**User Input**

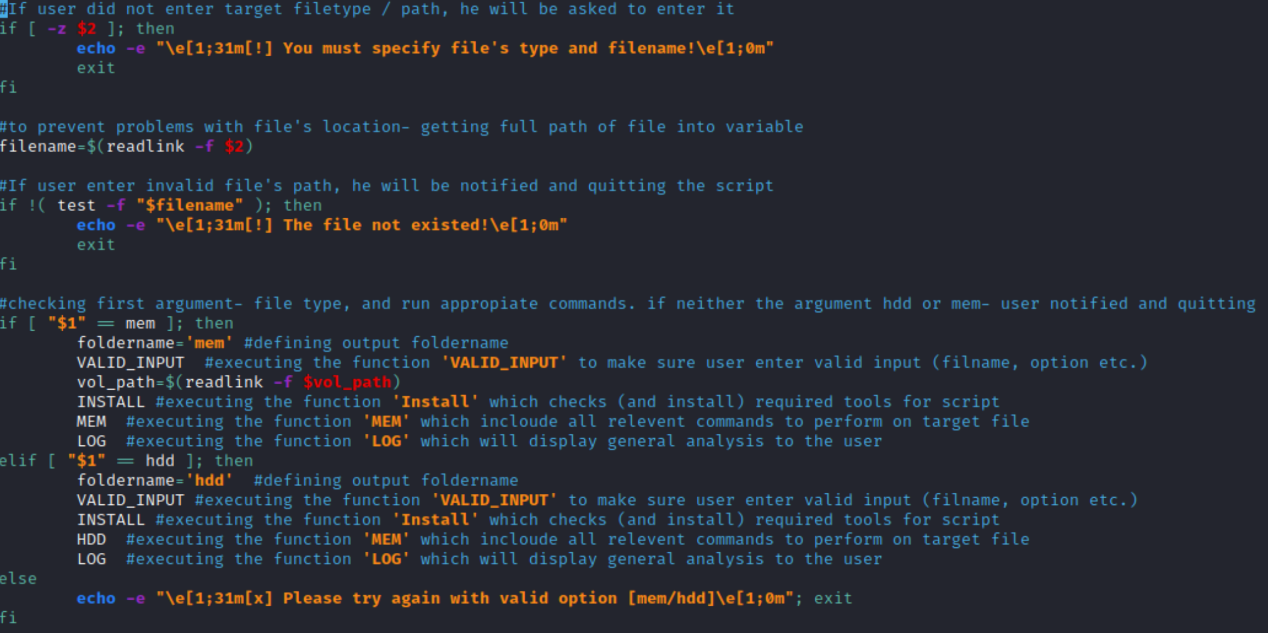
I was asked to write a script which takes input from user and run forensics-tools command on it according to file type.

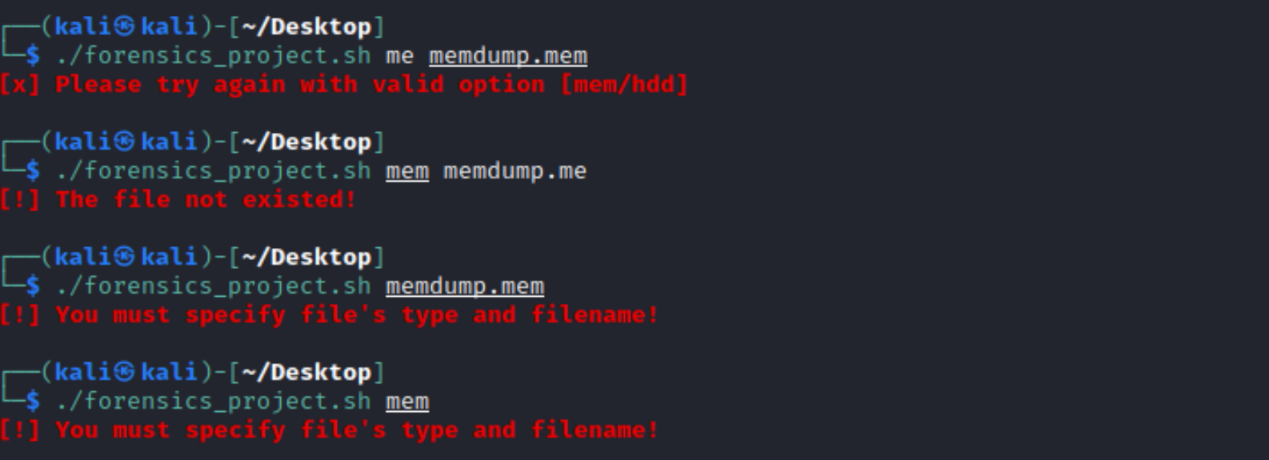
First – the bash script checking user input's syntax, if there are any problems- user notified and asked to correct it.

Then – the script checks what target file's type user chooses.

If 'mem' – the script runs memory file's commands.

If 'hdd' – the script runs hdd file's command.

**Code:**

**Realtime script:**

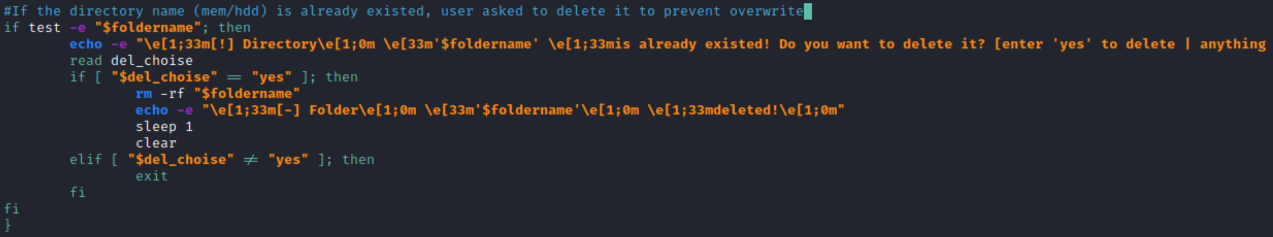
**Functions**

First function – **VALID\_INPUT**

**this function designed to make sure destination folder is not exist. if yes, user can delete it through the script.**

(There is another part of this function which relevant only to memory files. I will add it below)

**Code:**



**Realtime-script:**

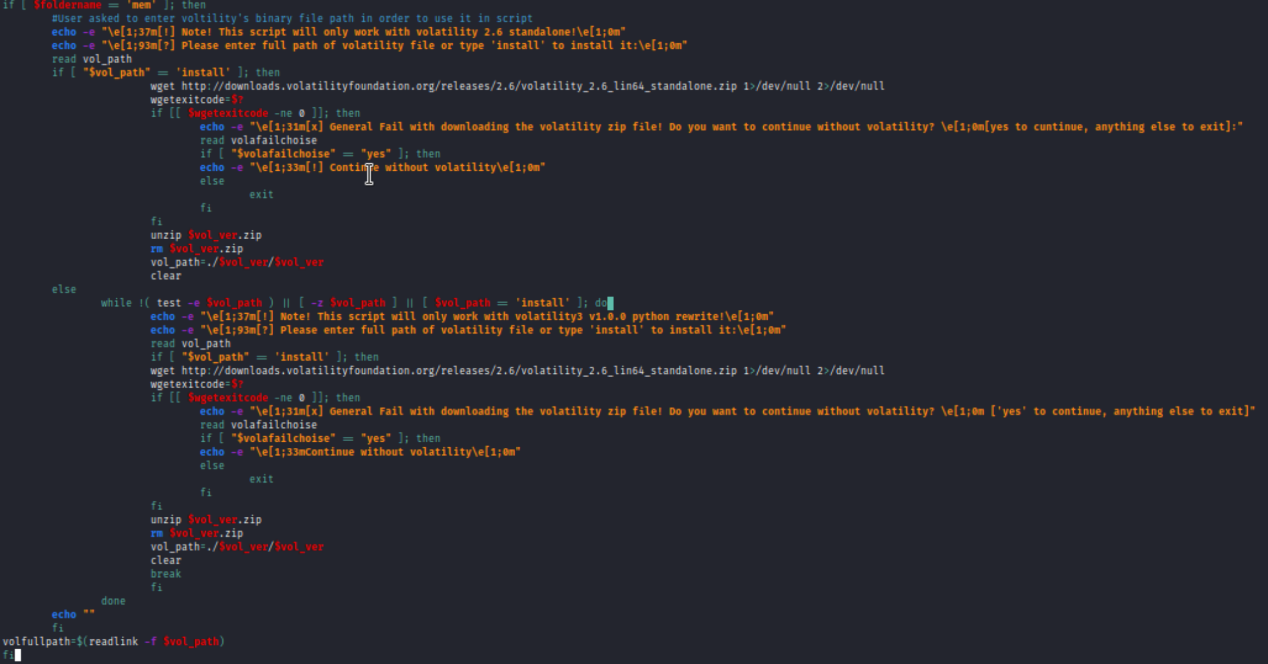
**The second (actually first) part of this function, designed to get volatility's binary file path.**

**If in entered path, the script can't find any file- he asked to correct it.**

**If he wants to download it through the script, he can do it by type 'install'.**

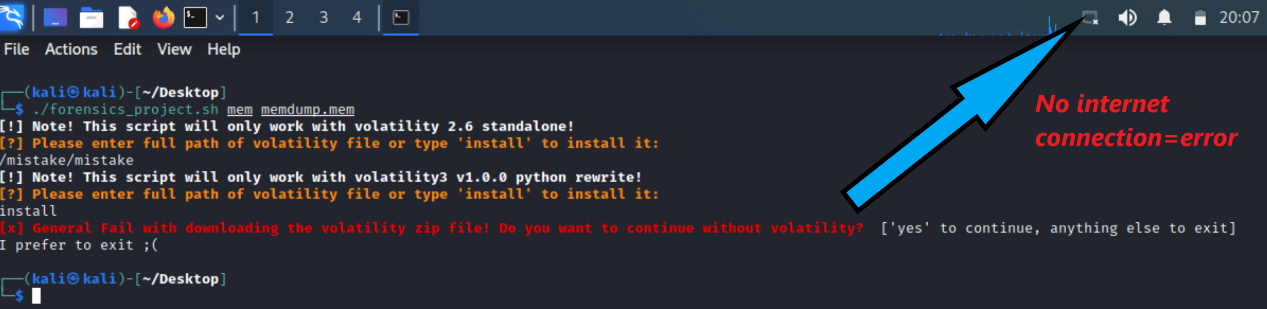
**He also can continue without volatility.**

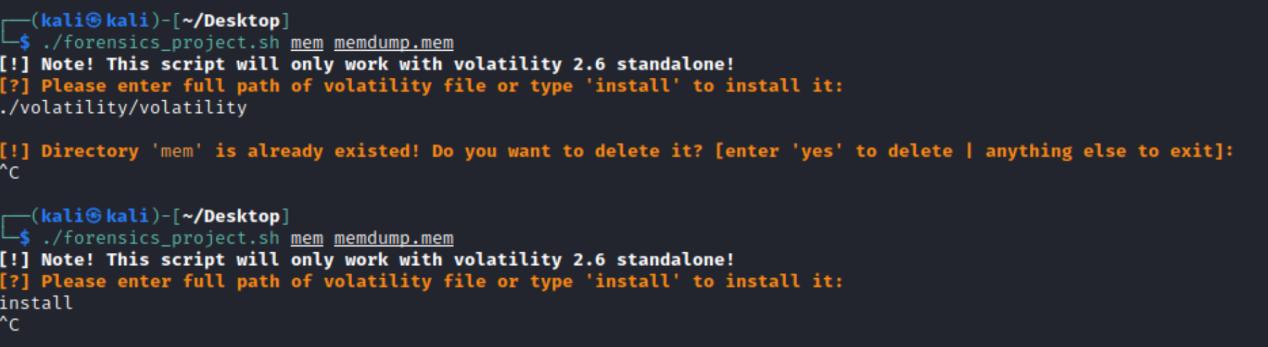
**Code:**

****

**Realtime-script:**

**With error (from user/downloading volatility):**

**Without errors or problems with downloading:**

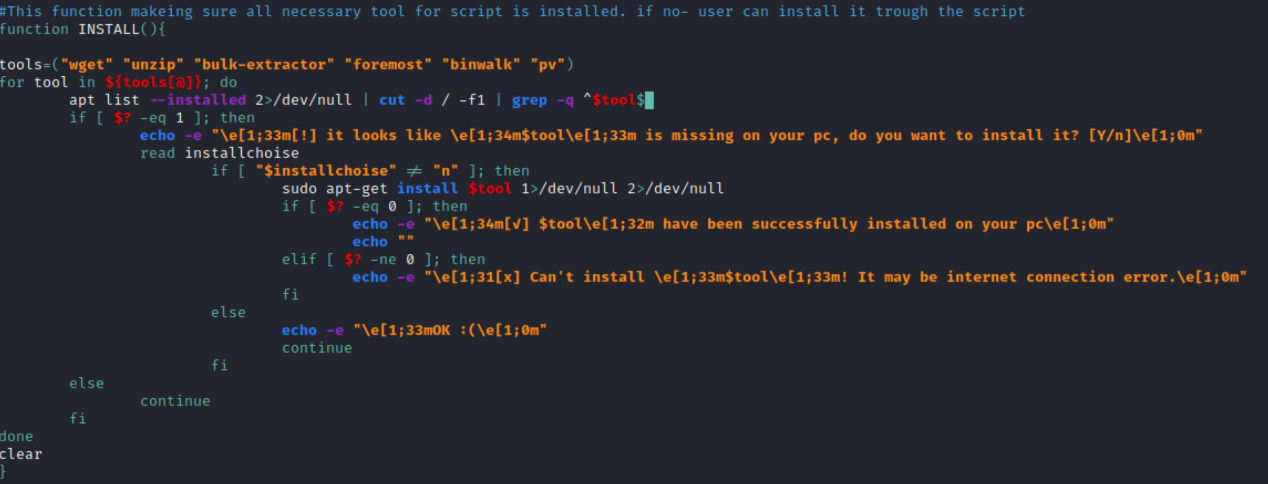
****Second function – **'INSTALL'**

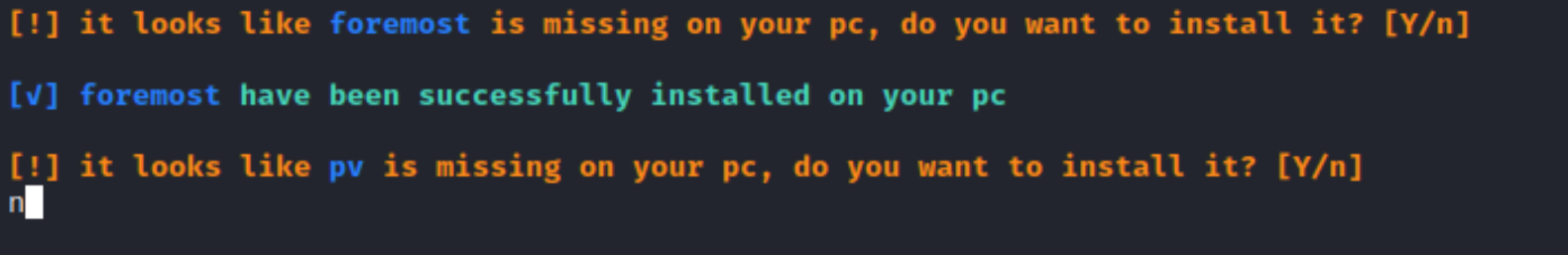
**This function designed to make sure all necessary tools is installed on the machine.**

**If all tools installed, it is doing nothing.**

**If any tool is missing- user notified and can choose to install it.**

**Code:**

**Realtime-script:**

****

Third function – **'MEM'/'HDD' (which includes the function 'COMMONCOMMANDS')**

The function **'COMMONCOMMANDS'**

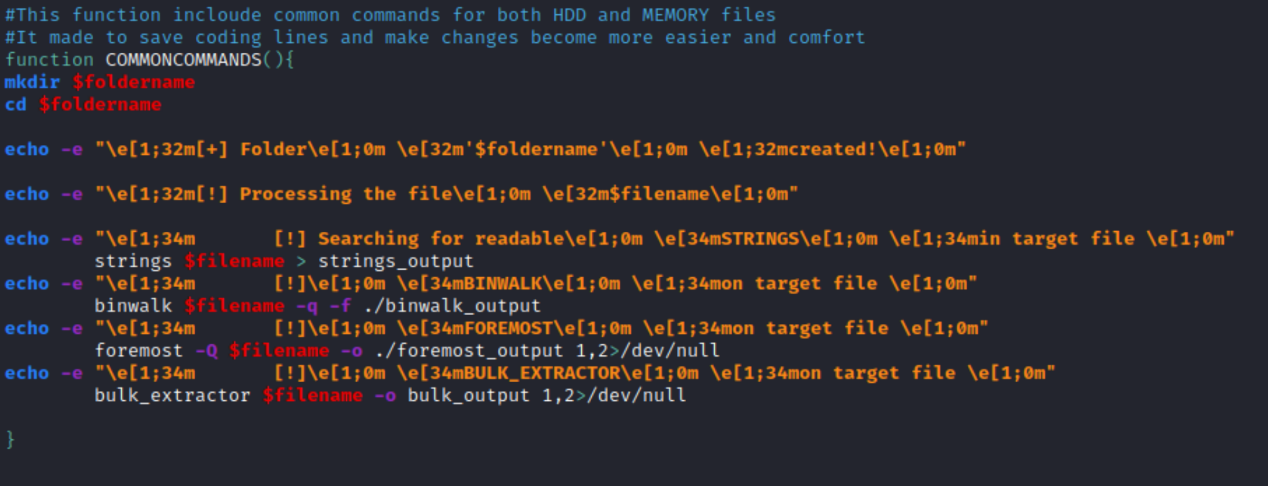
**This function designed to concentrate common command for both hdd and memory files.**

**It also creating relevant folder based on input ('mem'/'hdd')**

**It has two main advantages:**

1. **Changes for both functions ('MEM'/'HDD') becoming easier**
2. **It saves code lines and preventing mistakes in code**

**This function cares to show the user what actually being done in script and outputting the results of commands into relevant files.**

**Code:**

**Realtime-script:**

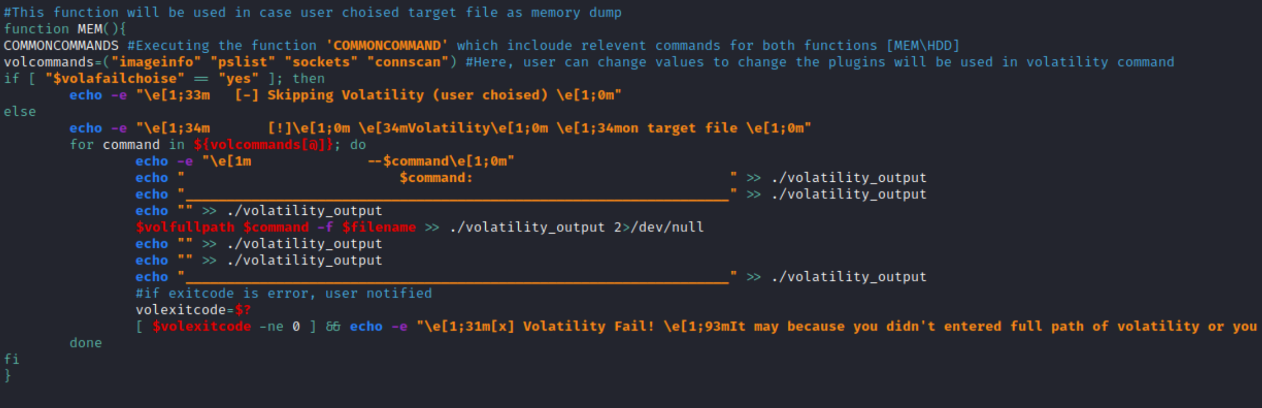
**In Realtime-script it simply integrated in the relevant function ('MEM'/'HDD').**

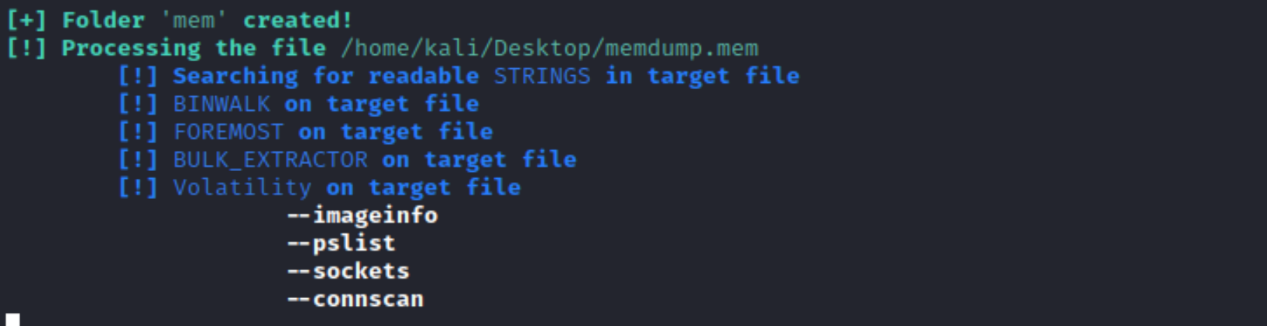
**Pictures will be added below, in function's pictures**

The function '**MEM'**

**This function designed to run commands on memory files. It includes the function 'COMMONCOMMANDS' (which relevant for both hdd and memory files), And volatility command includes the pre-selected plugins(in "volcommands" list).**

**Code:**

**Realtime-script:**

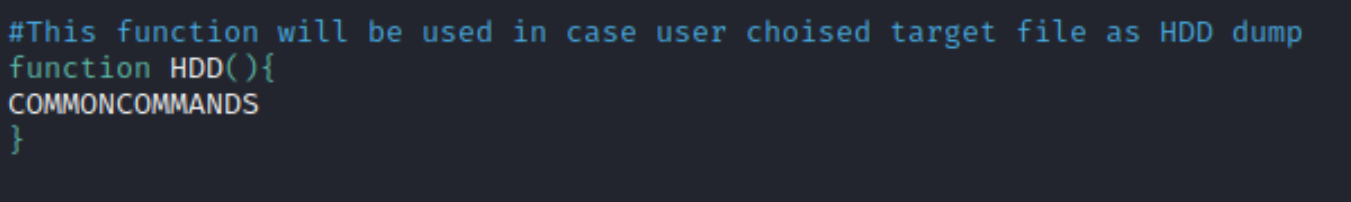
****

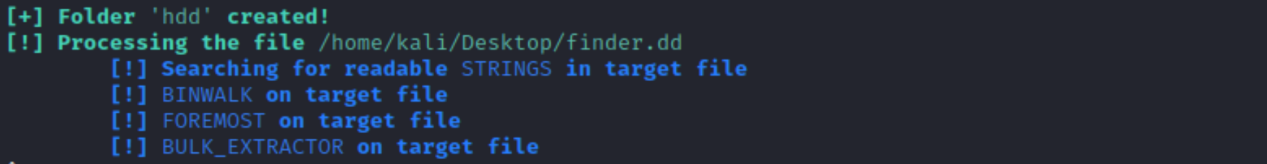
The function '**HDD'**

**This function designed to run commands on memory files. It includes the function 'COMMONCOMMANDS' (which relevant for both hdd and memory files)**.

**This function has not unique command except of common commands, but it can be edited and changed.**

**Code:**

****

**Realtime-script:**

Fourth function **'LOG'**

**This function designed to display general analysis to the user.**

**It shows the user concise report about the file.**

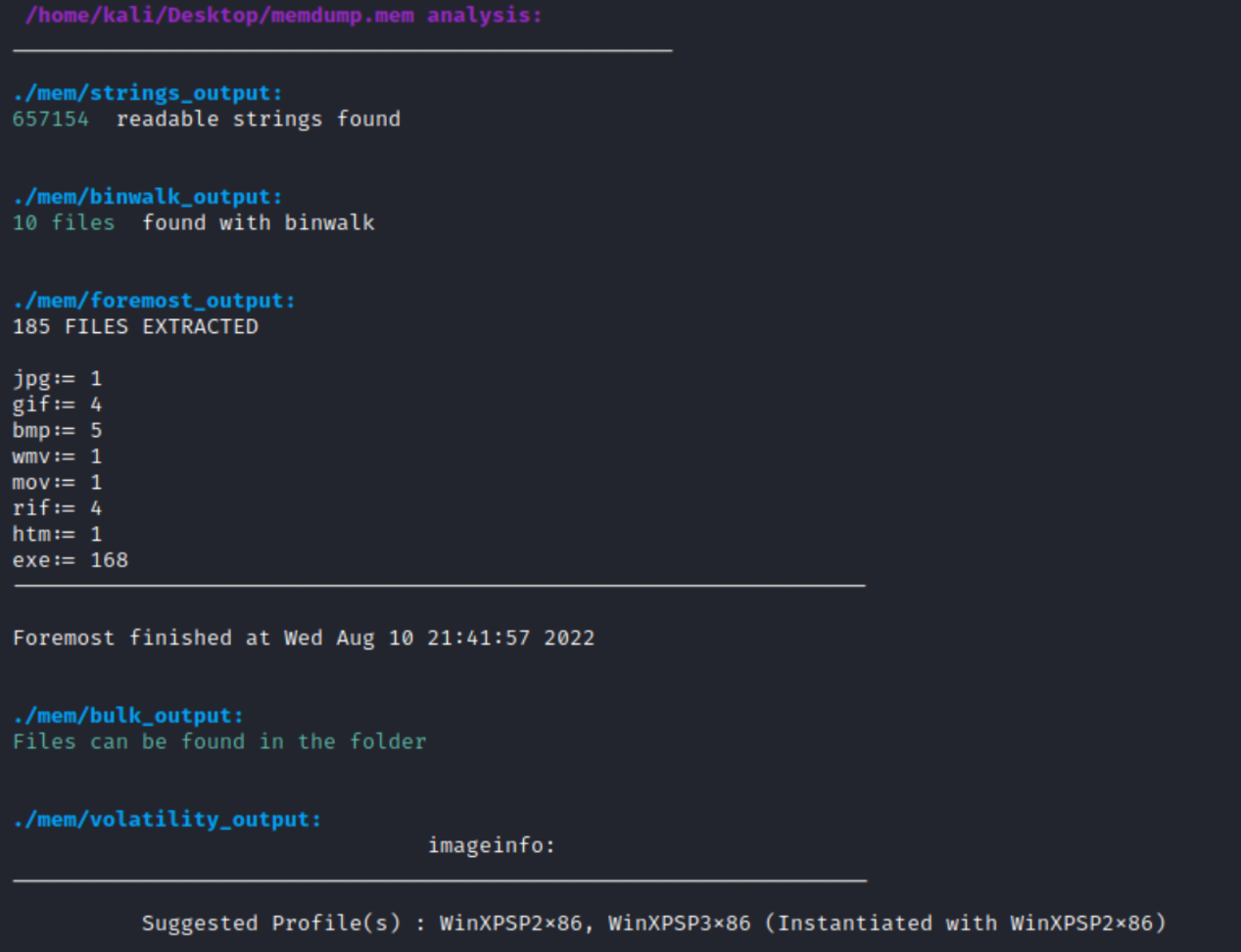
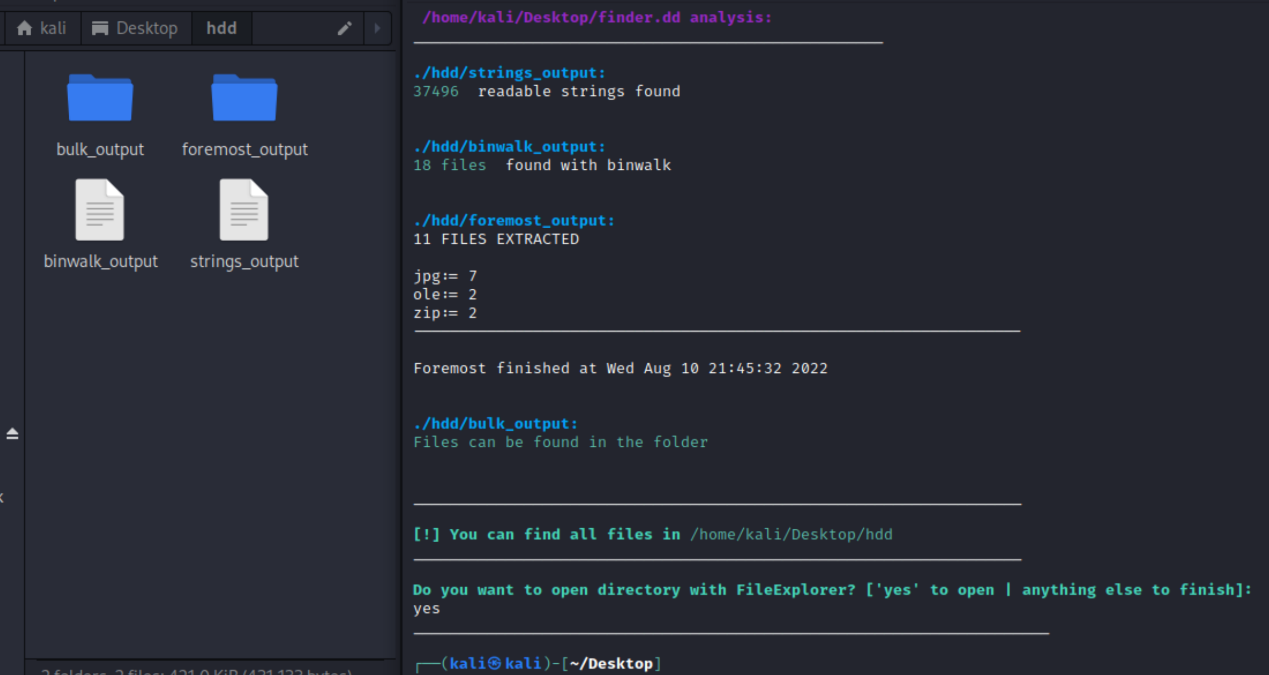
**The user notified about destination folder's path and he can also open destination folder in GUI view.**

**Code:**

****

**Realtime-script:**

**MEM(cropped screenshot) :**

**HDD:**

**תמונה שמכילה טקסט, צג, אלקטרוניקה, מקורה

התיאור נוצר באופן אוטומטיsample GIF of full process (HDD file)**