Part 6 – Hash Breaking Competition

I used an online md5 hash cracker that has over 312.072 billion cracked hashes in their cache. From the list of hashes in hashes.txt, I've managed to find most of the passwords except for 4 in the moderate range. With a larger dataset, chances of finding the plaintext password is higher.

The approach is similar to the brute force attack I did for part 2 of the lab, just that the there is a much larger dataset to compare with. My approach was to create a dictionary containing a list of plaintext password as key and its hash value as value. From the list, I will compare the hash value from hash5.txt with the hash value from the dictionary. If there is a match, then I print out the plaintext password corresponding to the hash value.