Michael Steven Towns

Password Cracking:

The first thing I did was to write a small python2 program to loop through all strings of length 5 composed entirely of the lowercase alphabet using the string.ascii_lowercase array provided by python. I then combined these 5 characters into a single string and hashed it using the *haslib.md5(string).hexdigest()* command. This command takes the string and uses a md5 hash on it. I then compared that string with the hash of each of the 3 passwords. On a success, it prints the password found and on a fail it tests the next one. I then added a boolean value for each of the files so that after it has found all 3 passwords the program would exit instead of continuing to test new passwords.

Opening the files

- File: Jkirk.zip
    - Password: troll
    - Hash: 9aeaed51f2b0f6680c4ed4b07fb1a83c
    - Containing:
        - INFO.txt
            - THIS IS JUST A USELESS TEXT FILE I ADDED HERE FOR NO REASON AT ALL!
- File: Lmccoy.zip
    - Password: lolol
    - Hash: 172346606e1d24062e891d537e917a90
    - Containing:
        - READ ME.txt
            - The picture in this ZIP may have been watermarked with a copyright notice! Maybe we should investigate to find out?
        - DCIM_2837.png
            - This has the copyright notice
- File: Cchapel.zip
    - Password: polar
    - Hash: fa5caf54a500bad246188a8769cb9947
    - Containing:
        - READ ME.txt
            - One of the pictures in this ZIP has a hidden message. Perform Least Significant Bit Steganalysis on one of the RGB colors of each pixel! If you extract the message correctly, you earn a BONUS!
        - mountain.png
        - mountain (copy).png
            - This has the hidden message

Finding hidden messages:

Jkirk had no useful information and was discarded. Lmccoy has the watermarked information in the image titled “DCIM_2837.png”. I wrote a program in python2 to open the image using the Image module of the Python Image Library(PIL) and loop through every pixel in it. I modded the green value by 2 (giving either a 1 or a 0) and saved that as a string. I then added “0b” to the beginning of it and then converted it to ascii using the python binascii library with the *binascii.unhexlify(‘%x’ % int(string,2))* command. I printed this value and it gave me.

“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. Copyrighted © 2015, Sangam Mulmi.”

Repeated through the rest of the image

Finding bonus messages:

Cchapel has the bonus information. The two images in the program are “mountain.png” and “mountain (copy).png”. I first tried with “mountain.png” converting the green channel to binary as I had for the copyright, this produced garbage so i tried the blue and red channel, which also produced nothing. After this I tried looking in “mountain (copy).png” I again tried the green, blue and then red channels. This time the red channel produced legible text that read:

“Lost and insecure
You found me, you found me
Lyin' on the floor
Surrounded, surrounded
Why'd you have to wait?
Where were you? Where were you?
Just a little late
You found me, you found me
-- THE FRAY --”

This text was repeated through the rest of the image.