PROJECT: ANALYZER

1.1 Check the current user; exit if not ‘root’.

#If not root :

```
┌──(kali㉿kali)-[~/Desktop/projects-final/windows_forensics]
└─$ bash TMagen773637.s14.nx212.sh
Error: This script must be run as root.
```

#As root -

1.2 Allow the user to specify the filename; check if the file exists.

```
===     PROJECT: ANALYZER (NX212)       ===
Please insert the full path of the Image: /home/kali/Desktop/projects-final/windows_forensics/memdump.mem
File exists...
```

1.3 Create a function to install the forensics tools if missing.

#Tools that were not installed

```
Checking if carving tools are installed...
binwalk is not installed, installing...
binwalk installed successfully
foremost is not installed, installing...
foremost installed successfully
bulk_extractor is not installed, installing...
bulk_extractor installed successfully
```

#Tool that is already installed

```
 strings is already installed
```

1.4 Use different carvers to automatically extract data.

1.5 Data should be saved into a directory.

```
---  Section 1: Data Carving & Extraction  ---
Running Foremost...
Foremost results saved to: memdump.mem_analysis_20251106_192939/foremost
Running Binwalk...
Binwalk results saved to: memdump.mem_analysis_20251106_192939/binwalk
Running Bulk Extractor...
Bulk Extractor results saved to:memdump.mem_analysis_20251106_192939/bulk_extractor
```

1.6 Attempt to extract network traffic; if found, display to the user the location and size.

```
Checking for extracted network traffic...
[*] Found Pcap file: memdump.mem_analysis_20251106_211806/bulk_extractor/packets.pcap (Size: 104K)
Running Strings...
```

1.7 Check for human-readable (exe files, passwords, usernames, etc.).

```
Running Strings...
Searching for interesting strings (passwords, users...)
Potential interesting strings saved to: memdump.mem_analysis_20251106_192939/strings/interesting_strings.txt
```

2.1 Check if the file can be analyzed in Volatility; if yes, run Volatility.

2.2 Find the memory profile and save it into a variable.

```
---  Section 2: Volatility Memory Analysis  ---
Attempting to identify memory profile...
[*] Success! Profile identified:WinXPSP2x86
```

2.3 Display the running processes.

2.4 Display network connections.

2.5 Attempt to extract registry information.

```
Starting to run Volatility plugins...
--- Running Plugin: pstree ---
pstree results saved to: memdump.mem_analysis_20251106_192939/vol_pstree.txt
--- Running Plugin: pslist ---
pslist results saved to: memdump.mem_analysis_20251106_192939/vol_pslist.txt
--- Running Plugin: psscan ---
psscan results saved to: memdump.mem_analysis_20251106_192939/vol_psscan.txt
--- Running Plugin: connscan ---
connscan results saved to: memdump.mem_analysis_20251106_192939/vol_connscan.txt
--- Running Plugin: netscan ---
netscan results saved to: memdump.mem_analysis_20251106_192939/vol_netscan.txt
--- Running Plugin: hivelist ---
hivelist results saved to: memdump.mem_analysis_20251106_192939/vol_hivelist.txt
--- Running Plugin: consoles ---
consoles results saved to: memdump.mem_analysis_20251106_192939/vol_consoles.txt
--- Running Plugin: hivedump ---
Attempting to dump registry hives (this may take time)...
Registry hives saved to: memdump.mem_analysis_20251106_192939/registry_hives
All plugins finished.
--- Analysis Complete ---
```

3.1 Display general statistics (time of analysis, number of found files, etc.).

3.2 Save all the results into a report (name, files extracted, etc.).

```
--- [ Section 3: Final Results & Zipping ] ---
Total analysis time: 107 seconds.
Total files found/created (including logs): 29
Main report file located at: memdump.mem_analysis_20251106_192939/report.txt
```

3.3 Zip the extracted files and the report file.

```
Zipping all result files...
[*] Success! All results zipped to: memdump.mem_analysis_20251106_192939.zip
--- Analysis Complete ---
```

DONE!