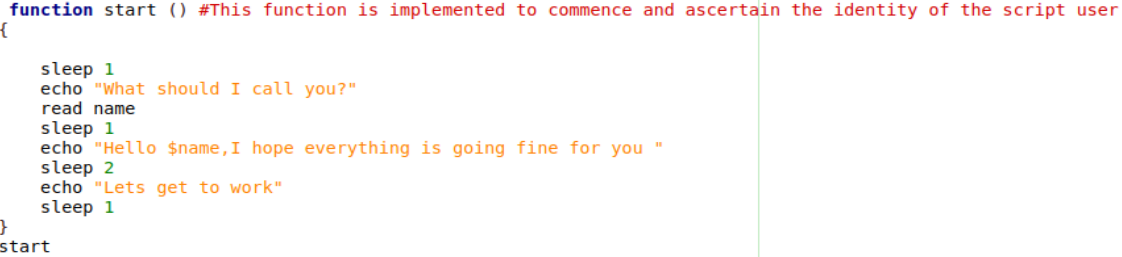
windows forensics project

Peleg odi

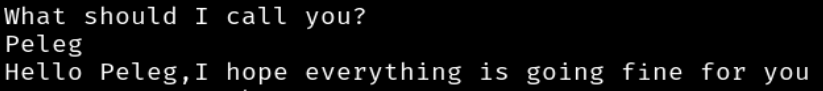
S24

function details

input:

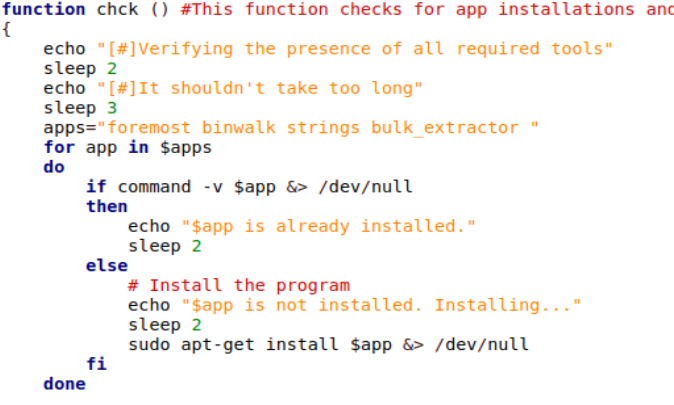


Output:

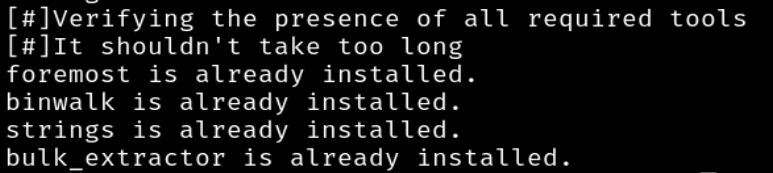


Function "start"-This function is implemented to commence and ascertain the identity of the script user.

Input:

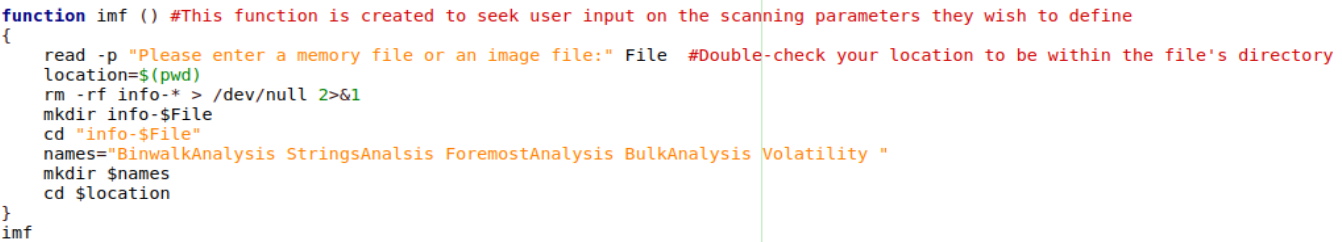


Output:



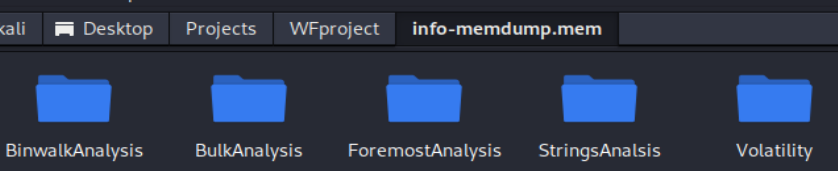
Function"chck"-This function checks for app installations and takes care of installing them if they are missing.

Input:



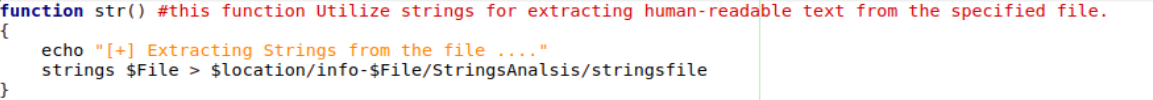
Output:





Function "imf"-this function Asks the user for a file (memory or image), Creates a new directory named "info and the name of the file",Inside this directory, it create "BinwalkAnalysis", "StringsAnalsis" files.

Input:

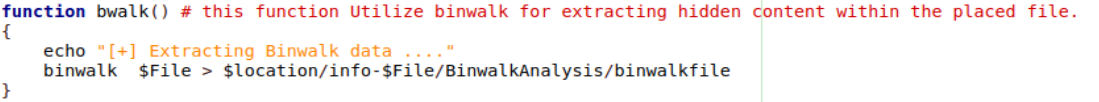


Output:



Function "str"-this function Utilize strings for extracting human-readable text from the specified file.

Input:

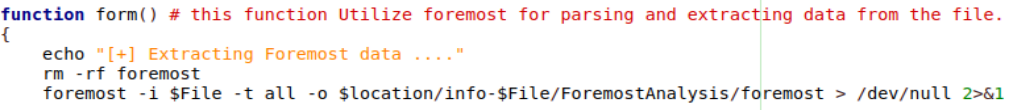


Output:



Function "bwalk"-this function Utilize binwalk for extracting hidden content within the placed file.

Input:



Output:



Function "form"-this function Utilize foremost for parsing and extracting data from the file.

Input:

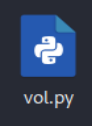


Output:

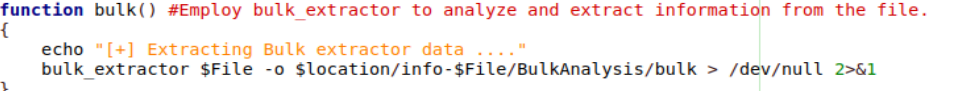


Function "vot+voldown"-this function Removes any existing files or directories related to the Volatility tool.

Uses Volatility to gather information about the file we placed in the script and stores the output in a file named vol.py



Input:

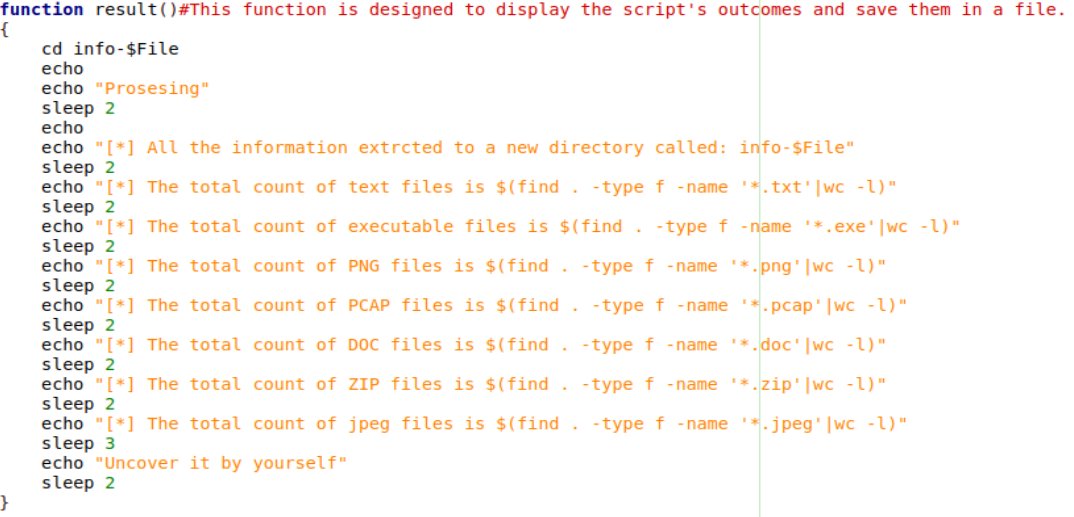


Output:

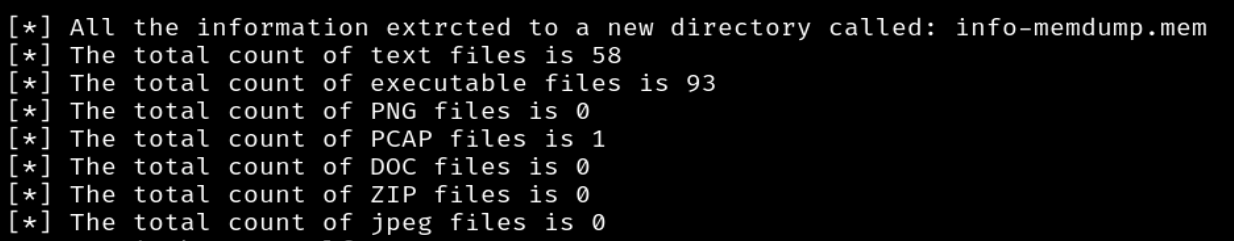


Function "bulk"-Employ bulk\_extractor to analyze and extract information from the file.

Input:

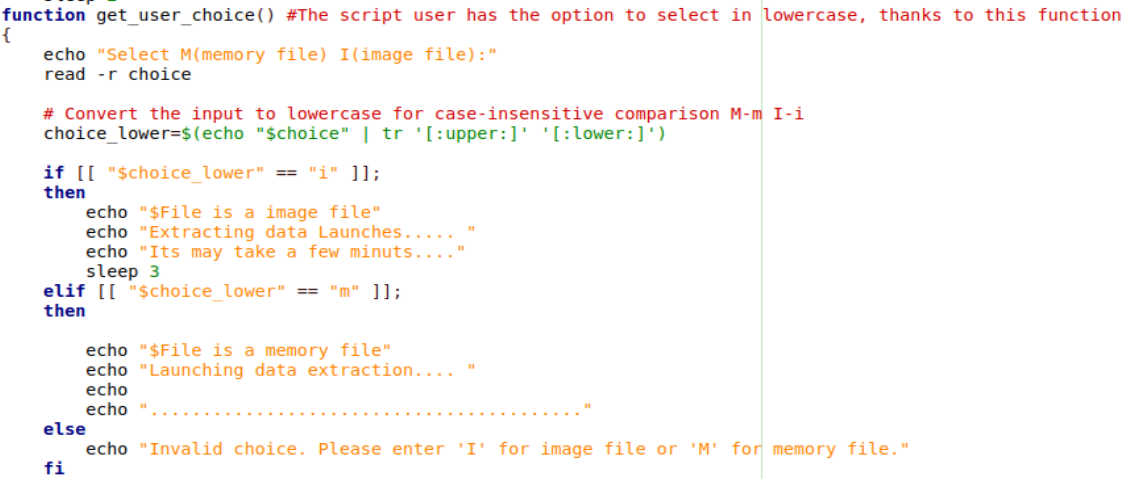


Output:



Function "result"-This function is designed to display the script's outcomes and save them in a file.

Input:



Output:



Function "get\_user\_choice"- The script user can exercise the option to choose in lowercase with this function.

Overview of the tools employed in this project

Binwalk- Binwalk is a firmware analysis tool that is used for searching binary files like firmware images for embedded file and executable signatures.

Strings- strings is a command-line tool that extracts printable character sequences from binary files.

Foremost- Foremost is a file recovery tool designed to extract files based on their headers, footers, and internal data structures.

Bulk extractor- Bulk Extractor is a computer forensics tool that scans digital media, such as disk images, files, or raw data, to extract information and patterns.

Volatility- Volatility is an open-source memory forensics framework that is used for analyzing the contents of computer memory (RAM) during a particular point in time.

Web sources incorporated in this script

<https://github.com/> Github -Great website for script codes

<https://stackoverflow.com/> Stack overflow- website for questions and answers around the world

<https://chat.openai.com/> ChatGpt- Helped me with accuracy and correct spelling and knowledge questions