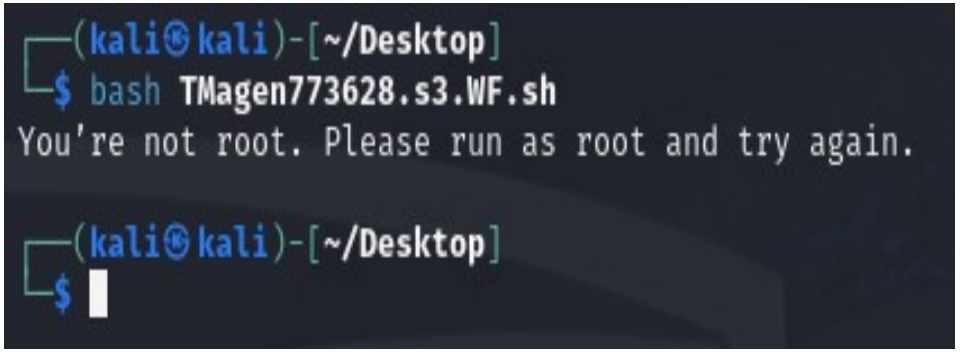
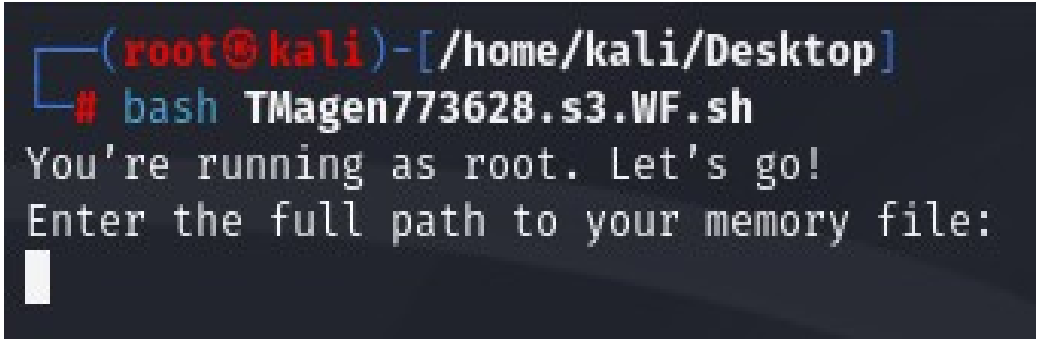
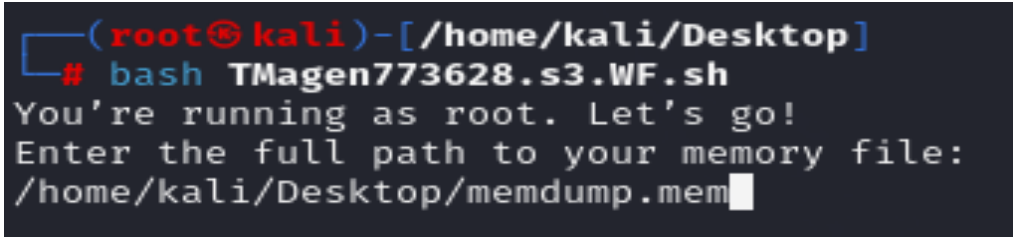
When executing the bash script as any user other than Root , the script will let you know that you need to be Root in order to continue using it. →

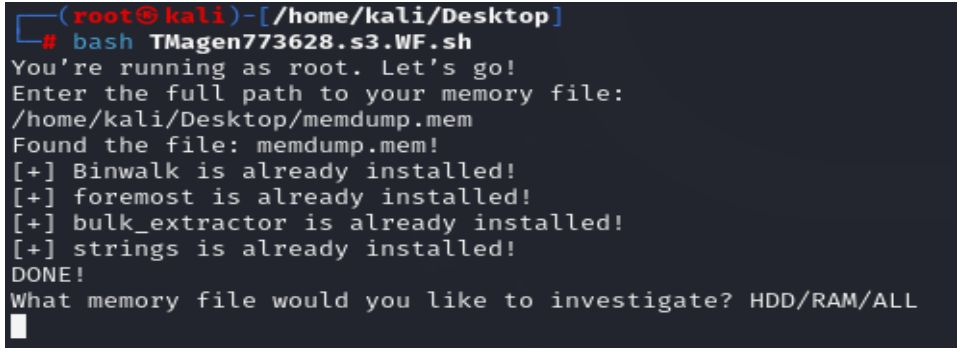




→ When executing the bash script as Root, the script will let the user know that he is Root and will continue.
The script asks the user for a path to a memory file in order to continue with the investigation.

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



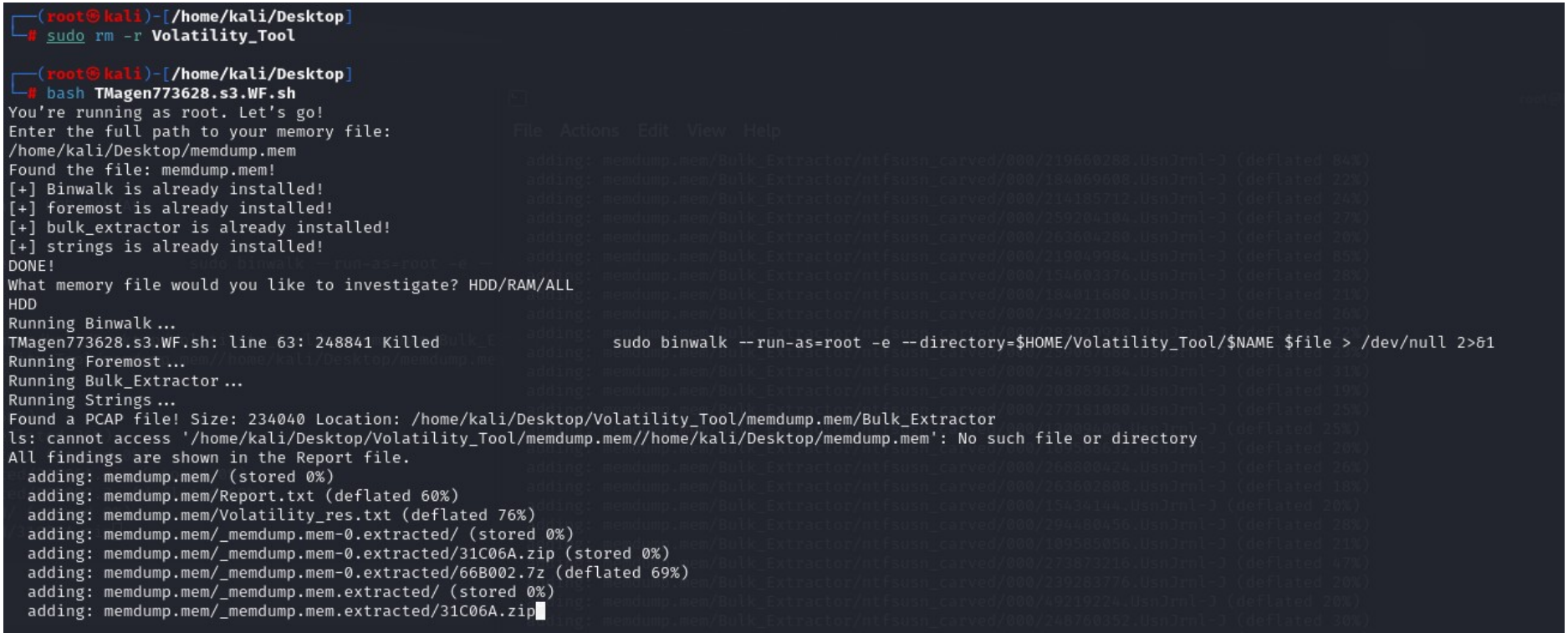


After providing the full path, the user is asked what kind of file he is investigating. HDD, RAM or ALL , meaning both HDD and RAM.

```
┌──(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
```

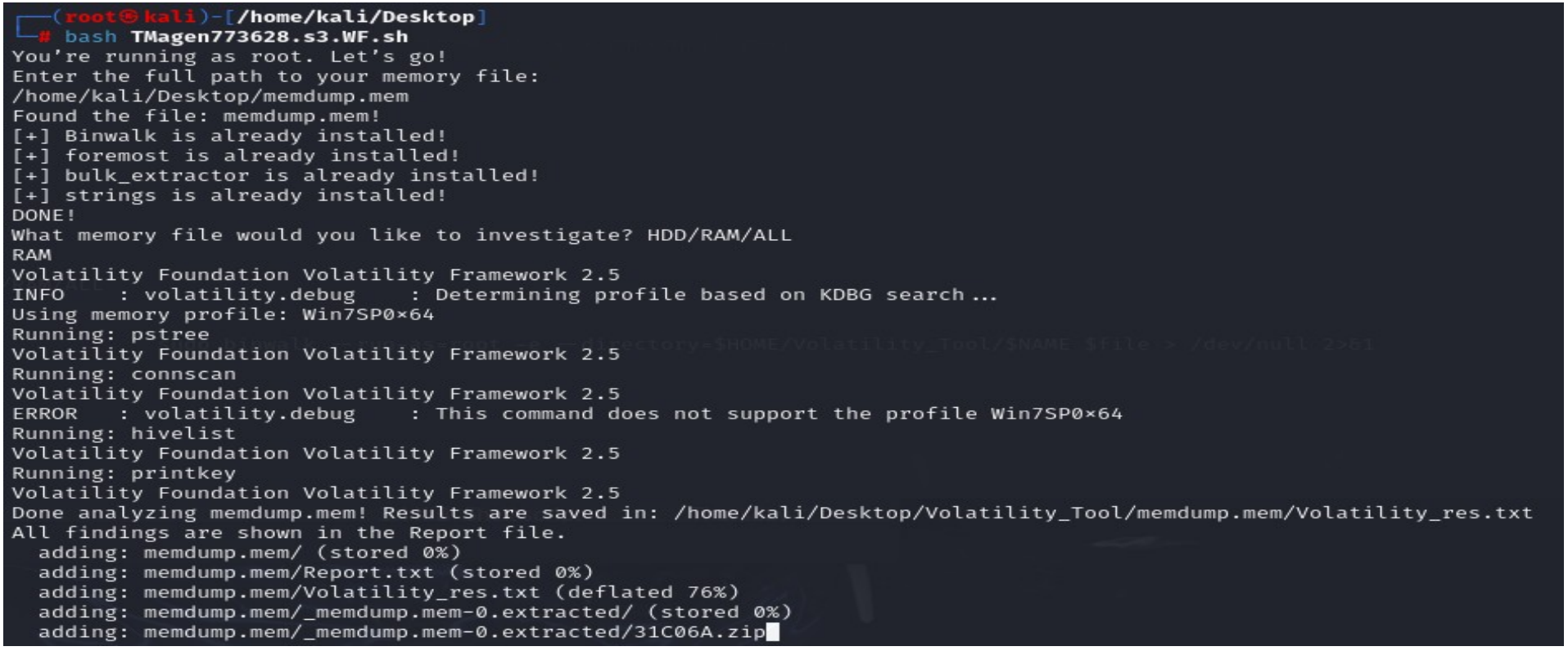


HDD – Running the HDD option starts the forensic tool Binwalk, Foremost, Bulk Extractor and Strings.

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.

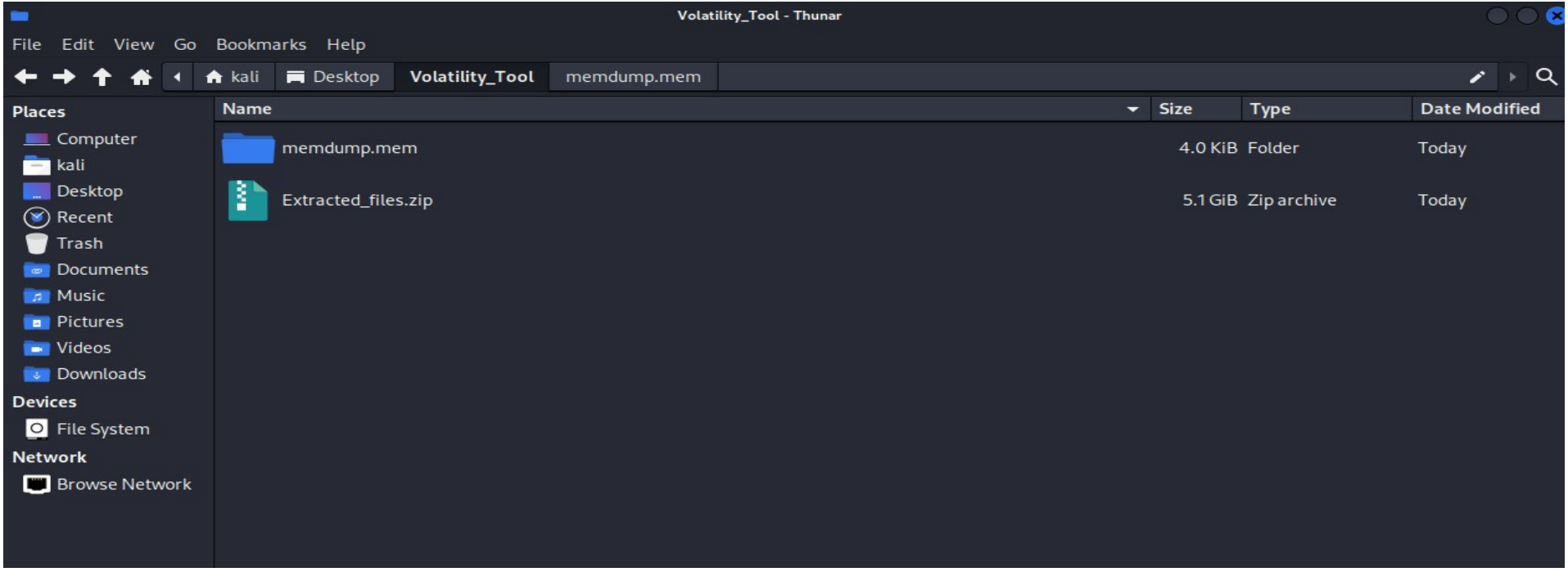
All of the forensic findings are saved into the report file.

Then, everything is zipped into a zip file.



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.