVol includes pre-configured batch files to simplify the usage of Volatility for malware analysis process. Furthermore, user can compare the output of Volatility for two images.

2.1] Supported Operating Systems:

- Windows XP, 7, 8, 8.1
- Linux OS.

2.2] Requirements:

- Java Runtime Environment

2.3] GVol predefined settings:

- GVol predefined batch files, plugins, options and profiles for Volatility toolkit is currently for windows operating systems based images analysis

3] GVOL FEATURES AND USAGE

3.1] GENERAL OVERVIEW:

Every function executed by an application or operating system produces a significant modification at (RAM) memory. Consequently, analyzing the data captured from memory image acquired from a target system gives a considerable insight into the runtime state of the memory, enables the analyst to track recent activities and bypass hiding tools such as those used by rootkits. One of the best toolkits used for memory analysis is Volatility.

Volatility toolkit is an open source command line tool built using python language. Analysts use Volatility to extract digital artifacts as it could analyze memory of (32-bit and 64 bit) Windows, Linux, Mac operating systems and also 32-bit Android systems.

But, malware analysts and investigators need more from Volatility. They need more automation, a description for each plugin, and helpful investigative notes. Frequently, users of Volatility want to compare the output of two memory images for the purpose of malware analysis. Also, some users prefer GUI to CLI. Therefore, a new tool named GVol has been developed to fulfill users' requirements.

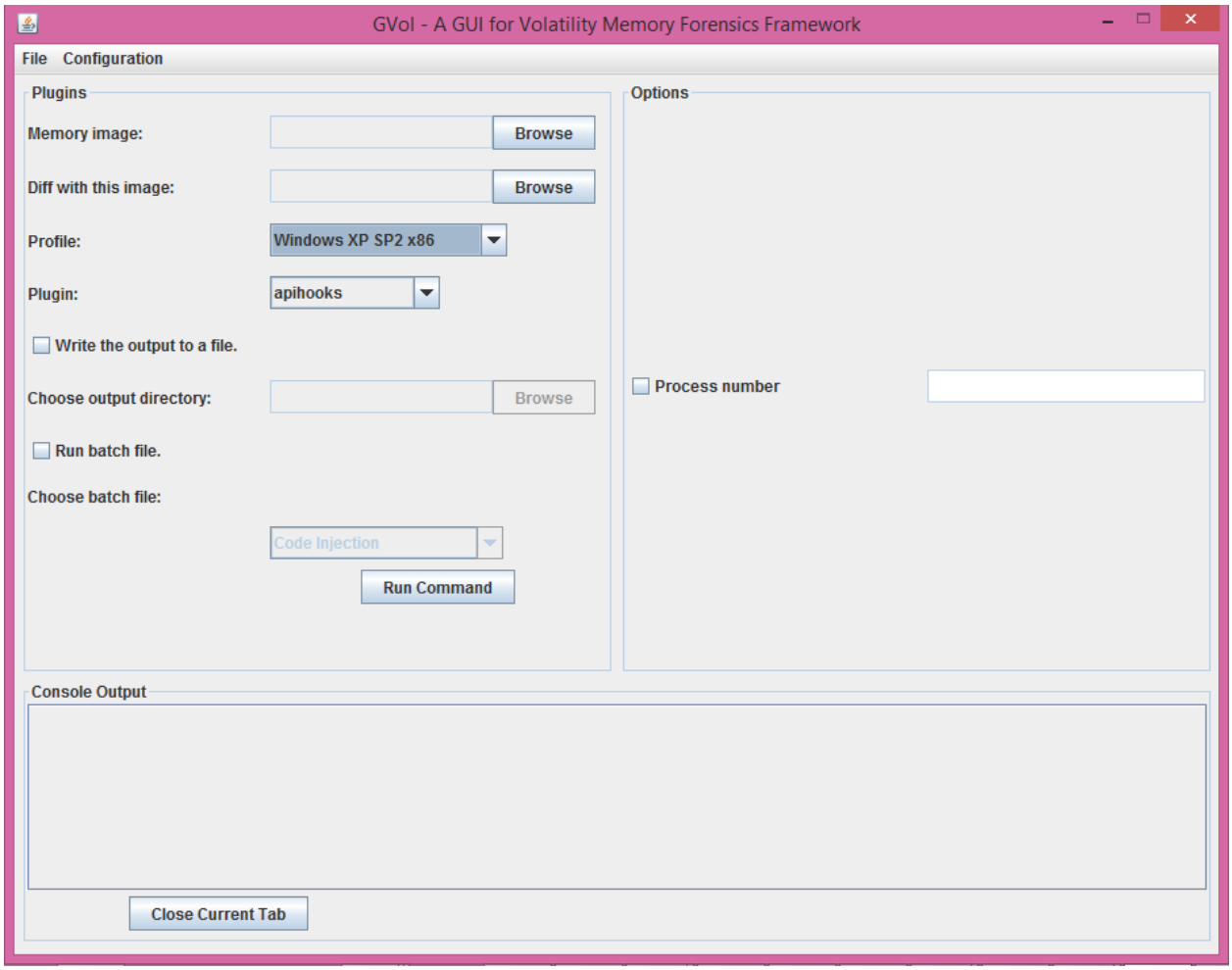
3.2] GVOL FEATURES:

- GVol automates the use of Volatility using a graphical user interface.
- It works with any Volatility version.
- GVol includes a set of predefined profiles for windows operating system; also the user can add new profiles of other operating systems.
- User can select plugins and related options from the existing database or add new plugins or options.
- GVol has batch file feature to run multiple plugins. In addition to that, user can set options for each plugin at batch file through a graphical wizard.
- GVol contains a plugin description and malware analysis hints gathered from "The Art of Memory Forensics" book and "Volatility Command Reference" which can downloaded from this link: https://code.google.com/p/wiki/CommandReference23
- GVol has a console output section which shows the command running at background and also the output generated. The user can chose to write this output to a file. The output file name will be a concatenation of the following image name, batch file name (if it was used) and plugin name.
- GVol now has a comparison feature, user can compare between the outputs of a plugin or batch files for two images and detect added or deleted lines.

3.3] USAGE GUIDE:

3.3.1] GVol Launching:

1. Open the file "GVol.jar" to open GVol main interface.



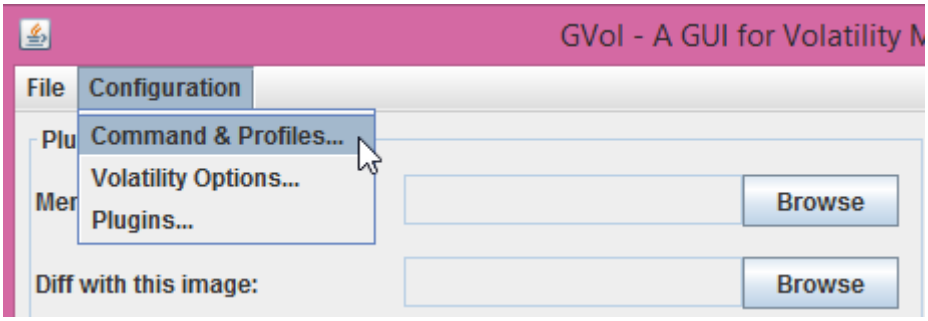
3.3.2] GVol Configuration:

1. Download Volatility toolkit

https://code.google.com/p/Volatility/downloads/list

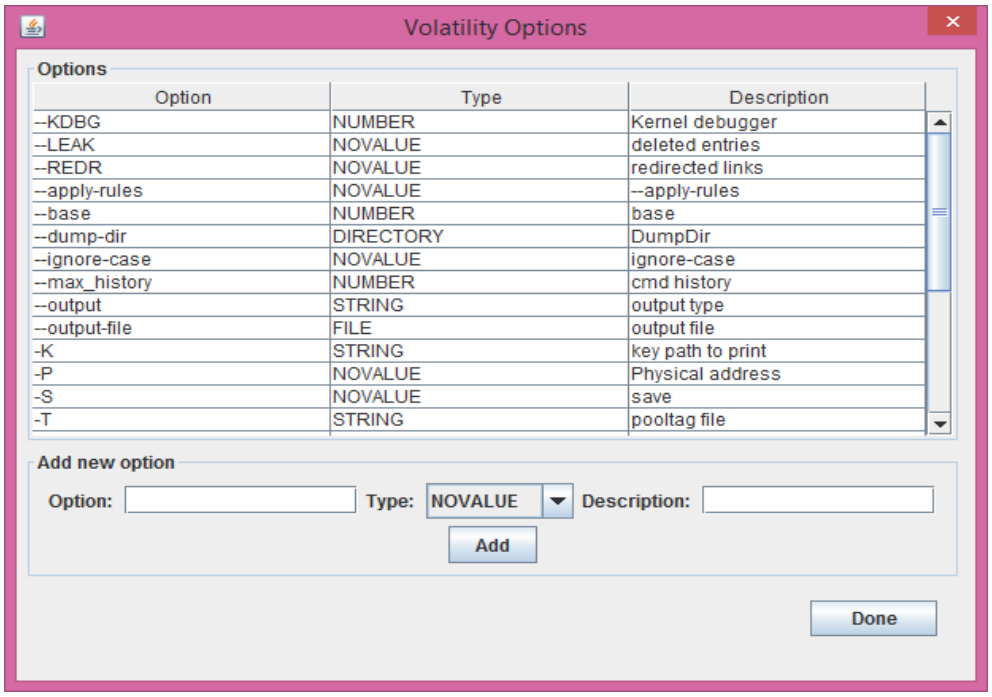
2. Select "Configuration" from the main interface to edit Volatility configurations.
3. Select "Command & Profiles".
4. Type the command that runs Volatility. It would be the path of the standalone executable or "Python vol.py" if you use the python script. Do not forget to click on "Apply Changes".

5. Profiles can be added through “Add new profiles” section by writing the new Volatility profile and its description then click “Add Profile”.

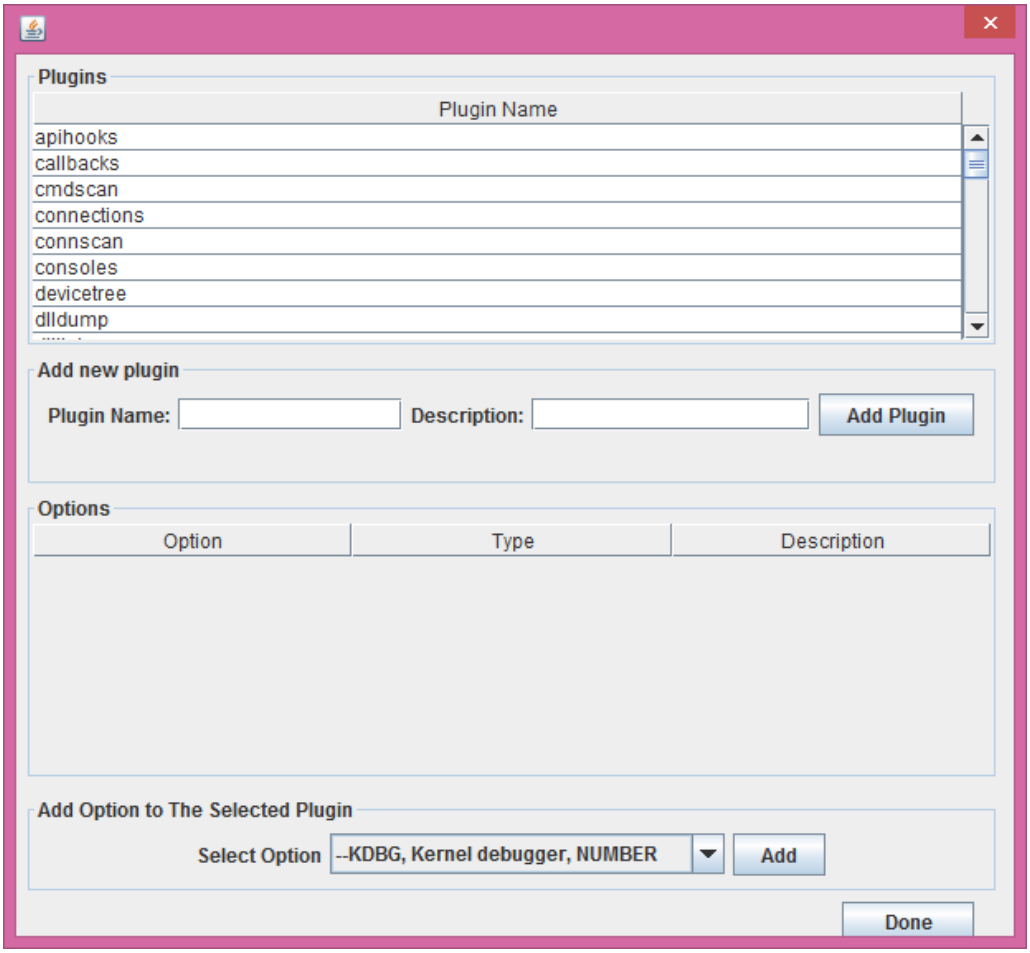


6. To add new options or delete an old one, From “Configuration” menu, select Volatility Options.

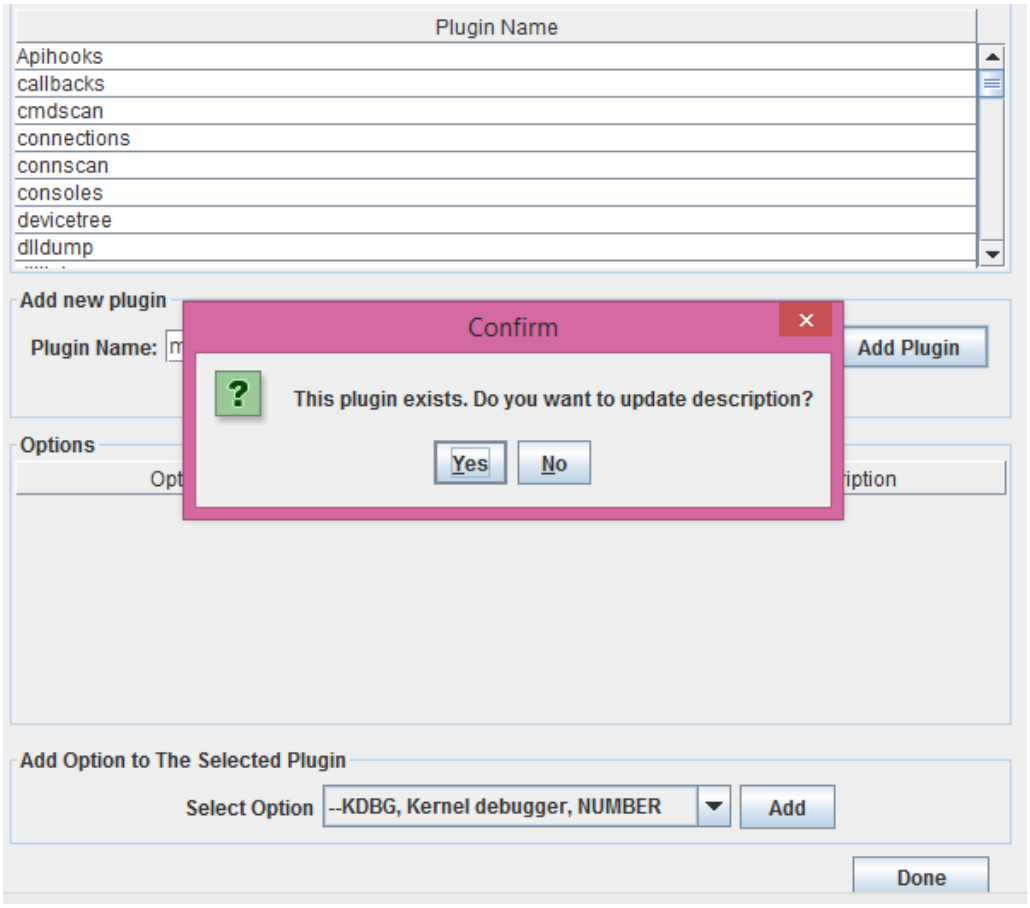
Note: You must specify the correct type for options



7. Also, user can edit Volatility plugins and select their convenient options by selecting plugins from “Configuration” menu.



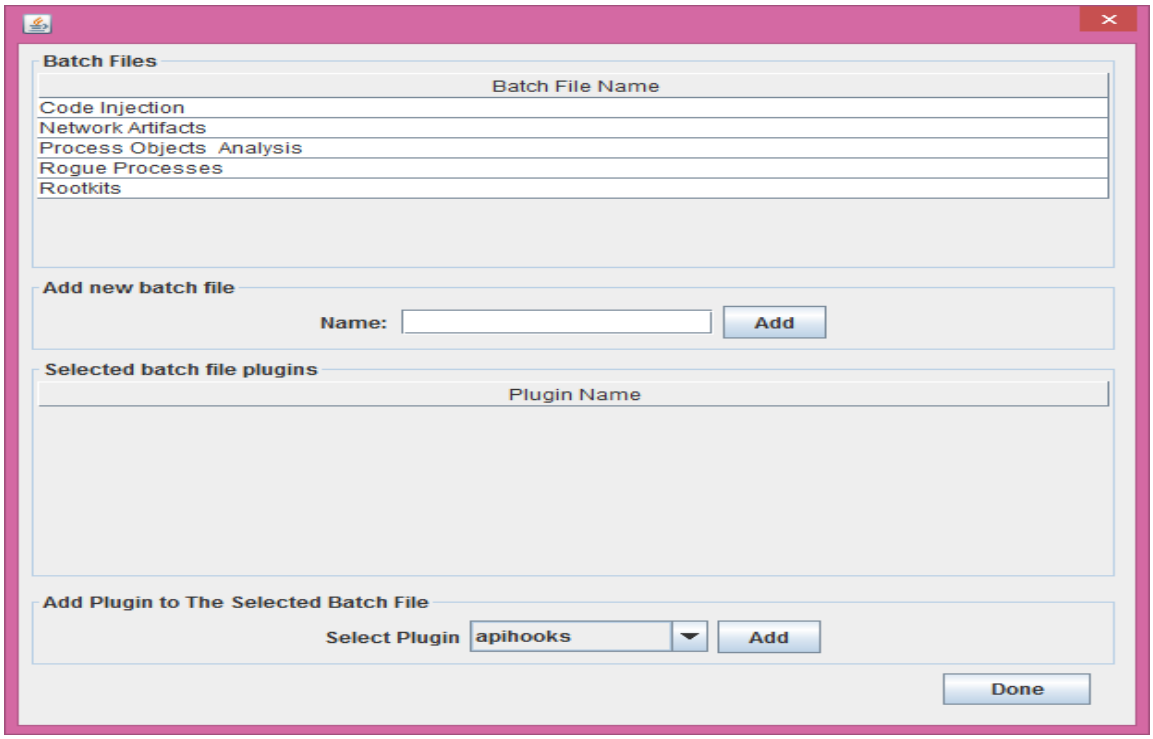
8. User also can update plugin description, by typing plugin name and its description then click “Yes” to update existing plugins as shown below:



3.3.3] GVol Batch File Configuration:

User can run multiple plugins to scan a single image through Batch files as follows:

1. First of all, batch file must be added or selected from the main menu
2. Select File then “Manage Batch Files”
3. A new batch file can be added by typing its name to “Add new batch file” section.
4. Attach required plugins to the batch file selected from “Add Plugins to the Selected Batch File.”

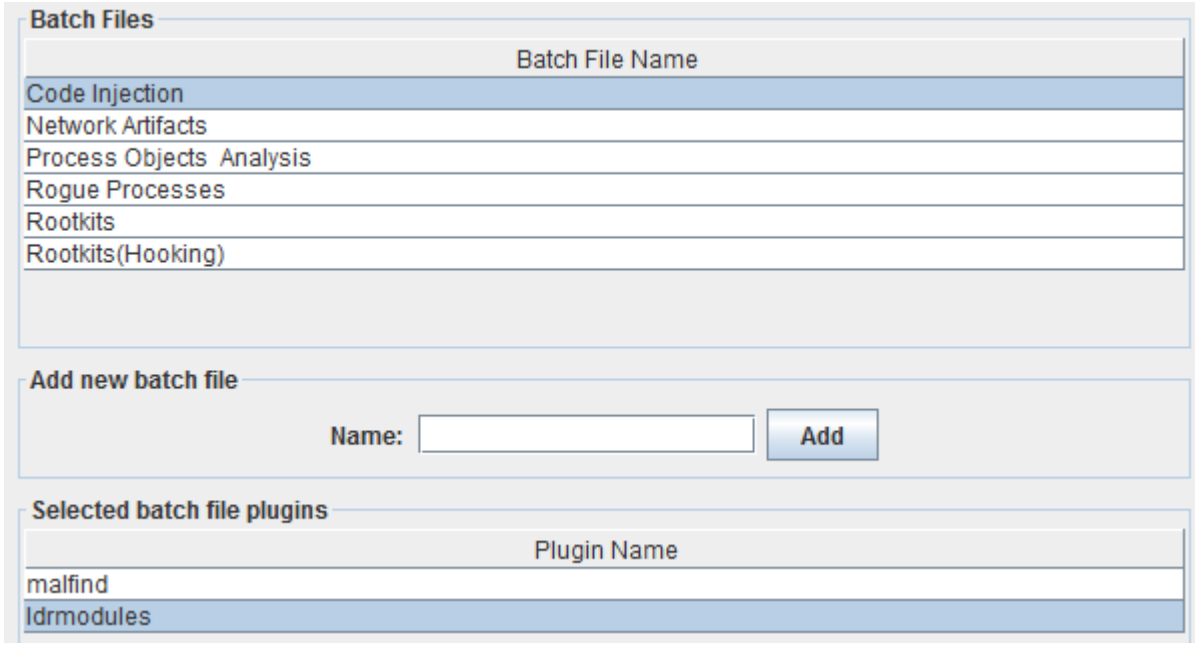


3.3.4] GVol Pre-configured Batch files:

GVol includes Preconfigured batch file, each batch file contains some plugins that could be used to achieve a certain scanning or detection

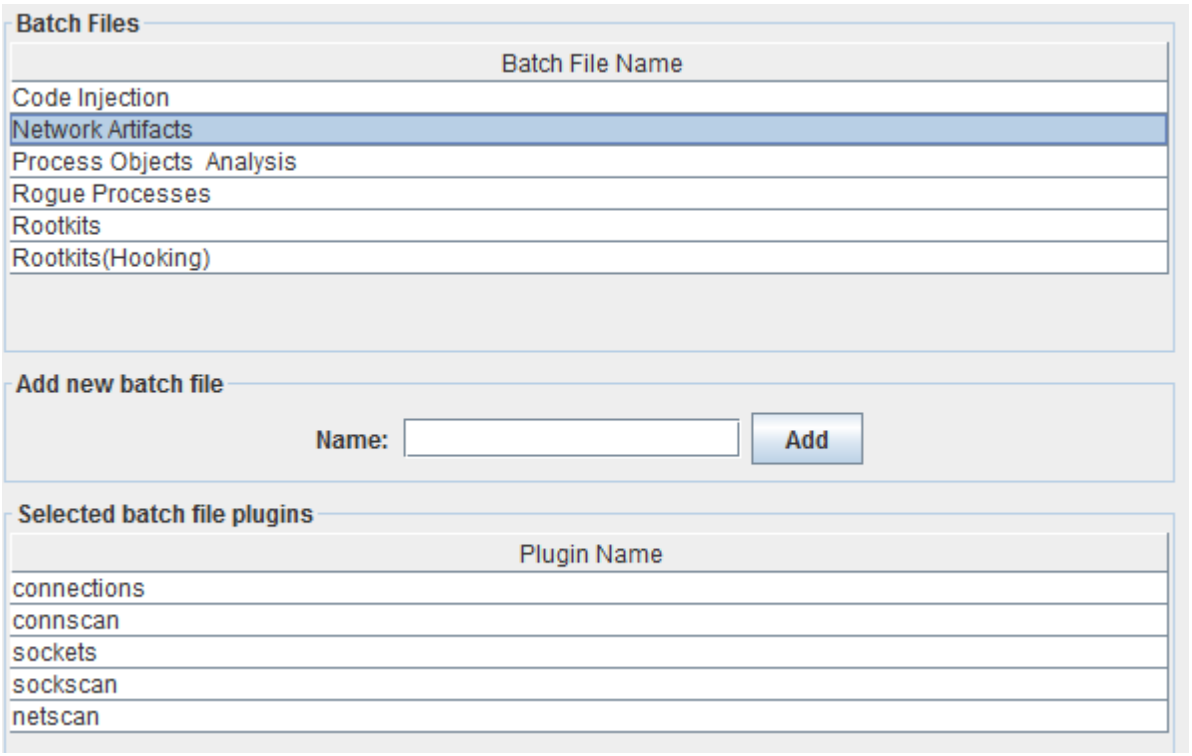
1] Code Injection batch file:

Code injection techniques used by malware to hide their activities. Using memory forensics knowledge and Volatility toolkit code injection could be easily detected using “malfind” plugin to scan for suspicious memory sections with the ability to dump them and “ldrmodules” plugin to detect unlinked dlls.



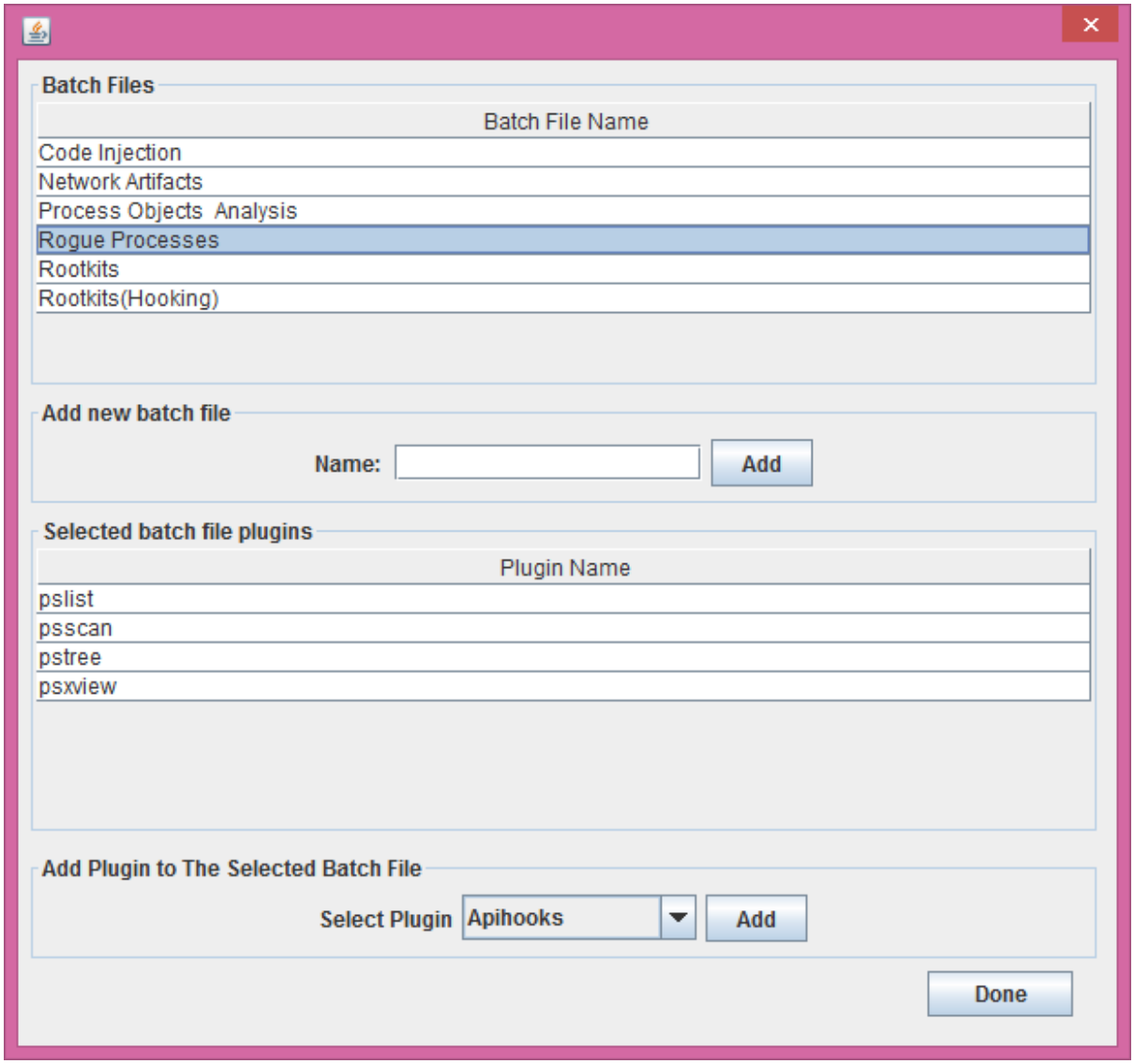
2] Network Artifacts batch file:

Network Artifacts batch file will provide all available information that resides in memory image about network artifacts as it includes Volatility network plugins as shown below:



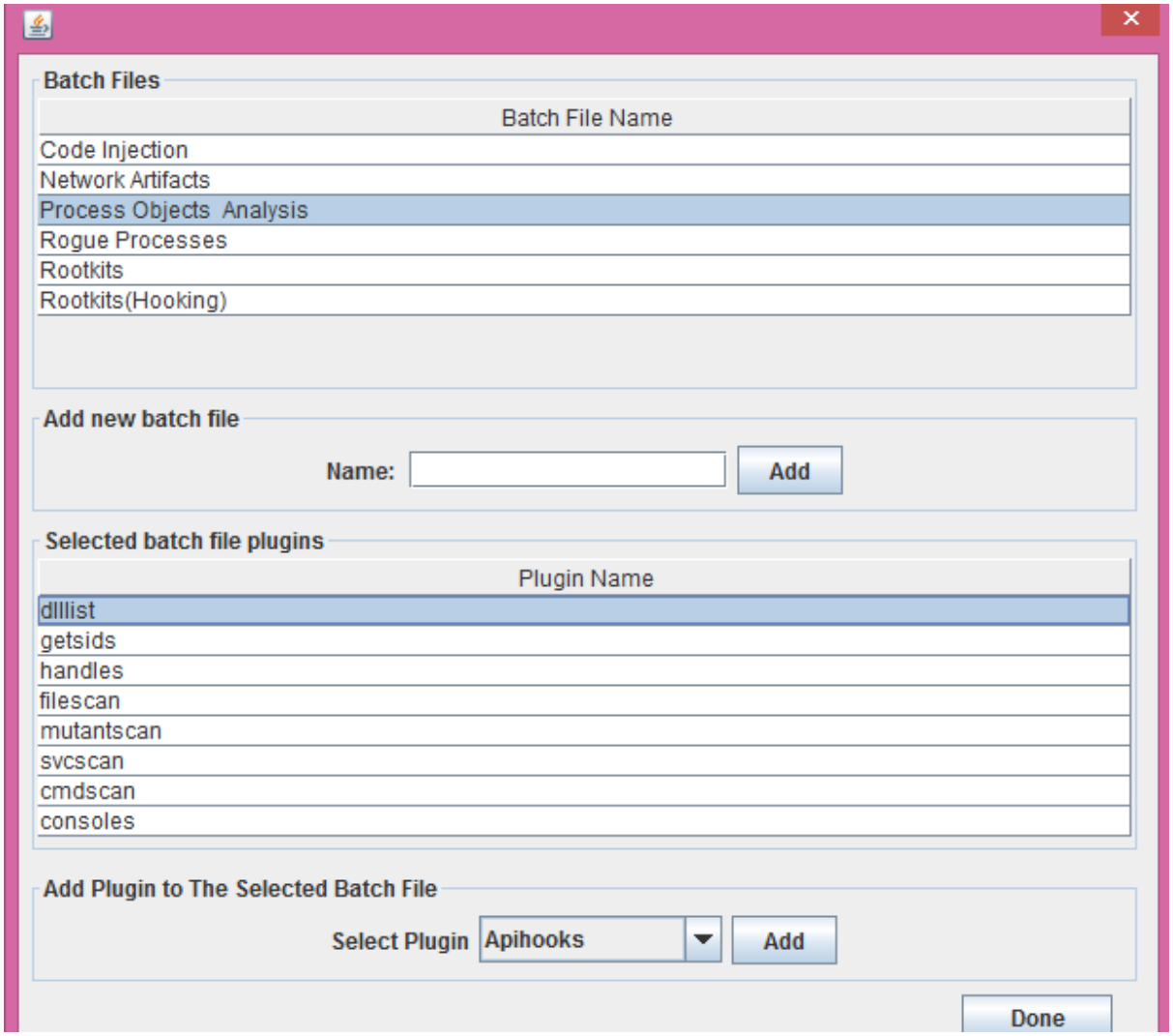
3] Rogue Processes batch file:

Identifying suspicious processes is a critical step during any analysis, Rogue Processes batch file consists plugins that could help investigators to determine the suspicious processes.



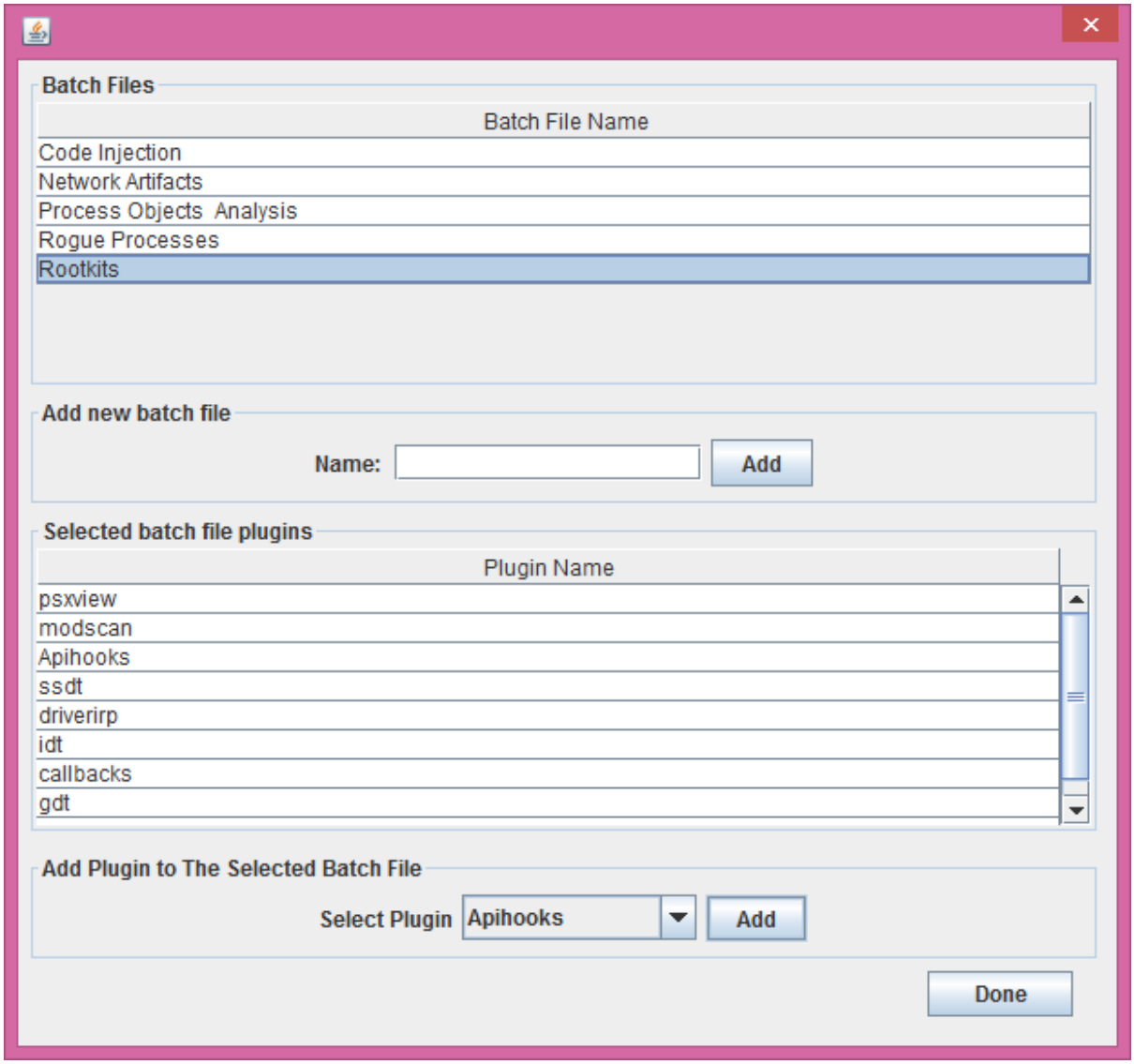
4] Process Objects Analysis:

After identifying the suspicious processes, it is required now to gather more information about them by analyzing their components and objects. Process Objects batch file run plugins that could collect information from memory about the components of those suspicious processes as follows:



5] Rootkits batch file:

One of the most effective techniques to detect rootkits is analyzing memory images to detect signs of infection. This batch file include plugins that help to detect rootkits.



3.3.6] GVol Compare feature:

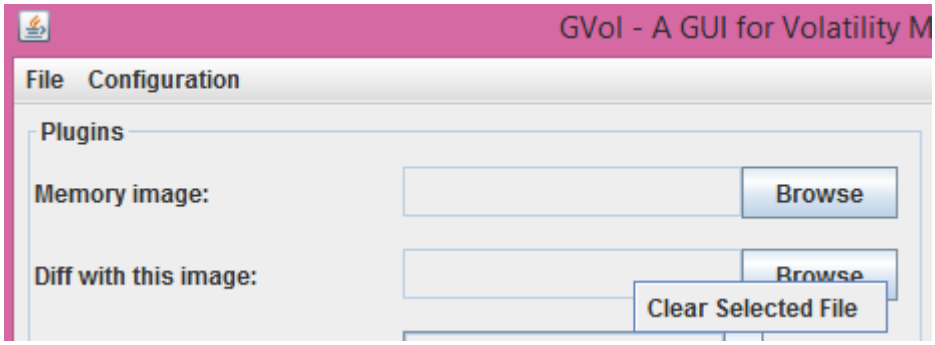
User can choose between running plugins or batch file for one image or two images to compare between them through the main interface. This feature also works with batch file, so user can run multiple plugins at once for both images.

Output Color Code:

Green Line=Added line to the second snapshot
Red Line=Deleted line (Line exists at first snapshot but does not exist at second snapshot)
Yellow Line=Modified line (Line exists at both snapshot but it has modified values)

Note: This feature is not expected to work well if a single entry in the output spans multiple lines.

Note: If you want to clear the selected image, right click the file chooser then select “Clear selected file”



Output sample of the compare feature shown below:

```
1016 wmiprvse.exe 0x77f60000 True True True \WINDOWS\system32\shlwapi.dll
1016 wmiprvse.exe 0x71aa0000 True True True \WINDOWS\system32\ws2help.dll
1016 wmiprvse.exe 0x77fe0000 True True True \WINDOWS\system32\secur32.dll
676 services.exe 0x76e80000 True True True \WINDOWS\system32\rtutils.dll
676 services.exe 0x771b0000 True True True \WINDOWS\system32\wininet.dll
676 services.exe 0x5e0c0000 True True True \WINDOWS\system32\pstorec.dll
```

3.3.5] Running GVol:

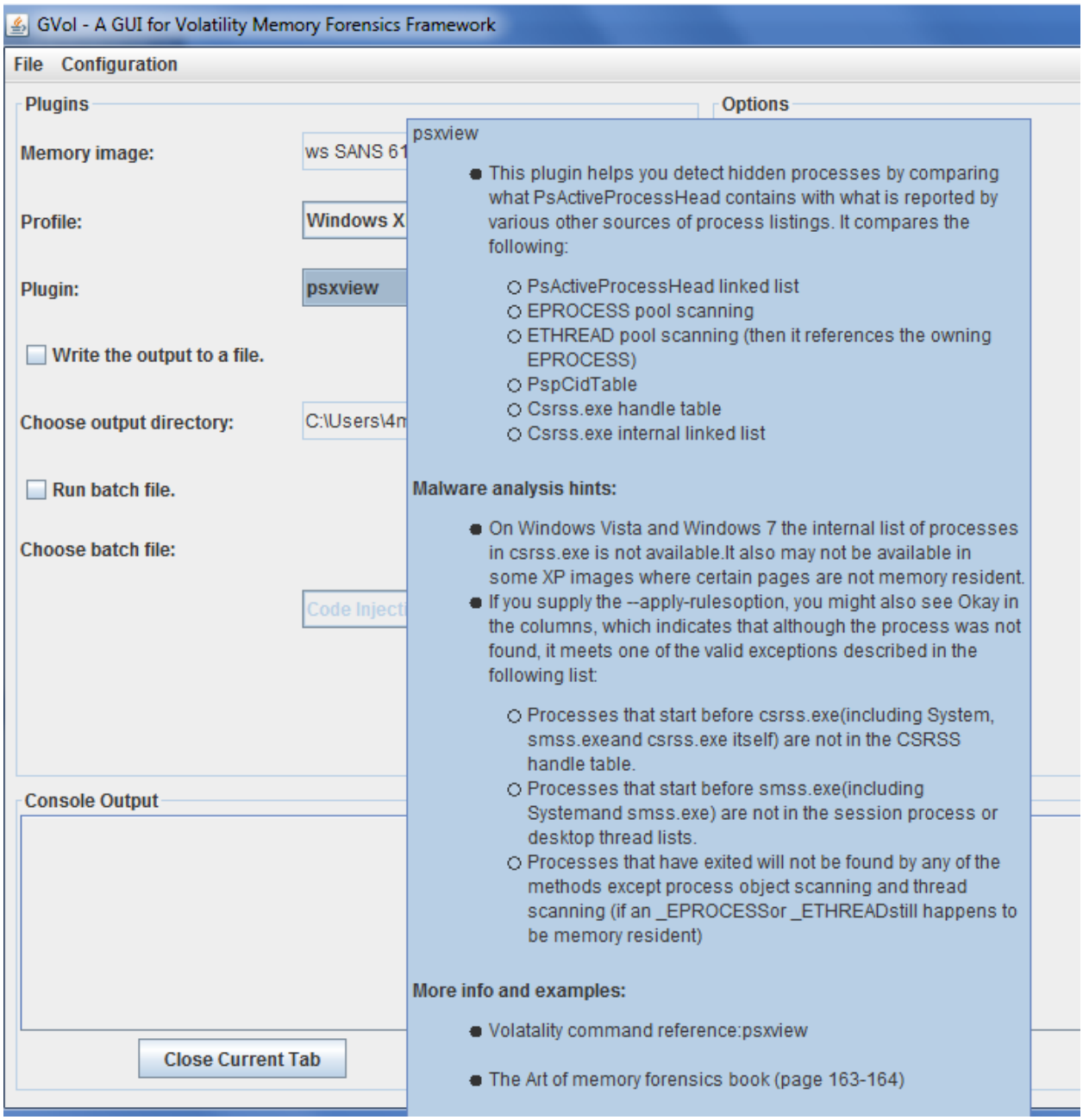
User can select between two options either running GVol with single plugin or running multiple plugins by using the batch file option.

Steps:

A] Running single plugin:

1. Determine the target image to scan and specify its profile
2. Check plugin description and hints by just pausing the mouse pointer to the selected plugin

Note: Plugin description and hints collected from “The Art of memory forensics” book and Volatility command reference which can be found at
https://code.google.com/p/Volatility/downloads/list



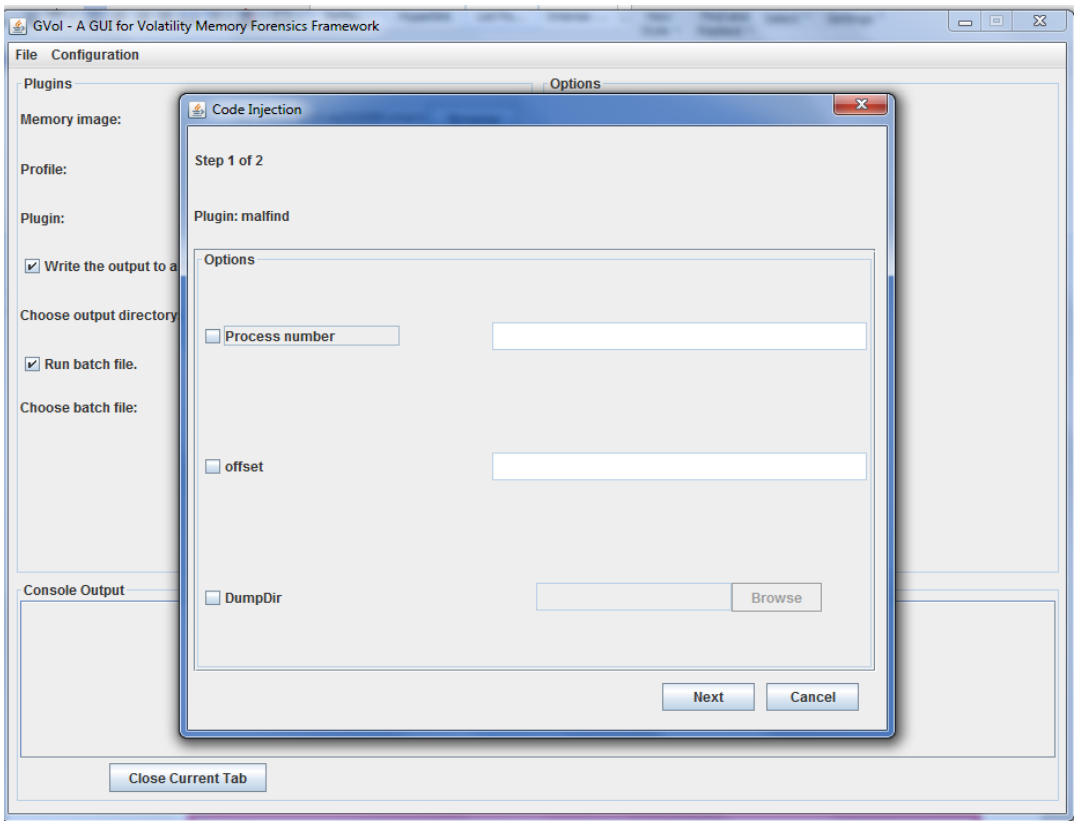
3. Choose plugins and set options
4. Select “Write the output to a file”
5. Select the output directory
6. Click “Run command”

Notes:

You can run another simultaneous command by repeating these steps (1-6). The output of the new command will be visible in a new tab.
You can stop a running command by selecting its tab and clicking on the “Close current tab” button.

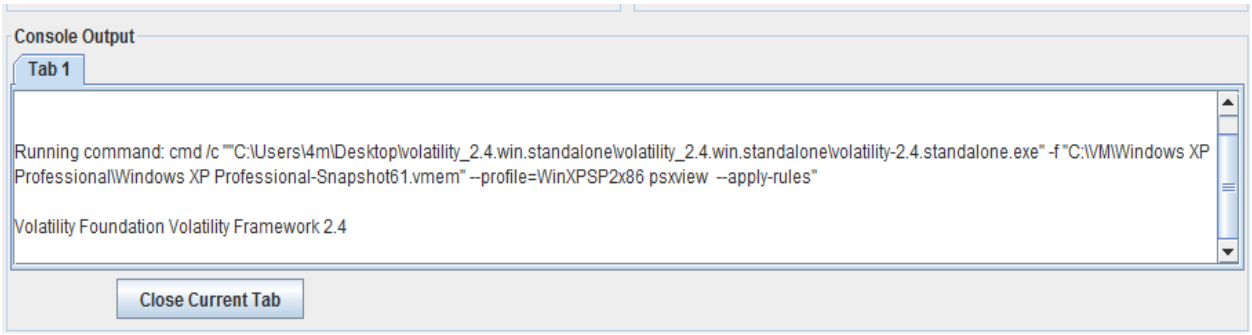
B] Running multiple plugins:

1. Determine the target image to scan and specify its profile
2. Select the check box “Run batch file”
3. Specify the required batch file
4. Select the output directory
5. click “Run Batch”
6. A wizard will appear to enable user set options for each plugin listed at the selected batch file



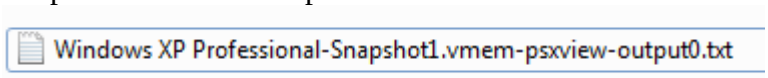
3.3.6] GVol output:

After running single plugin or batch file, user can check the running command and output also at “Console Output”

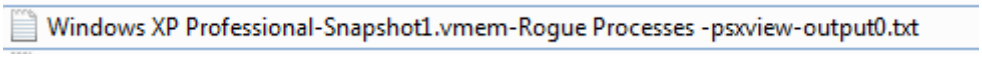


If the user selected the “write the output to a file” option and he specified the output directory. The output file will be generated as the following:

- For single plugin, the output file name format will be as shown below:
Image name: Windows XP Professional-Snapshot1
Plugin name: psxview
Output file number: output0



-For batch file, the output file name will be as shown below:
Image Name: Windows XP Professional-Snapshot1
Batch file name: Rogue Processes
Plugin Name: psxview
Output file number: output0



-For comparison feature, the output will be three files:

1. Plugin output for first image
2. Plugin output for second image
3. Html file contains the difference between the two images with the following format:
Image Name: Windows XP Professional-Snapshot47.vme
Plugin Name: psxview
Output file number: output0.txt
Comparison note: diff