

## MemAnalyzer.sh

1. Check the current user, if not root exit.
2. Request the user to submit file for analysis.
3. Check if automatic carving forensic tools are installed. If missing – install.

```
root@kali: /home/kali/Desktop
File Actions Edit View Help
(kali㉿kali)-[~/Desktop]
$ ./MemAnalyzer.sh
[-] You need to be root to run this script. Exiting ...

(kali㉿kali)-[~/Desktop]
$ sudo -i
[sudo] password for kali:
(kali㉿kali)-[~/]
# cd /home/kali/Desktop

(kali㉿kali)-[~/Desktop]
# ./MemAnalyzer.sh
[>] Welcome to Memory Analyzer!
[>] Please specify filename including full path for analysis:
dump2.mem
[+] You submitted: dump2.mem

[>] Checking if automatic carving tools are installed ...

[-] binwalk is not installed, installing ...
[+] binwalk installed successfully
```

1. Automatic file carving. Option for the user to choose a carver or use all available carvers.

```
[+] foremost is already installed
[+] bulk_extractor is already installed
[+] strings is already installed

[>] Extracting data with carvers

[>] Carving mode:
Enter C to choose a carver to use
Enter A to use all available carvers (Binwalk, Foremost, Bulk_extractor, Strings)C
[>] Which carver do you want to use?
Enter 1 for Binwalk
2 for Foremost
3 for Bulk_Extractor
4 for Strings (looking for human-readable data)3
[>] Extracting data with Bulk_Extractor... it might take a while
[+] Done

[>] Do you want to use another carver? y/n
y

[>] Extracting data with carvers
```

- 1.Extracting data with Bulk\_Extractor and Strings.
2. Option for the user to submit to Strings keywords.
- 3.Results are saved into files.

```
[→] Extracting data with carvers

[→] Carving mode:
Enter C to choose a carver to use
Enter A to use all available carvers (Binwalk, Foremost, Bulk_extractor, Strings)C
[→] Which carver do you want to use?
Enter 1 for Binwalk
2 for Foremost
3 for Bulk_Extractor
4 for Strings (looking for human-readable data)4
[→] Extracting data with Strings. Looking for keywords: exe, password, username, http...
[→] Do you want to submit your keyword y/n?
y
[→] Enter your keyword:
root
$Microsoft Root Certificate Authority
?http://crl.microsoft.com/pki/crl/products/microsoftrootcert.crl0T
8http://www.microsoft.com/pki/certs/MicrosoftRootCert.crt0
{*..1106.287C.0.0.0.00000000.00020000}, \    ;; bit 17 PCI_HACK_IGNORE_ROOT_TOPOLOGY
```

- 1.Pcap file detection.
2. Checks if the submitted file is a memory file that can be analyzed with Volatility.
- 3.If yes – start running volatility plugins.
4. Results are saved into files.

```
Baltimore CyberTrust Root0
-http://cybertrust.omniroot.com/repository.cfm0
1http://cdp1.public-trust.com/CRL/Omniroot2025.crl0
Nb37\SystemRoot\System32\drivers\etc\lmhosts
[+] Done. Results are saved
[→] Do you want to submit another keyword? y/n
n

[+] Done

[→] Do you want to use another carver? y/n
n
[+] All results are saved in: Analyzer/dump2.mem

[!]Detected pcap network file. Saved in:
/home/kali/Desktop/Analyzer/dump2.mem/bulk_results
[+] Network file size: 1.2M
[→]Analyzing file with Volatility. Trying to extract profile ...
This might take a few minutes
[+]Extracted profile is: VistaSP1x86
[→]Running pstree plugin
```

1. General statistics.
2. Option to zip the results.
3. Bye-bye

```
[→]Running pslist plugin
[→]Running psscan plugin
[→]Running connscan plugin
[→]Running netscan plugin
[→]Running hivelist plugin
[→]Running hivedump plugin
[→]Running consoles plugin

[→] Statistics:

[+]Analysis completed in 8 minutes and 29 seconds
[+]Found 19165 files
[+]All results are saved in /home/kali/Desktop/Analyzer/dump2.mem
[→] Do you want to zip the extracted files? y/ny
[+] Done. Archive dump2.mem.tar is saved in /home/kali/Desktop/Analyzer. Bye-bye
```