Project : ANALYZER

This script is an automated forensic analysis tool designed to process memory dumps and other files, extracting meaningful information for forensic investigations. It performs the following key tasks:

1. **Environment**: Ensures the required forensic tools (binwalk, bulk_extractor, foremost, Volatility) are installed and prepares a structured directory for case files.
2. **File Analysis**:
    - Uses **Volatility** to analyze memory dumps, extract profiles, process lists, network connections, registry hives, and other forensic artifacts.
    - Executes **carving tools** such as binwalk, bulk_extractor, and foremost to extract embedded data and artifacts like executables and PCAP files.
    - Utilizes strings to search for sensitive information, including usernames, passwords, and hidden data.
3. **Reporting**:
    - Logs all actions and results to a central log file.
    - Counts and summarizes extracted files.
    - Compresses the output into a ZIP file.

```
┌──(kali㉿kali)-[~/Desktop]
└─$ bash TMagen773632.s16.nx212.sh
Logging started at Wed Nov 27 04:43:36 AM EST 2024
────── Starting START at Wed Nov 27 04:43:36 AM EST 2024 ──────
You are not root.. exiting...
```

- The script needs the user ‘root’ to operate.
  In the example you can see that the script checks for ‘root’ user.

```
┌──(kali㉿kali)-[~/Desktop]
└─$ sudo su root
[sudo] password for kali:
┌──(root㉿kali)-[/home/kali/Desktop]
└─# bash TMagen773632.s16.nx212.sh
Logging started at Wed Nov 27 04:45:52 AM EST 2024
────── Starting START at Wed Nov 27 04:45:52 AM EST 2024 ──────
You are root.. continuing..
Please enter a full path to the file you would like to investigate:
```

- After using the script with user ‘root’, the user needs to give a full path to the file that is being investigated.

```
You are root.. continuing..
Please enter a full path to the file you would like to investigate:
/kali/home/mumdump.mem
/kali/home/mumdump.mem is not found... exiting...
```

- The script checks whether the file exists. If not it terminates the process.

```
You are root.. continuing..
Please enter a full path to the file you would like to investigate:
/home/kali/Desktop/memdump.mem
/home/kali/Desktop/memdump.mem exists, continuing....
Creating a directory for the case...
```

- The script creates a new directory named forensic_case to store all the gathered info on the investigated file.

```
Archive:  /home/kali/Desktop/dJ0xloCr26lr
   creating: /home/kali/Desktop/vol/
  inflating: /home/kali/Desktop/vol/AUTHORS.txt
  inflating: /home/kali/Desktop/vol/CREDITS.txt
  inflating: /home/kali/Desktop/vol/LEGAL.txt
  inflating: /home/kali/Desktop/vol/LICENSE.txt
  inflating: /home/kali/Desktop/vol/README.txt
  inflating: /home/kali/Desktop/vol/vol
  inflating: /home/kali/Desktop/vol/volatility_2.5_linux_x86
binwalk is already installed
bulk_extractor is already installed
foremost is already installed
------ Starting CARVERS at Wed Nov 27 05:24:12 AM EST 2024 ------
```

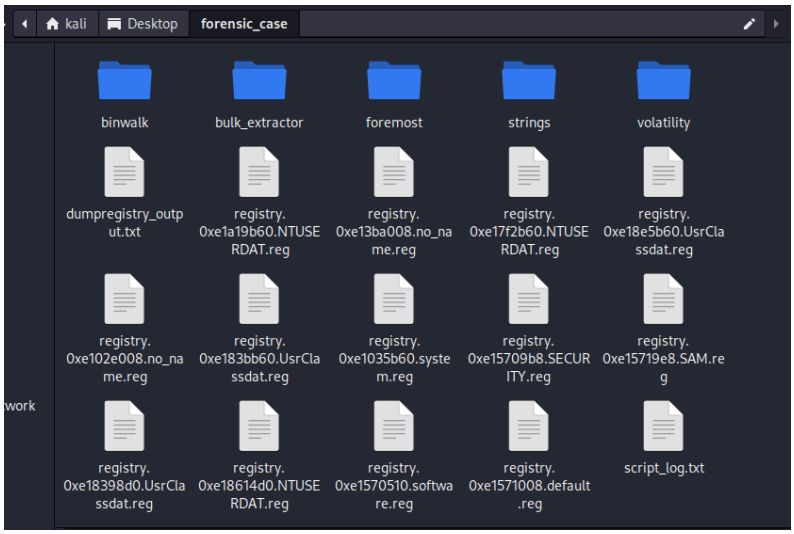
- The script installs the Volatility tool, and checks if binwalk, bulk_extractor and foremost tools are installed. If the tools are not found it will install them.

```
[+] Checking for PCAP file....
packets.pcap
PCAP file was found! Location: /home/kali/Desktop/forensic_case/bulk_extractor
File size: 103629 bytes
```

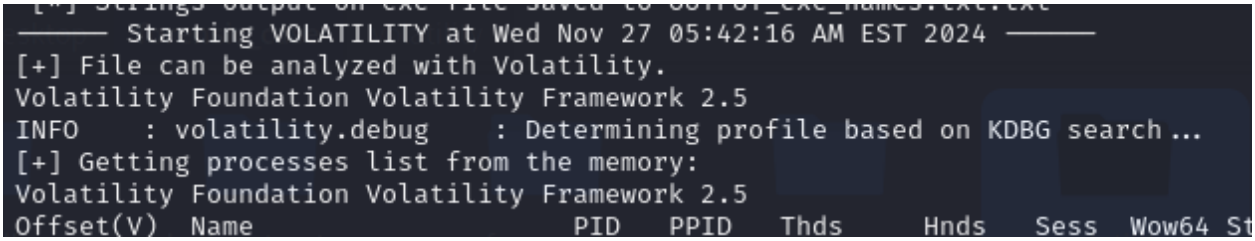
- The script checks for ‘pcap’ file, if found - displays location and size.

```
EXE file was found! Location: /home/kali/Desktop/forensic_case/foremost/exe/00000294.exe
File size: 230400 bytes
 [*] Strings output on exe file saved to OUTPUT_00000294.exe.txt
EXE file was found! Location: /home/kali/Desktop/forensic_case/foremost/exe/00002360.exe
File size: 83072 bytes
```

- The script checks for exe file, if found - displays location and size.

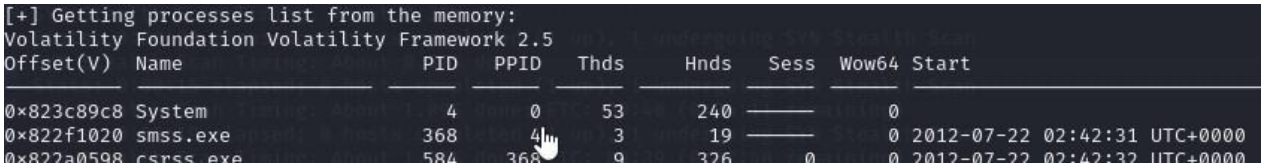


- The directories of the tools we use to investigate. Using the tools to extract data and readable strings from the investigated file. The extracted data is then securely stored for further analysis.

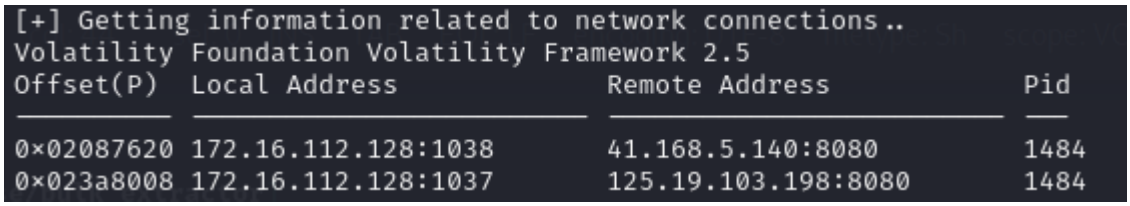


- The script verifies the compatibility of the Volatility tool by determining whether a valid profile can be identified using the “imageinfo” command.

- The profile is stored as a variable to facilitate data extraction using Volatility.



- Displays process list.



- Displays network connections.

```
[+] Making an attempt to provide hive list:
Volatility Foundation Volatility Framework 2.5
Virtual    Physical   Name
---------- ---------- ----
0x0e18e5b60 0x093f8b60 \Device\HarddiskVolume1\Documents and Settings\Robert\Local Settings\Application Data\
0x0e1a19b60 0x0a5a9b60 \Device\HarddiskVolume1\Documents and Settings\Robert\NTUSER.DAT
0x0e18398d0 0x08a838d0 \Device\HarddiskVolume1\Documents and Settings\LocalService\Local Settings\Application
0x0e18614d0 0x08e624d0 \Device\HarddiskVolume1\Documents and Settings\LocalService\NTUSER.DAT
0x0e183bb60 0x08e2db60 \Device\HarddiskVolume1\Documents and Settings\NetworkService\Local Settings\Applicati
0x0e17f2b60 0x08519b60 \Device\HarddiskVolume1\Documents and Settings\NetworkService\NTUSER.DAT
0x0e1570510 0x07669510 \Device\HarddiskVolume1\WINDOWS\system32\config\software
0x0e1571008 0x0777f008 \Device\HarddiskVolume1\WINDOWS\system32\config\default
0x0e15709b8 0x076699b8 \Device\HarddiskVolume1\WINDOWS\system32\config\SECURITY
0x0e15719e8 0x0777f9e8 \Device\HarddiskVolume1\WINDOWS\system32\config\SAM
0x0e13ba008 0x02e4b008 [no name]
0x0e1035b60 0x02ac3b60 \Device\HarddiskVolume1\WINDOWS\system32\config\system
0x0e102e008 0x02a7d008 [no name]
Volatility Foundation Volatility Framework 2.5
**************************************************
Writing out registry: registry.0x0e18e5b60.UsrClassdat.reg

**************************************************
**************************************************
Writing out registry: registry.0x0e1a19b60.NTUSERDAT.reg
```

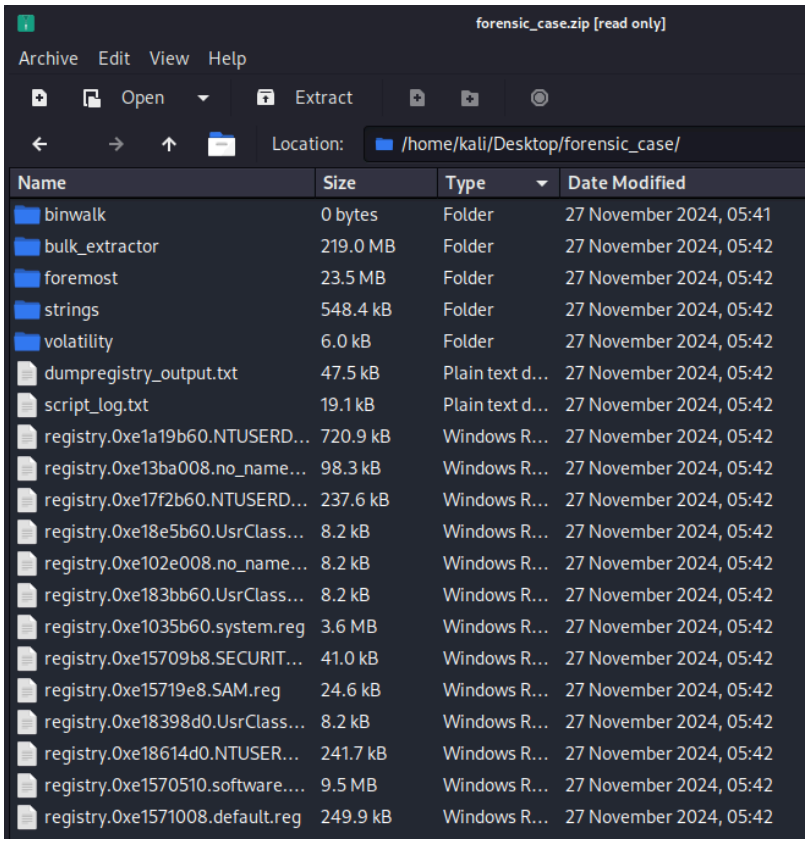
- The script attempts to extract hive list and dump registries.

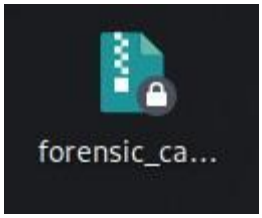
```
[*] The number of files extracted is: 3610
------ Finished Volatility at Wed Nov 27 06:39:41 AM EST 2024 ------
------ Forensic_case directory has been zipped to forensic_case.zip ------
------ Finished at Wed Nov 27 06:39:46 AM EST 2024 ------
```

- The script provides a summary of the total number of extracted files and logs the completion time. Additionally, the entire forensic_case directory, including the log file (report and extracted data in TXT format), is compressed into a ZIP file.

```
echo "[+] Getting processes list from the memory:" | tee -a "$LOG_FILE"
$HOME/vol/vol -f $file --profile=$PROFILE pslist | tee -a "$HOME/forensic_case/volatility/processes.txt"

$HOME/vol/vol -f $file --profile=$PROFILE connscan | tee -a "$HOME/forensic_case/volatility/connections_scan.txt"

$HOME/vol/vol -f $file --profile=$PROFILE hivelist | tee -a "$HOME/forensic_case/volatility/hives.txt"

$HOME/vol/vol -f $file --profile=$PROFILE dumpregistry --dump-dir $HOME/forensic_case | tee -a "$HOME/forensic_case/dumpregistry_output.txt"

$HOME/vol/vol -f $file --profile=$PROFILE printkey -K "SAM\\Domains\\Account\\Users\\Names" | tee -a "$HOME/forensic_case/volatility/SAM_usernames.txt

$HOME/vol/vol -f $file --profile=$PROFILE printkey -K "Software\\Microsoft\\Windows\\CurrentVersion\\Run" | tee -a "$HOME/forensic_case/volatility/executables_names.txt"
```

- Each command line to extract data with volatility is saved in a txt file.





- The forensic_case directory is compressed into ‘forensic_case’ ZIP file with all the data (log report file, txt file of gathered data etc).