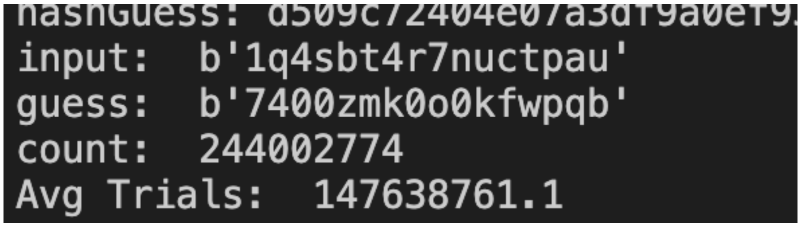
1. **[35pts] How many trials will it take you to break the weak collision resistance property using the brute-force method? You should repeat your experiment for multiple times (100 or more depending on how long each trial takes) and report your average number of trials.**

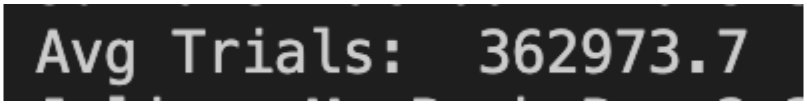
I created a for loop to make my program run 10 times. The average trials (out of 10 runs) is 147638761. I couldn't run up to 100 trials because it took so long to run one time. It took me hours to run my program.



```
hashGuess: d509c72404e07a3df9a0ef9
input:  b'1q4sbt4r7nuctpau'
guess:  b'7400zmk0o0kfwpqb'
count:  244002774
Avg Trials:  147638761.1
```

2. **[35pts] How many trials will it take you to break the collision-free property using the brute-force method? Similarly, you should report the average.**

The average trials (out of 100 runs) it took to break the collision-free is 362973.



```
Avg Trials:  362973.7
```

3. **[10pts] Based on your observation, which property is easier to break using the brute-force method?**

Based on my observation, the collision free is easier to break using the brute-force method because it took way less time to find 2 random inputs that have a collision in hash values.

4. **[10pts] Can you explain the difference in your observations?**

I think the difference is that with the weak collison, we had to find the random string that matches the original string; while with the collision free, we only needed to find 2 random strings that matched out of a certain number of random strings which made it easier to find a collision.