Evelyn Okougbo
Read me.

Brute Force password cracking is the technique implemented in my program to obtain the passwords of given files. The program concatenates 5 combinations of characters, converts it to hash, and checks it against the known hash. This cycle repeats until the generated hash exactly the same as the known hash.

To run password_cracker: open password_cracker, press f5

To extract the hidden watermark from a given image:
Iterate over the width and height to get pixel coordinates of red, green and blue and convert them to binary. Extract the least significant bit of each and concatenate them. Using a for loop, 8 bit of lsb is extracted and converted to ASCII.

To run message_extractor.py: open password_cracker, press f5

Watermark extracted from Themoon.png (blue) : *This image is the exclusive property of Sangam Mulmi and is protected under the United States and International Copyright laws. Any unauthorized reproduction, manipulation, or distribution of this image is strictly prohibited. This image is the exclusive property of Sangam Mulmi and is protected under the United States and International Copyright laws. Any unauthorized reproduction, manipulation, or distribution of this image is strictly prohibited.*

Watermark extracted from confession.png (green): *I am Anakin Skywalker, and I have been overfeeding cats since 1780. I confess that this has distressed thousands of cats throughout the years, resulting in reduction of purring.*

sources:

https://stackoverflow.com/questions/464864/how-to-get-all-possible-combinations-of-a-list-s-elements
https://stackoverflow.com/questions/3099987/generating-permutations-with-repetitions-in-python

https://www.packtpub.com/mapt/book/networking_and_servers/9781784392932/6/ch06lvl1sec53/extracting-messages-hidden-in-lsb

http://blog.justsophie.com/image-steganography-in-python/