

When executing the bash script as any user other than Root , the script will let you know that you need to be Root in order to continue using it. →

```
(kali@kali)-[~/Desktop]
$ bash TMagen773628.s3.WF.sh
You're not root. Please run as root and try again.

(kali@kali)-[~/Desktop]
$
```

```
(root@kali)-[/home/kali/Desktop]
# bash TMagen773628.s3.WF.sh
You're running as root. Let's go!
Enter the full path to your memory file:

```

→ When executing the bash script as Root, the script will let the user know that he is Root and will continue.  
The script asks the user for a path to a memory file in order to continue with the investigation.

The user must provide the full path for a memory file.

```
(root@kali)-[/home/kali/Desktop]
# bash TMagen773628.s3.WF.sh
You're running as root. Let's go!
Enter the full path to your memory file:
/home/kali/Desktop/memdump.mem
```

```
(root@kali)-[/home/kali/Desktop]
# bash TMagen773628.s3.WF.sh
You're running as root. Let's go!
Enter the full path to your memory file:
/home/kali/Desktop/memdump.mem
Found the file: memdump.mem!
[+] Binwalk is already installed!
[+] foremost is already installed!
[+] bulk_extractor is already installed!
[+] strings is already installed!
DONE!
What memory file would you like to investigate? HDD/RAM/ALL
```

After providing the full path, the user is asked what kind of file he is investigating. HDD, RAM or ALL , meaning both HDD and RAM.

```
(root@kali)-[/home/kali/Desktop]
# bash TMagen773628.s3.WF.sh
You're running as root. Let's go!
Enter the full path to your memory file:
/home/kali/Desktop/memdump.mme
Invalid file path! Try again.
Enter the full path to your memory file:

```

The script can understand when a wrong path was typed or miss input occurred, and tell the user to try again.

```
(root@kali)-[/home/kali/Desktop]
# bash TMagen773628.s3.WF.sh
You're running as root. Let's go!
Enter the full path to your memory file:
/home/kali/Desktop/memdump.mme
Invalid file path! Try again.
Enter the full path to your memory file:
/home/kali/Desktop/memdump.mem
Found the file: memdump.mem!
[+] Binwalk is already installed!
[+] foremost is already installed!
[+] bulk_extractor is already installed!
[+] strings is already installed!
DONE!
What memory file would you like to investigate? HDD/RAM/ALL
asd
Wrong input. try again.
[+] Binwalk is already installed!
[+] foremost is already installed!
[+] bulk_extractor is already installed!
[+] strings is already installed!
DONE!
What memory file would you like to investigate? HDD/RAM/ALL

```

```

(root@kali)-[/home/kali/Desktop]
# sudo rm -r Volatility_Tool

(root@kali)-[/home/kali/Desktop]
# bash TMagen773628.s3.WF.sh
You're running as root. Let's go!
Enter the full path to your memory file:
/home/kali/Desktop/memdump.mem
Found the file: memdump.mem!
[+] Binwalk is already installed!
[+] foremost is already installed!
[+] bulk_extractor is already installed!
[+] strings is already installed!
DONE!
What memory file would you like to investigate? HDD/RAM/ALL
HDD
Running Binwalk ...
TMagen773628.s3.WF.sh: line 63: 248841 Killed sudo binwalk --run-as=root -e --directory=$HOME/Volatility_Tool/$NAME $file > /dev/null 2>&1
Running Foremost ...
Running Bulk_Extractor ...
Running Strings ...
Found a PCAP file! Size: 234040 Location: /home/kali/Desktop/Volatility_Tool/memdump.mem/Bulk_Extractor
ls: cannot access '/home/kali/Desktop/Volatility_Tool/memdump.mem//home/kali/Desktop/memdump.mem': No such file or directory
All findings are shown in the Report file.
adding: memdump.mem/ (stored 0%)
adding: memdump.mem/Report.txt (deflated 60%)
adding: memdump.mem/Volatility_res.txt (deflated 76%)
adding: memdump.mem/_memdump.mem-0.extracted/ (stored 0%)
adding: memdump.mem/_memdump.mem-0.extracted/31C06A.zip (stored 0%)
adding: memdump.mem/_memdump.mem-0.extracted/66B002.7z (deflated 69%)
adding: memdump.mem/_memdump.mem.extracted/ (stored 0%)
adding: memdump.mem/_memdump.mem.extracted/31C06A.zip

```

HDD – Running the HDD option starts the forensic tool Binwalk, Foremost, Bulk Extractor and Strings.

Then, the script looks for a PCAP file inside the Bulk Extractor folder, and if a PCAP file is found the size and path location of the PCAP file is given to the user.

All of the forensic findings are saved into the report file.

Then, everything is zipped into a zip file.

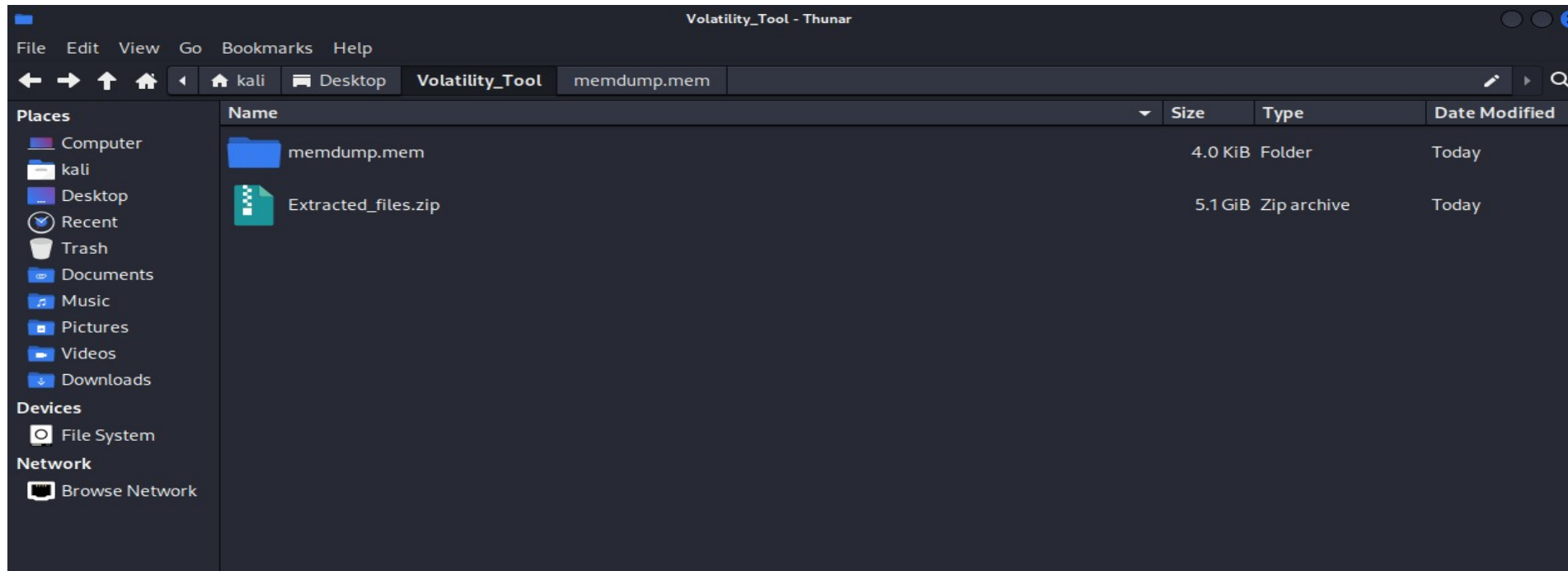
```

(root@kali)-[/home/kali/Desktop]
# bash TMagen773628.s3.WF.sh
You're running as root. Let's go!
Enter the full path to your memory file:
/home/kali/Desktop/memdump.mem
Found the file: memdump.mem!
[+] Binwalk is already installed!
[+] foremost is already installed!
[+] bulk_extractor is already installed!
[+] strings is already installed!
DONE!
What memory file would you like to investigate? HDD/RAM/ALL
RAM
Volatility Foundation Volatility Framework 2.5
INFO      : volatility.debug      : Determining profile based on KDBG search...
Using memory profile: Win7SP0x64
Running: pstree
Volatility Foundation Volatility Framework 2.5
Running: connscan
Volatility Foundation Volatility Framework 2.5
ERROR     : volatility.debug      : This command does not support the profile Win7SP0x64
Running: hivelist
Volatility Foundation Volatility Framework 2.5
Running: printkey
Volatility Foundation Volatility Framework 2.5
Done analyzing memdump.mem! Results are saved in: /home/kali/Desktop/Volatility_Tool/memdump.mem/Volatility_res.txt
All findings are shown in the Report file.
  adding: memdump.mem/ (stored 0%)
  adding: memdump.mem/Report.txt (stored 0%)
  adding: memdump.mem/Volatility_res.txt (deflated 76%)
  adding: memdump.mem/_memdump.mem-0.extracted/ (stored 0%)
  adding: memdump.mem/_memdump.mem-0.extracted/31C06A.zip

```

RAM – Running the RAM option starts Volatility with some command, such as: pstree, connscan, hivelist and printkey. All of the command findings are saved into the report file. Then, everything is zipped into a zip file.

\*If the ALL option is selected, the script will do HDD and RAM together.



When the script finishes, all of the files will show up at the folder created by the script in a zip file.