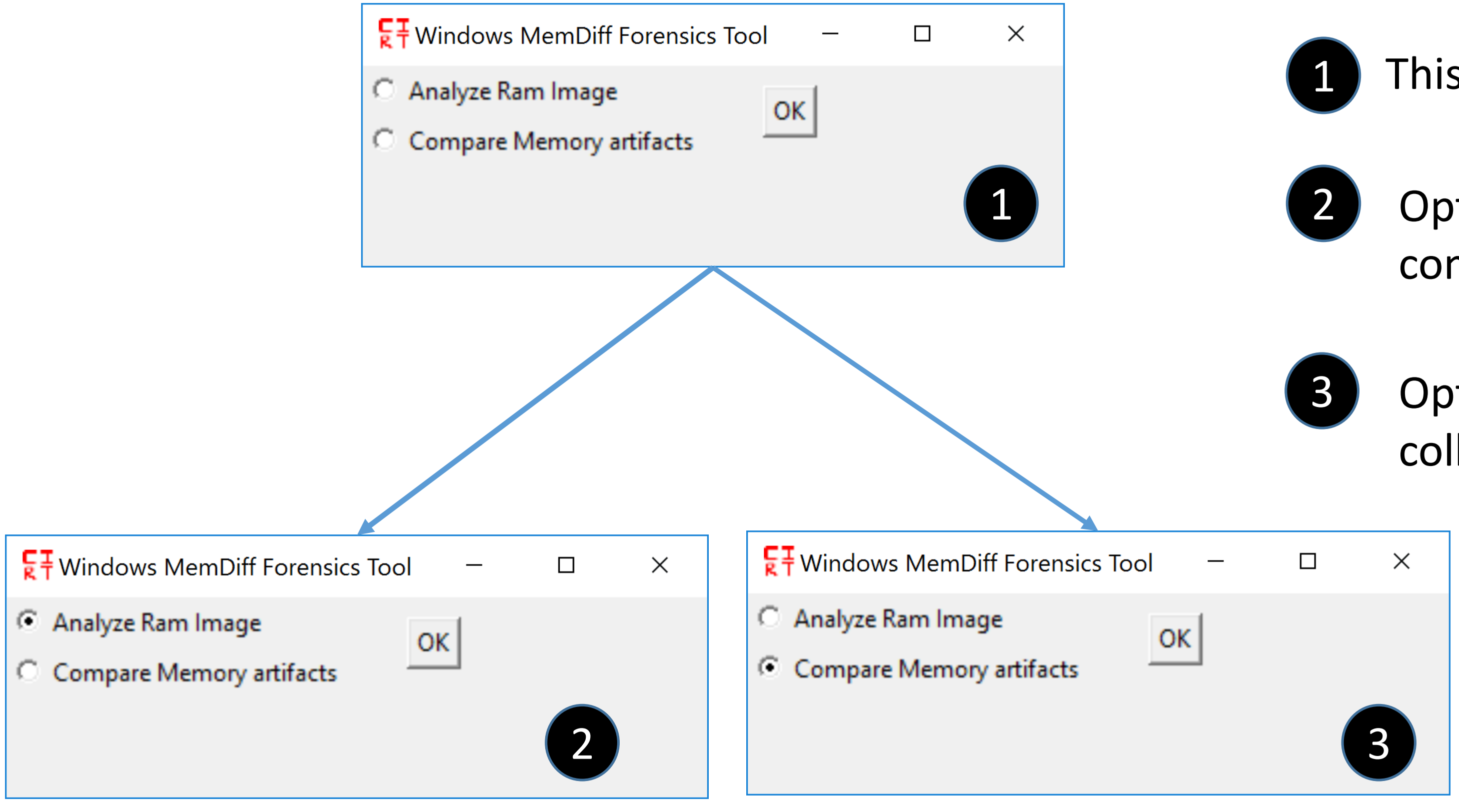
Windows MemDiff Forensics Tool

Developed and documented by :
Hemant Kumar , Sajeev Nair
CIRT-IN , Accenture



Windows MemDiff Forensics Tool

○ Analyze Ram Image

○ Compare Memory artifacts

1

Windows MemDiff Forensics Tool

● Analyze Ram Image

○ Compare Memory artifacts

2

Windows MemDiff Forensics Tool

○ Analyze Ram Image

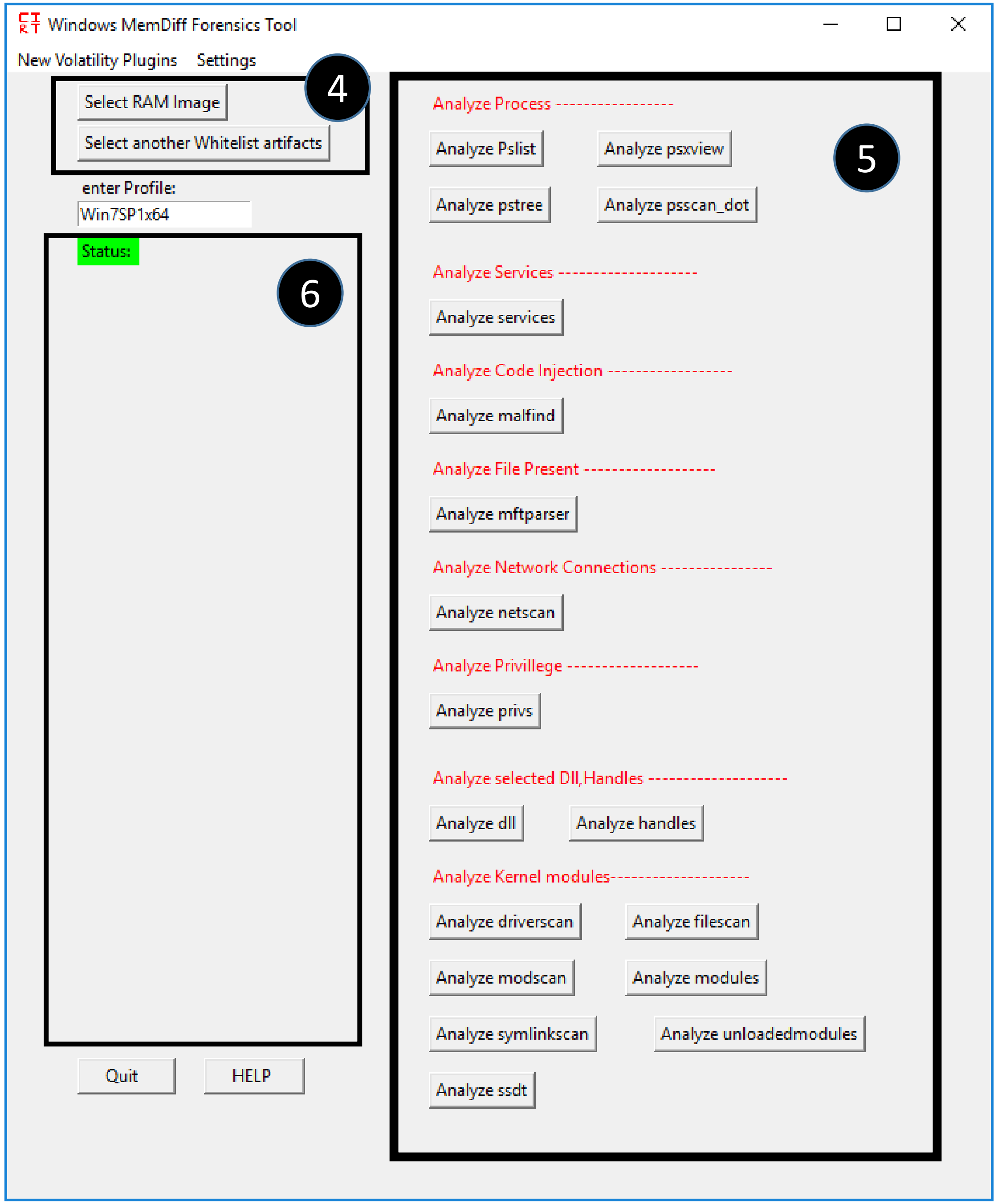
● Compare Memory artifacts

3

1 This is the First Graphical Interface presented to user.

2 Opt for 1st option, If you want to analyze RAM Image and compare its memory artifacts with whitelisted databases.

3 Opt for 2nd option, If you want to compare already collected memory artifacts with whitelisted databases.


Windows MemDiff Forensics Tool
New Volatility Plugins
Settings
Select RAM Image
Select another Whitelist artifacts
4
Status:
6
Quit
HELP
Analyze Process ----------------
Analyze Pslist
Analyze psxview
5
Analyze pstree
Analyze psscan_dot
Analyze Services -------------------
Analyze services
Analyze Code Injection -----------------
Analyze malfind
Analyze File Present ------------------
Analyze mftparser
Analyze Network Connections ---------------
Analyze netscan
Analyze Privillege ------------------
Analyze privs
Analyze selected Dll,Handles ------------------
Analyze dll
Analyze handles
Analyze Kernel modules------------------
Analyze driverscan
Analyze filescan
Analyze modscan
Analyze modules
Analyze symlinkscan
Analyze unloadedmodules
Analyze ssdt

enter Profile: Win7SP1x64

4 By clicking this button "Select RAM Image" user can select the RAM Image to be analyzed of our choice. By clicking "Select another Whitelist artifacts" user can select whitelist database of their choice for comparison rather than default whitelist databases.

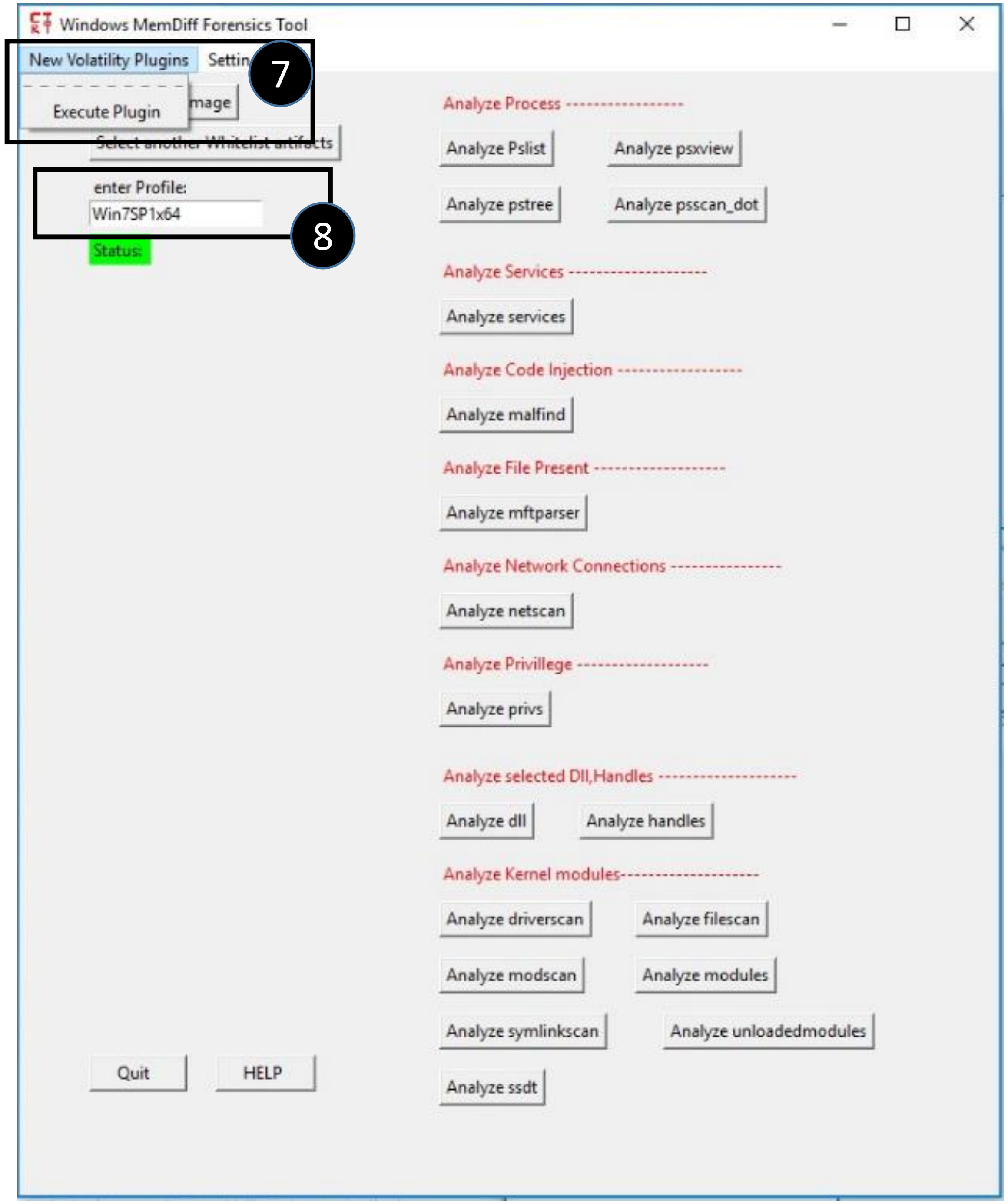
5 This area contains buttons that :

a) Execute specific plugins of volatility.

b) Calculates the difference between the extracted and whitelisted information.

c) After calculating the difference it displays it either in excel or text format.

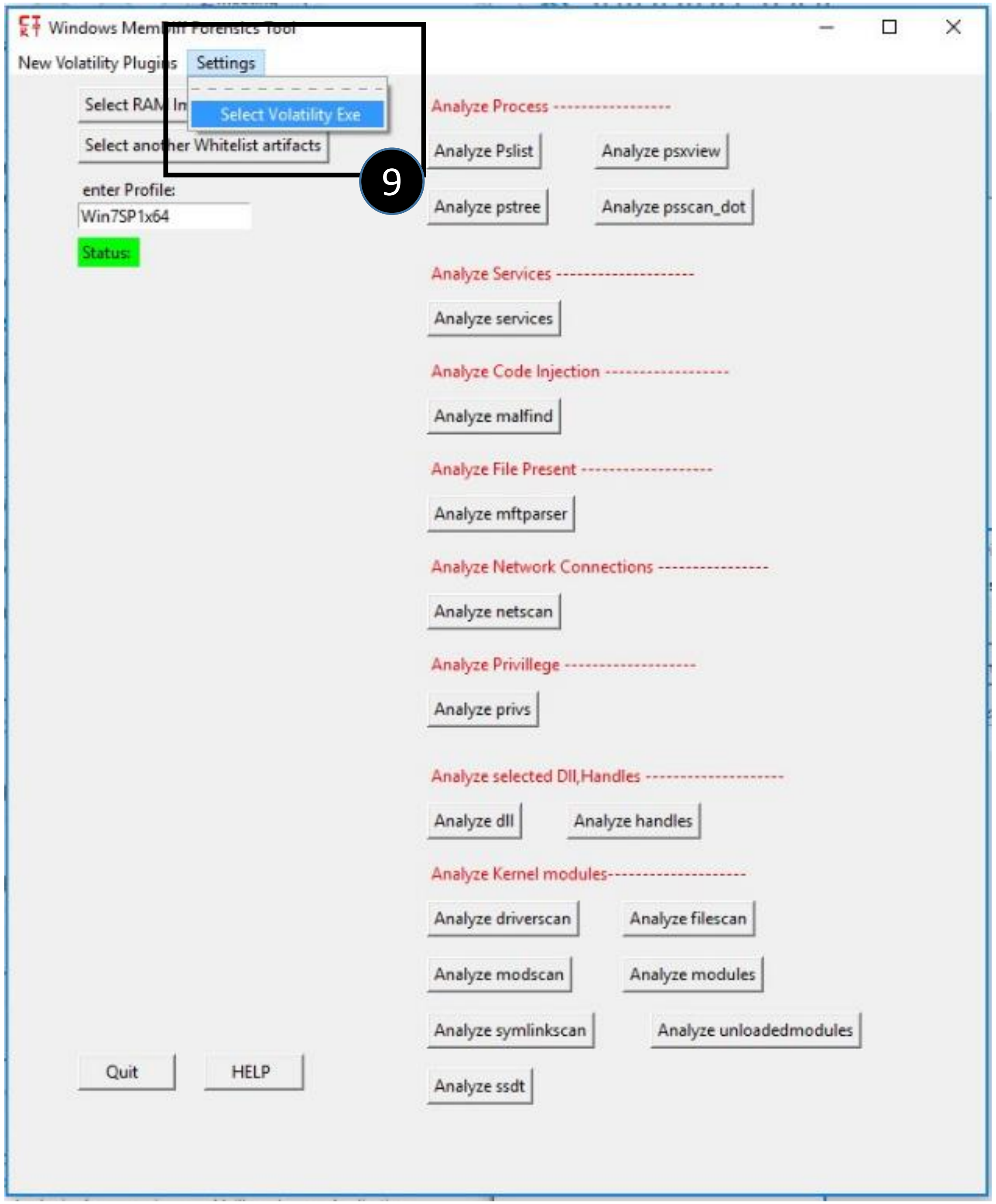
6 This is the status bar area that displays what all plugins difference has been calculated and also displays error that occurred during processing.


Windows MemDiff Forensics Tool
New Volatility Plugins
Settin
7
Execute Plugin
mage
Select another Whitelist artifacts
8
Status:
Analyze Process -----------------
Analyze Pslist
Analyze psxview
Analyze pstree
Analyze psscan_dot
Analyze Services --------------------
Analyze services
Analyze Code Injection ------------------
Analyze malfind
Analyze File Present -------------------
Analyze mftparser
Analyze Network Connections ----------------
Analyze netscan
Analyze Privillege -------------------
Analyze privs
Analyze selected Dll,Handles --------------------
Analyze dll
Analyze handles
Analyze Kernel modules-------------------
Analyze driverscan
Analyze filescan
Analyze modscan
Analyze modules
Analyze symlinkscan
Analyze unloadedmodules
Analyze ssdt
Quit
HELP

enter Profile: Win7SP1x64

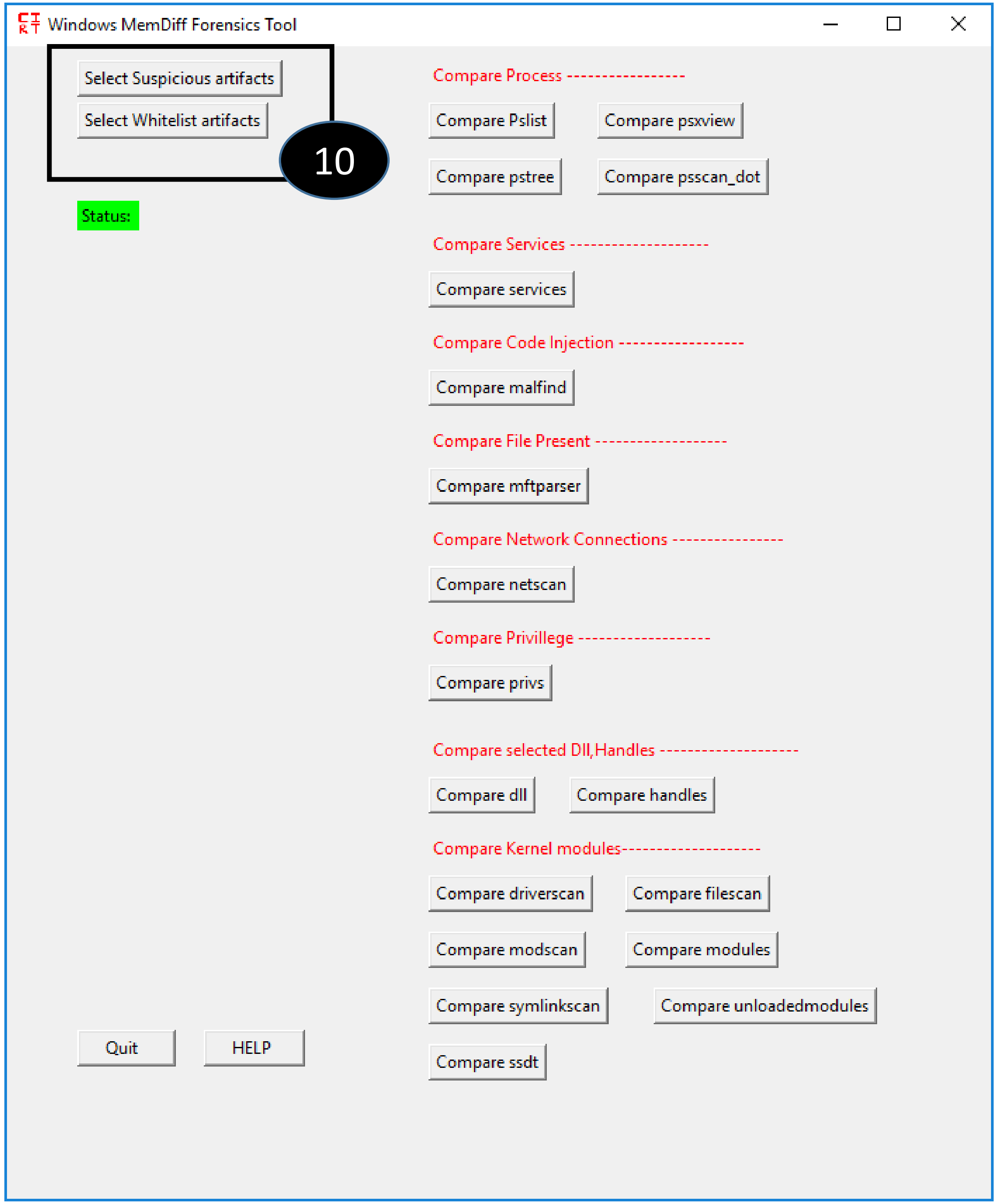
7 Selecting this menu “Execute Plugin”, User can execute any plugin of their choice on the RAM Image.
The Plugin needs to be in Python Compiled Version .pyc

8 Here User can enter profile of the RAM Image.
Default value is Win7SP1x64.



enter Profile: Win7SP1x64

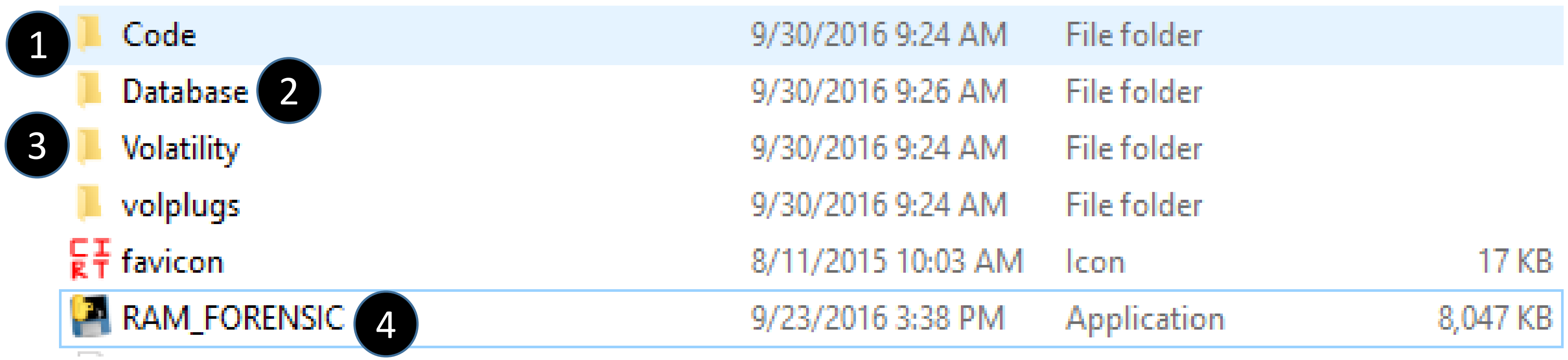
9 Selecting this menu “Select Volatility Exe”, User can select Volatility Framework exe version of their choice.


Windows MemDiff Forensics Tool
Select Suspicious artifacts
Select Whitelist artifacts
10
Status:
Compare Process -----------------
Compare Pslist
Compare psxview
Compare pstree
Compare psscan_dot
Compare Services -------------------
Compare services
Compare Code Injection -----------------
Compare malfind
Compare File Present ------------------
Compare mftparser
Compare Network Connections ---------------
Compare netscan
Compare Privillege ------------------
Compare privs
Compare selected Dll,Handles -------------------
Compare dll
Compare handles
Compare Kernel modules-------------------
Compare driverscan
Compare filescan
Compare modscan
Compare modules
Compare symlinkscan
Compare unloadedmodules
Compare ssdt
Quit
HELP

10 When User select “Compare Memory artifacts” , User can compare artifacts from already extracted artifacts previously using Volatility.

Background folder Structure

This Folder contains the volatility framework exe file that is used to extr
RAM memory.



Code	9/30/2016 9:24 AM	File folder	
Database	9/30/2016 9:26 AM	File folder	
Volatility	9/30/2016 9:24 AM	File folder	
volplugs	9/30/2016 9:24 AM	File folder	
favicon	8/11/2015 10:03 AM	Icon	17 KB
RAM_FORENSIC	9/23/2016 3:38 PM	Application	8,047 KB

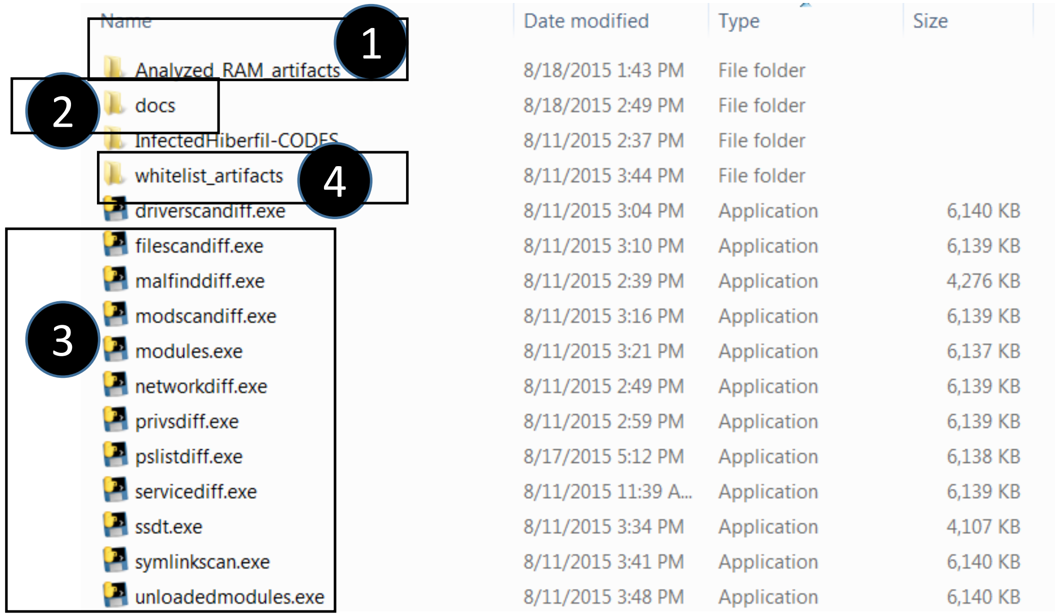
1 This folder contains all the source codes.

2 This Folder contains all the whitelisted artifacts , developed exe's required to calculated differences between current and whitelist artifacts. All extracted artifacts recovered from selected RAM memory are saved inside this folder.

3 This folder contain the Volatility exe itself.

4 This is the main exe file that needs to be run to calculate changes done by malware on computer.

Background folder Structure



Name	Date modified	Type	Size
Analyzed_RAM_artifacts	8/18/2015 1:43 PM	File folder	
docs	8/18/2015 2:49 PM	File folder	
InfectedHiberfil-CODES	8/11/2015 2:37 PM	File folder	
whitelist_artifacts	8/11/2015 3:44 PM	File folder	
driverscandiff.exe	8/11/2015 3:04 PM	Application	6,140 KB
filescandiff.exe	8/11/2015 3:10 PM	Application	6,139 KB
malfinddiff.exe	8/11/2015 2:39 PM	Application	4,276 KB
modscandiff.exe	8/11/2015 3:16 PM	Application	6,139 KB
modules.exe	8/11/2015 3:21 PM	Application	6,137 KB
networkdiff.exe	8/11/2015 2:49 PM	Application	6,139 KB
privsdiff.exe	8/11/2015 2:59 PM	Application	6,139 KB
pslistdiff.exe	8/17/2015 5:12 PM	Application	6,138 KB
servicediff.exe	8/11/2015 11:39 A...	Application	6,139 KB
ssdt.exe	8/11/2015 3:34 PM	Application	4,107 KB
symlinkscan.exe	8/11/2015 3:41 PM	Application	6,140 KB
unloadedmodules.exe	8/11/2015 3:48 PM	Application	6,140 KB

1 This folder contains all the artifacts recovered from selected RAM memory.

2 The doc file is present inside this folder.

3 This are the exe file that are executed to calculate differences between current and whitelisted artifacts .

4 This folder contains all whitelisted artifcats.

Important Information

1. Most of the Whitelisted database memory artifacts should be suffixed with *whi.

 These are:

Driverscanwhi.txt, networkwhi.txt
Filescanwhi.txt, privswhi.txt
Malfindwhi.txt, pslistwhi.txt
Modscanwhi.txt, pstreewhi.txt
Moduleswhi.txt, servicewhi.txt
Ssdtwhi.txt,symlinkscanwhi.txt,unloadedmoduleswhi.txt

2. Most of the artifacts collected from suspicious RAM Image should be suffixed with *inf.

These are:

Driverscaninf.txt, networkinf.txt
Filescaninf.txt, privsinf.txt
Malfindinf.txt, pslistinf.txt
Modscaninf.txt, pstreeinf.txt
Modulesinf.txt, serviceinf.txt
Ssdtinf.txt,symlinkscaninf.txt,unloadedmodulesinf.txt