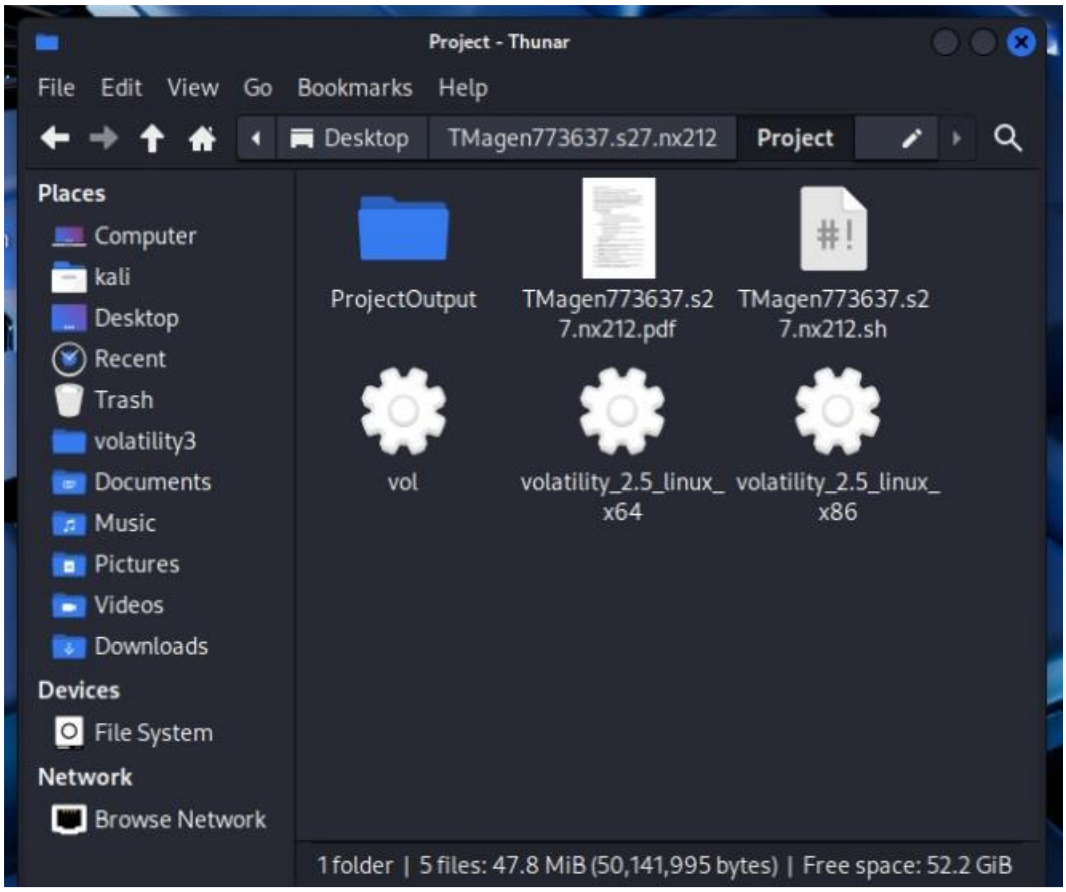
Dor Amihai – John Bryce- class 7736.37 -lecturer's name Erel Regev.

Forensic Investigation Automation Script – Summary

This Bash script is designed to automate memory and disk forensic analysis on Linux-based systems, particularly **Kali Linux**. It provides an interactive terminal interface that guides the user through analyzing a forensic image (typically a memory dump or disk capture). The script ensures the required tools are installed, performs various forensic operations, and compiles the results into a final compressed archive for reporting and review.

This zip file contains:

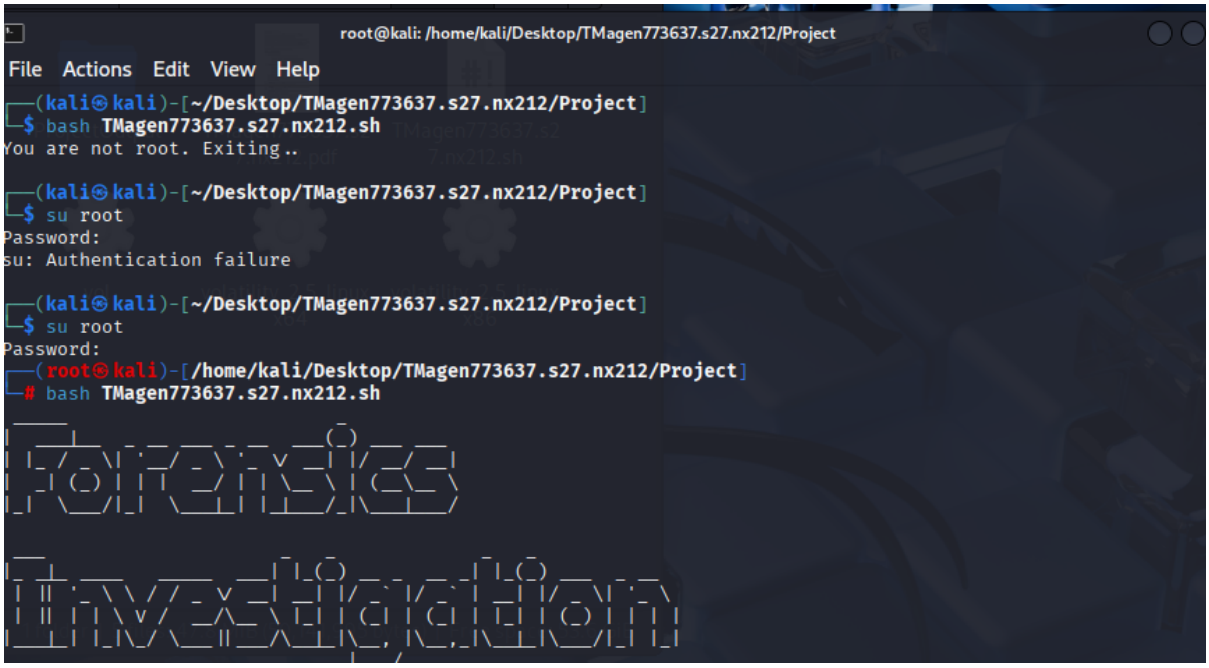
1. Script. 2. Pdf. 3. Voladility stand-alone version 2.5 + lnk (vol).



Features and Capabilities

Environment Setup:

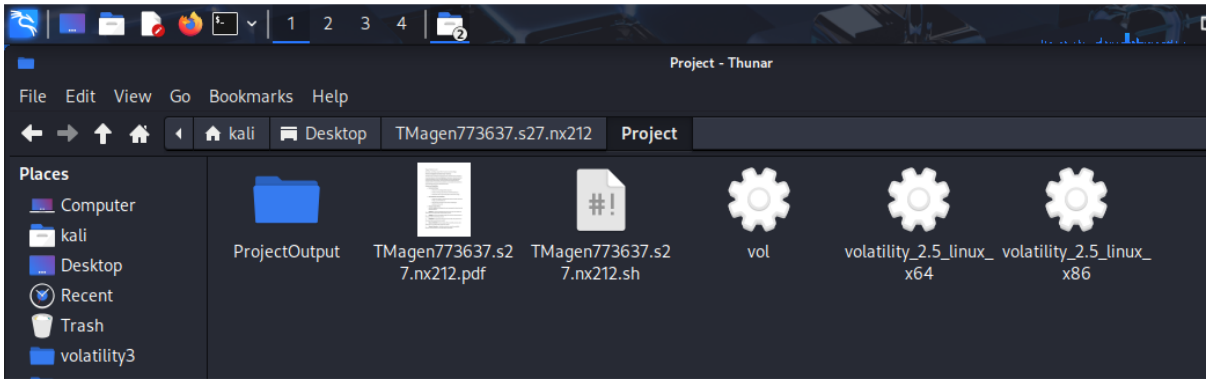
1. Checks for root privileges before execution.



As seen, if you are not root the script will exit. The script will work only for root user.

2. Creates a working output directory named ProjectOutput.

The script uses mkdir command to create a output folder as seen.



3. Prompts the user to input the full path to the forensic image.

As seen: "Please insert full path of image file.

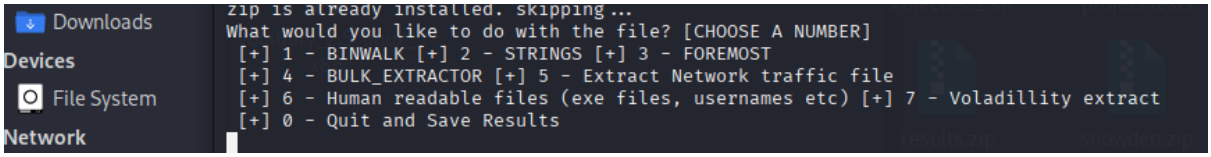
Tool Verification and Installation: Verifies and installs (if missing): bulk_extractor, binwalk, foremost, strings, zip, and Volatility 2.5.

By executing the commands of the (above) checking if exist on the user system. If the script detects that one (or more) of the above are not installed it install it to be ready to use. Voladility 2.5 is attached as standalone – due to Voladility 3.0 is out not – and the project requirements are built for Voladility 2.5 version.

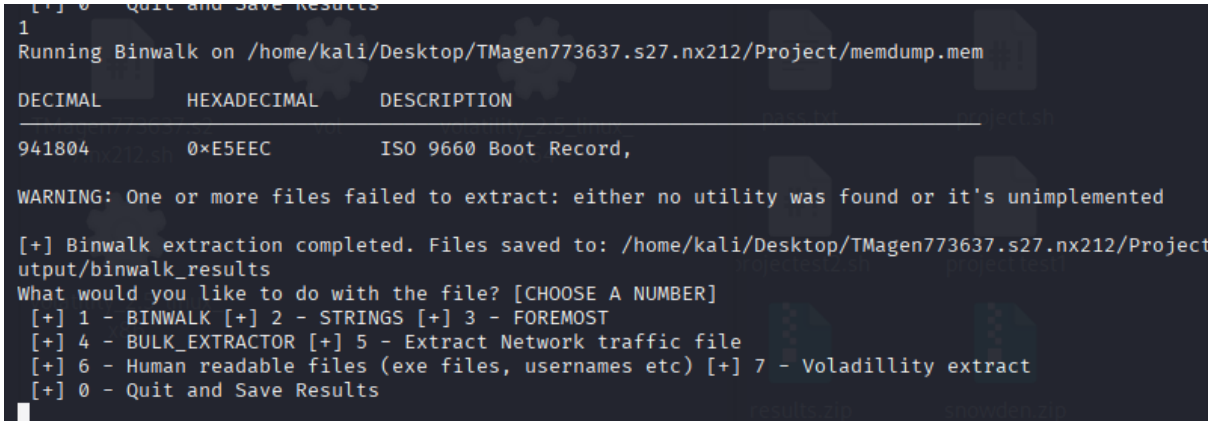
o Sets execution permission and confirms availability of volatility_2.5_linux_x64.

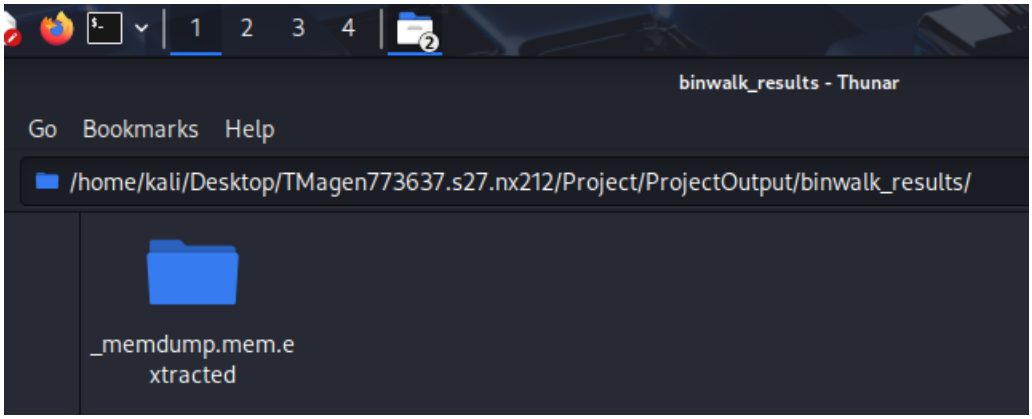
- **Modular Analysis Menu:**

After the image path is validated, the user is prompted to choose from the following options: (The script is smart and works as "loop" – will exit just after entering **0** [results + exit).

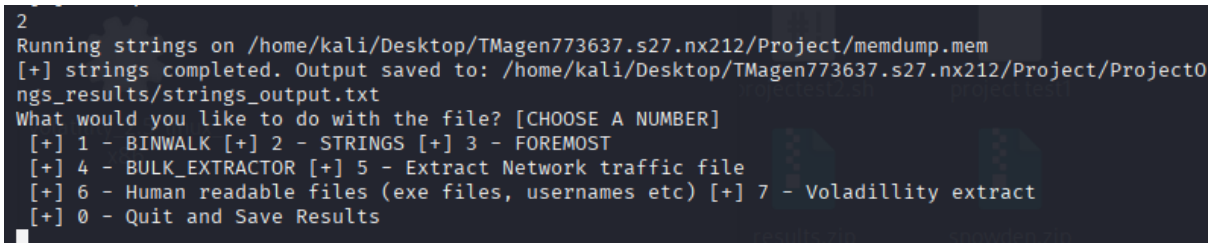


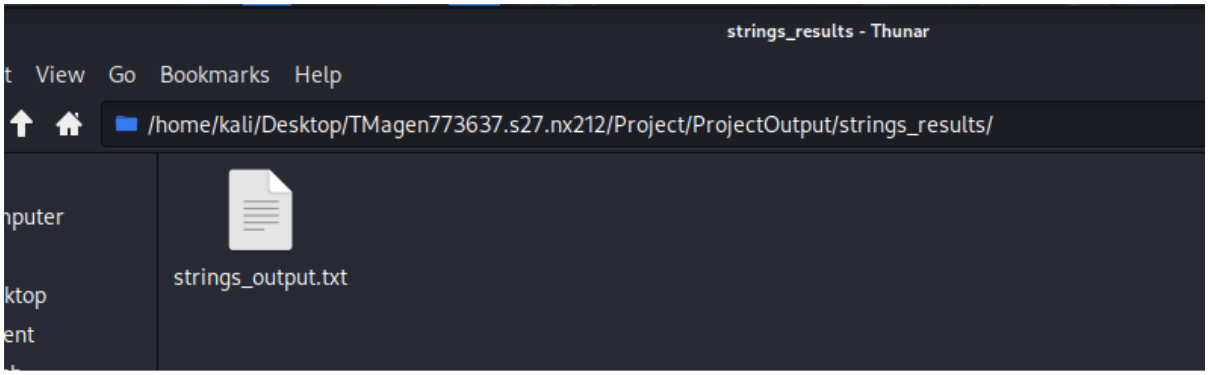
1. BINWALK – Extracts embedded files and firmware from the image. And saves them in the output folder named binwalk_results.



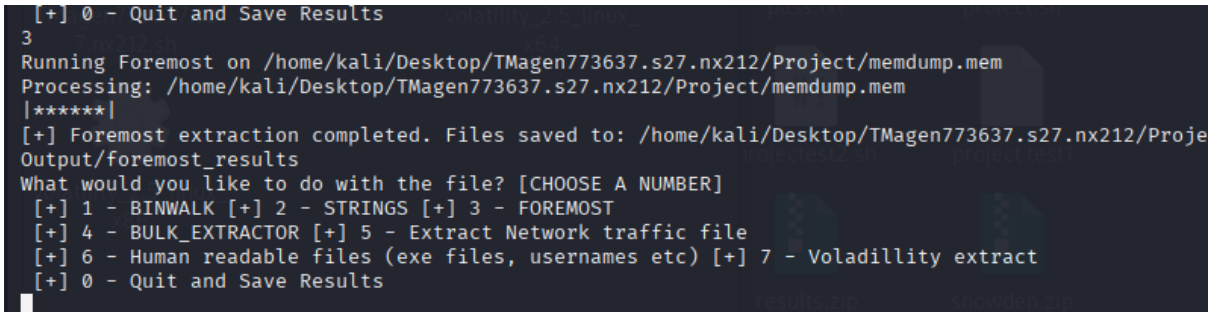


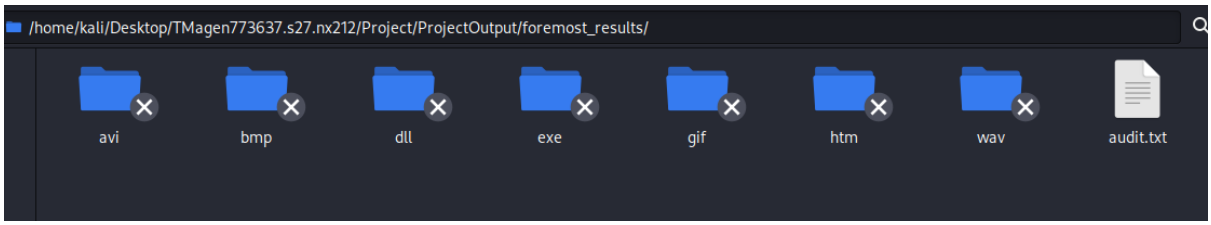
2. STRINGS – Extracts all readable strings into a text file. And saves them in the output folder named strings_results.



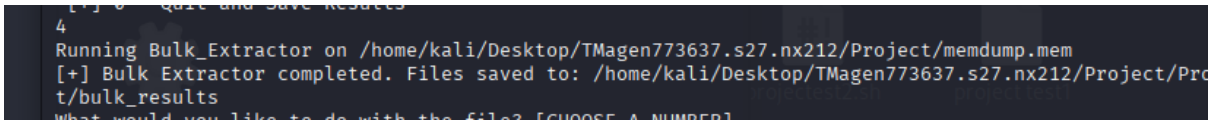


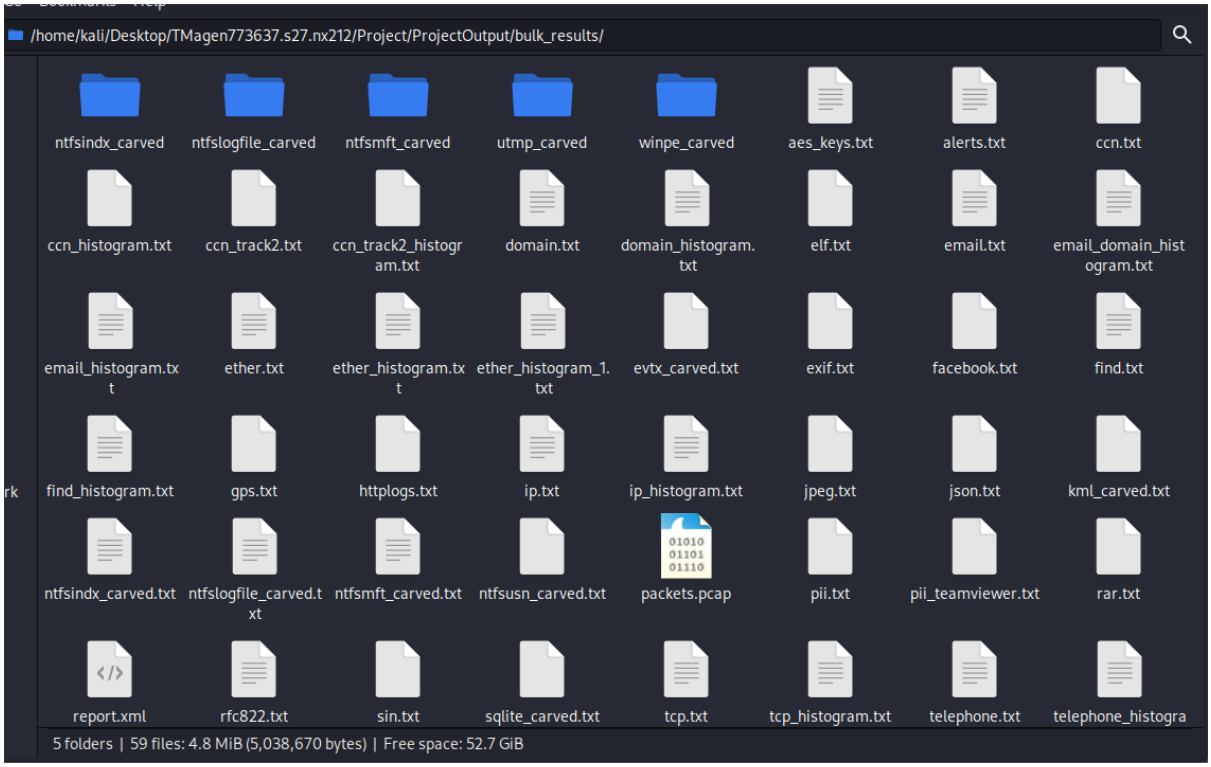
3. FOREMOST – Carves known file types from raw data. And saves them in the output folder named foremost_results.





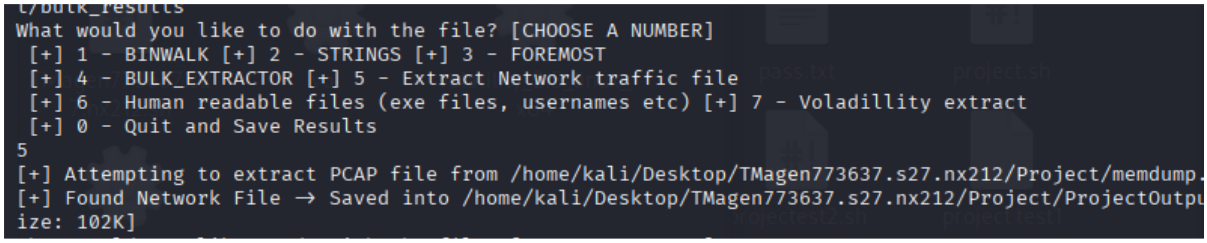
4. BULK_EXTRACTOR – Extracts emails, URLs, net traffic, and more. And saves them in the output folder named bulk_results.

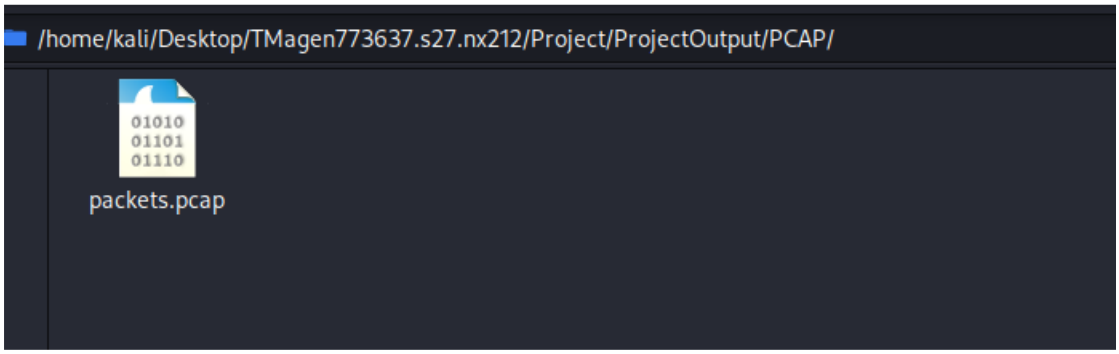




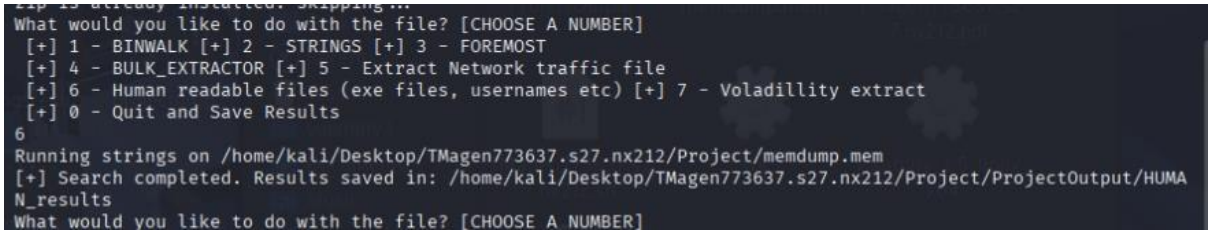
5. Network Extraction – Identifies and extracts .pcap files using Bulk Extractor. And saves them in the output folder named Pcap.

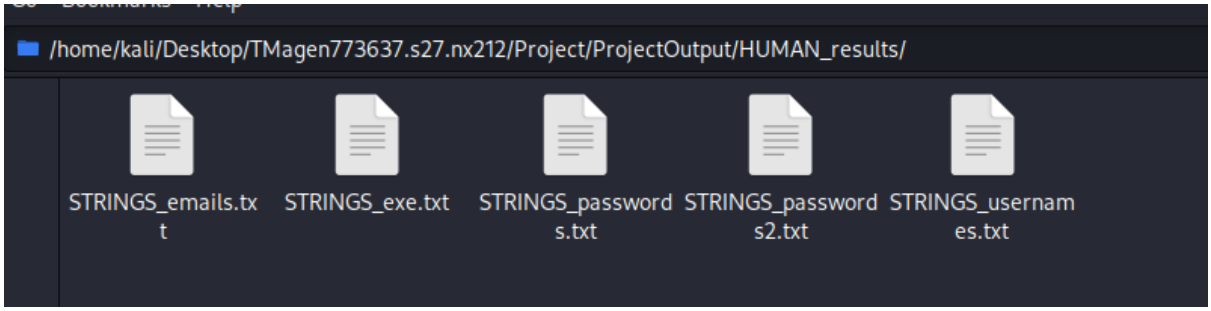
The script first saving the result after excluding most of foremost options by ignore executable file types and **Only extract** network info HTTP logs, and maybe hidden pcap's in compressed files. The result is saved in temp folder – than the script is copying the PCAP file to the Pcap folder and delete the temp folder.



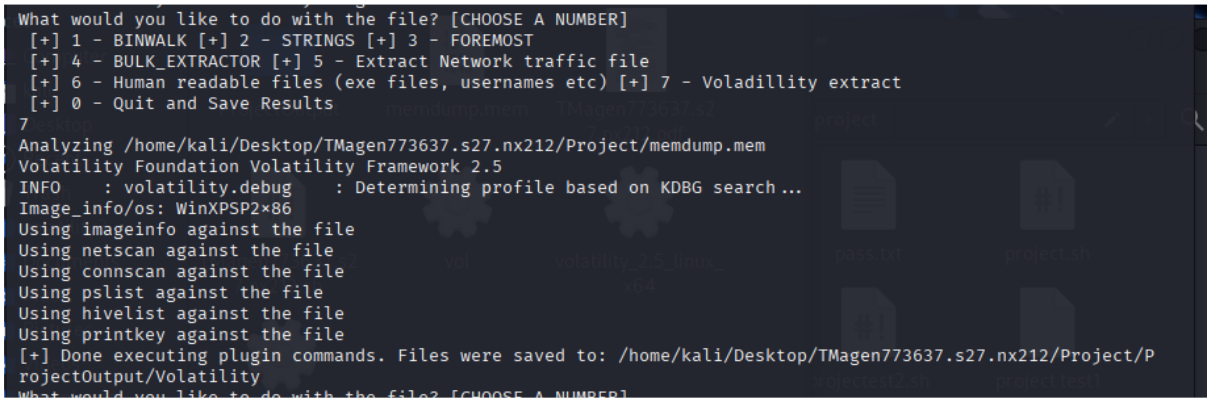


6. Human Readable Data – Searches for email addresses, .exe filenames, passwords, and usernames via strings and grep. And saves them in the output folder named Human_Result. The results are in few files. Pay attention for two Passwords txt files. One is trying locating password by the next word after "pass or password". Second is trying locating password including words contains the word "pass" within.

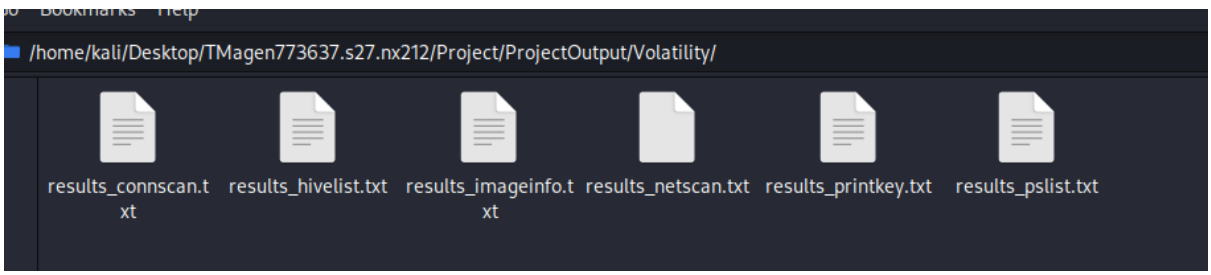




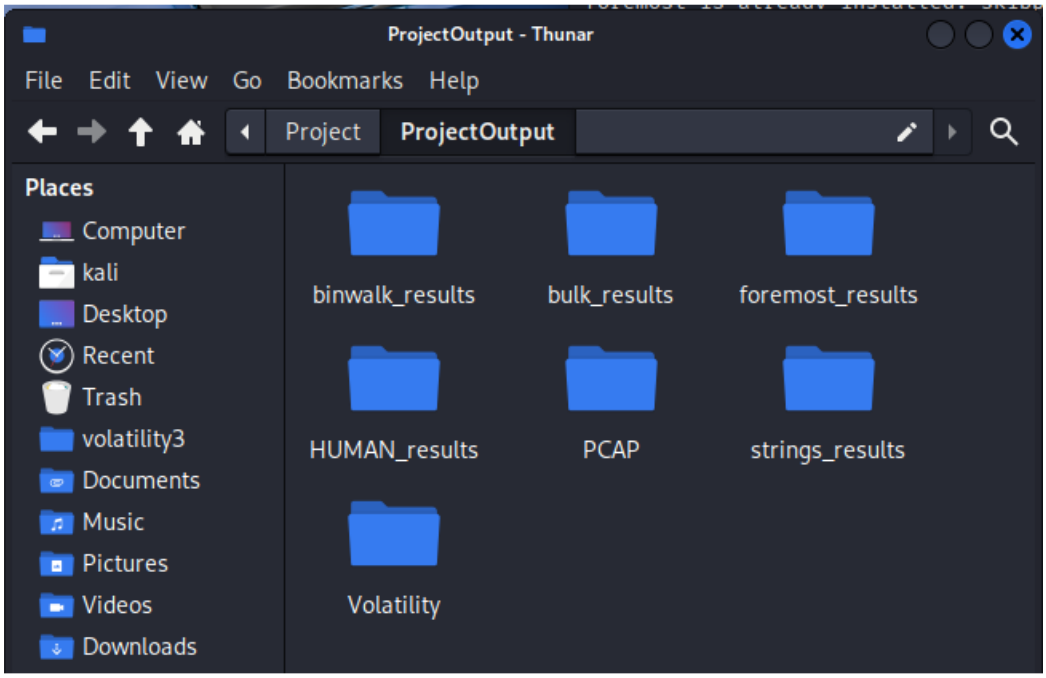
7. **Volatility 2.5 Analysis** – Detects the correct profile and runs multiple plugins including imageinfo, pslist, hivelist, connscan, netscan, and printkey. In order to find running processes, memory profile, network connections, extracting system information all displayed in the output folder of Voladility.



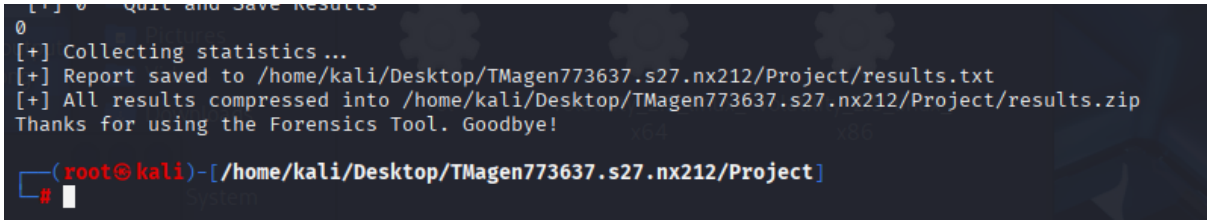
As seen the Image info is represented to the user. And all the results are saved in specific folder.



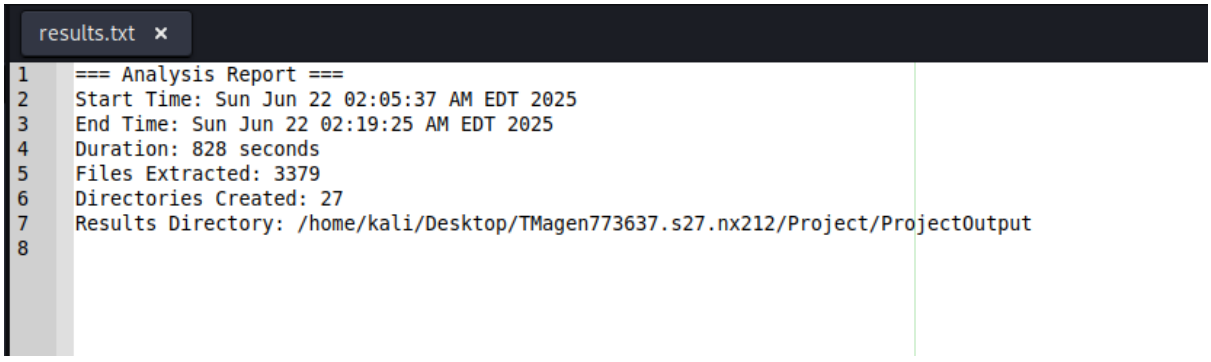
The output folder "Projectoutput" looks like this after using all options:



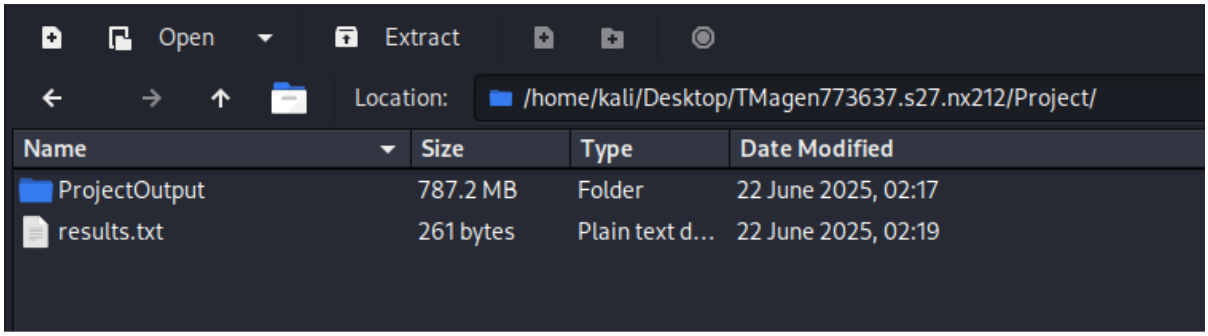
• **Result Collection and Archiving (Quitting thescript) (Option 0):**



o Analyze analysis time, number of files/directories created, and stores this in a results.txt report.



o Compresses the entire ProjectOutput directory along with the report into a results.zip file.



You don’t have to use all options to get the analaysis (time etc) and the compressed outputfolder. It's up to you how much time you will use the script and what option you will choose.

Script (attached) includes notes ## explaining each command. The script is silent and friendly regards to dev null command.

Best Regards,

Dor Amihai