CTFLearn: Binwalk

This is a forensics challenge about finding hidden files from within a “disguise” file.

Used: ***Foremost:*** Is a command line forensics tool capable of finding lost or deleted data from inside a file.

“Foremost can recover the files for hard disk, memory card, pen drive, and another mode of memory devices easily. It can also work on the image files that are being generated by any other Application”

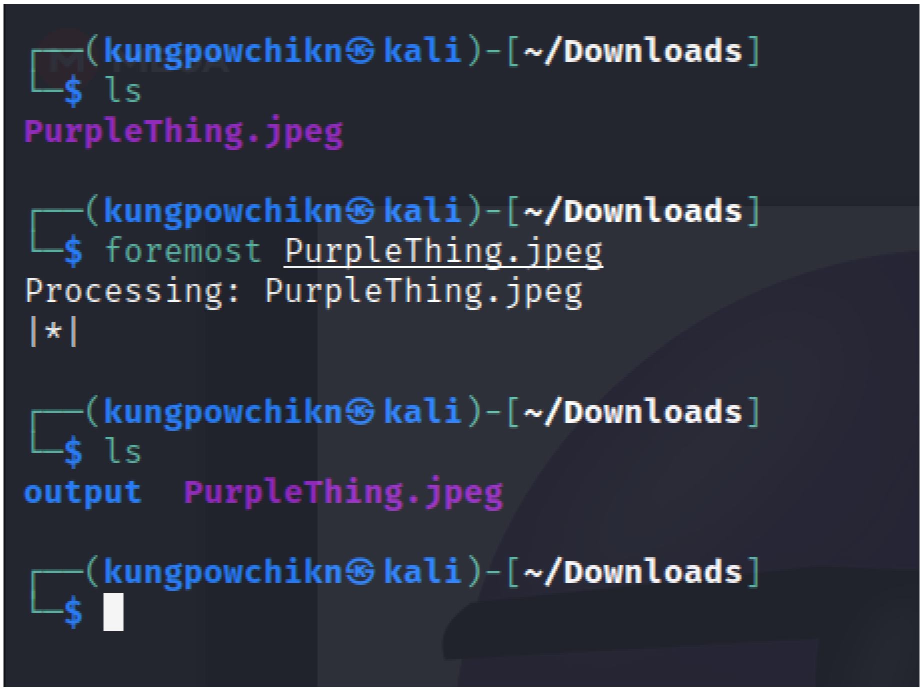
- GeeksforGeeks.com

Guide:

After downloading the image file simply type command

- **foremost <imageFileName.ext>**
  - In this case its “foremost PurpleThing.jpeg”

The command will execute and a directory with the name *output* will appear next to the file

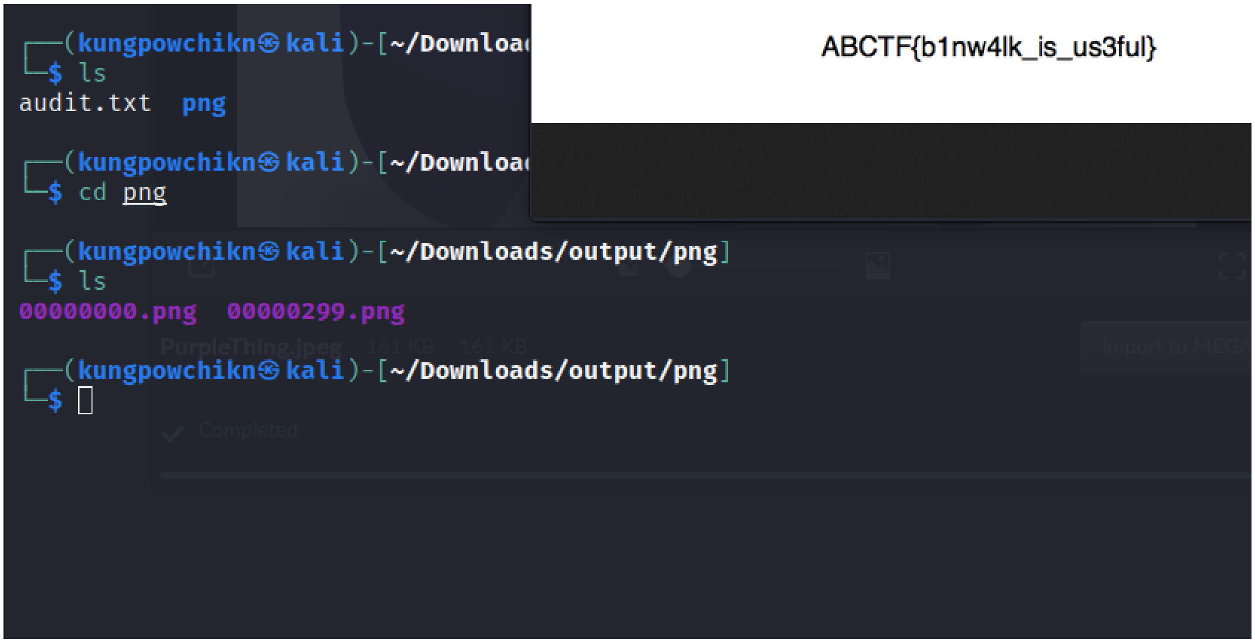


```
┌──(kungpowchikn㉿kali)-[~/Downloads]
└─$ ls
PurpleThing.jpeg

┌──(kungpowchikn㉿kali)-[~/Downloads]
└─$ foremost PurpleThing.jpeg
Processing: PurpleThing.jpeg
|*|

┌──(kungpowchikn㉿kali)-[~/Downloads]
└─$ ls
output  PurpleThing.jpeg

┌──(kungpowchikn㉿kali)-[~/Downloads]
└─$ 
```

Inside the directory you'll find additional files:

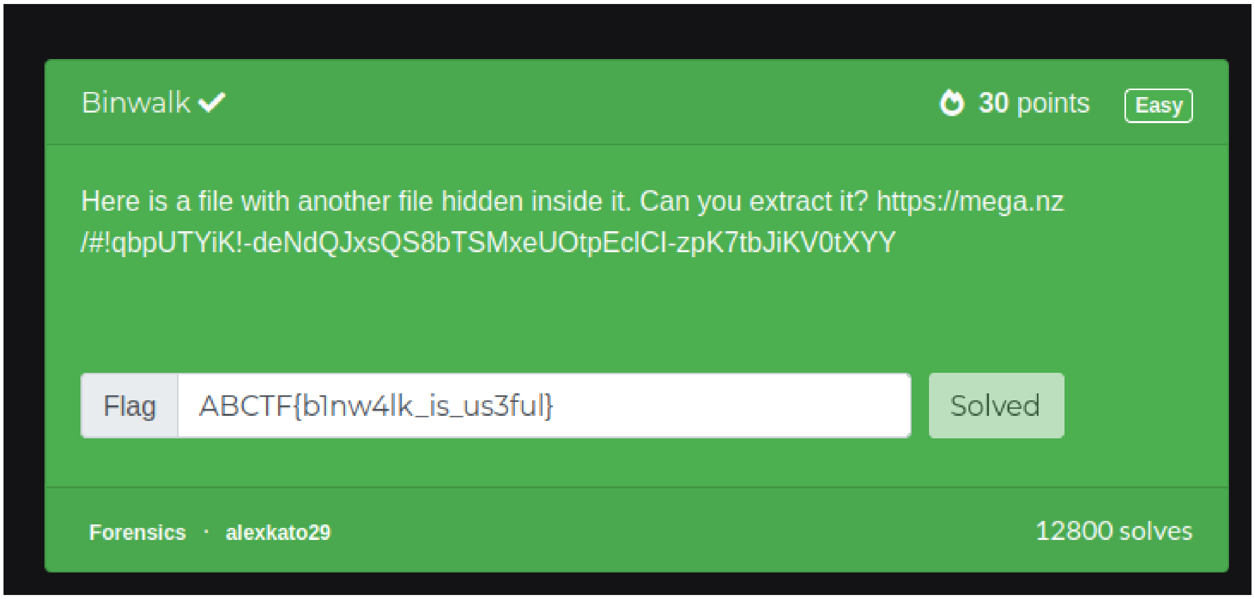
1) *audit .txt* contains the results of the above command
2) Either another file or another directory

Inside the new directory there were (for this specific challenge) two additional image files. Inspecting them reveals the flag



```
┌──(kungpowchikn㉿kali)-[~/Downloa
└─$ ls
audit.txt   png

┌──(kungpowchikn㉿kali)-[~/Downloa
└─$ cd png

┌──(kungpowchikn㉿kali)-[~/Downloads/output/png]
└─$ ls
00000000.png   00000299.png

┌──(kungpowchikn㉿kali)-[~/Downloads/output/png]
└─$ 
```

ABCTF{b1nw4lk_is_us3ful}



Here is a file with another file hidden inside it. Can you extract it? https://mega.nz/#!qbpUTYiK!-deNdQJxsQS8bTSMxeUOtpEclCl-zpK7tbJiKV0tXYY

Flag: ABCTF{b1nw4lk_is_us3ful}

And that's a wrap