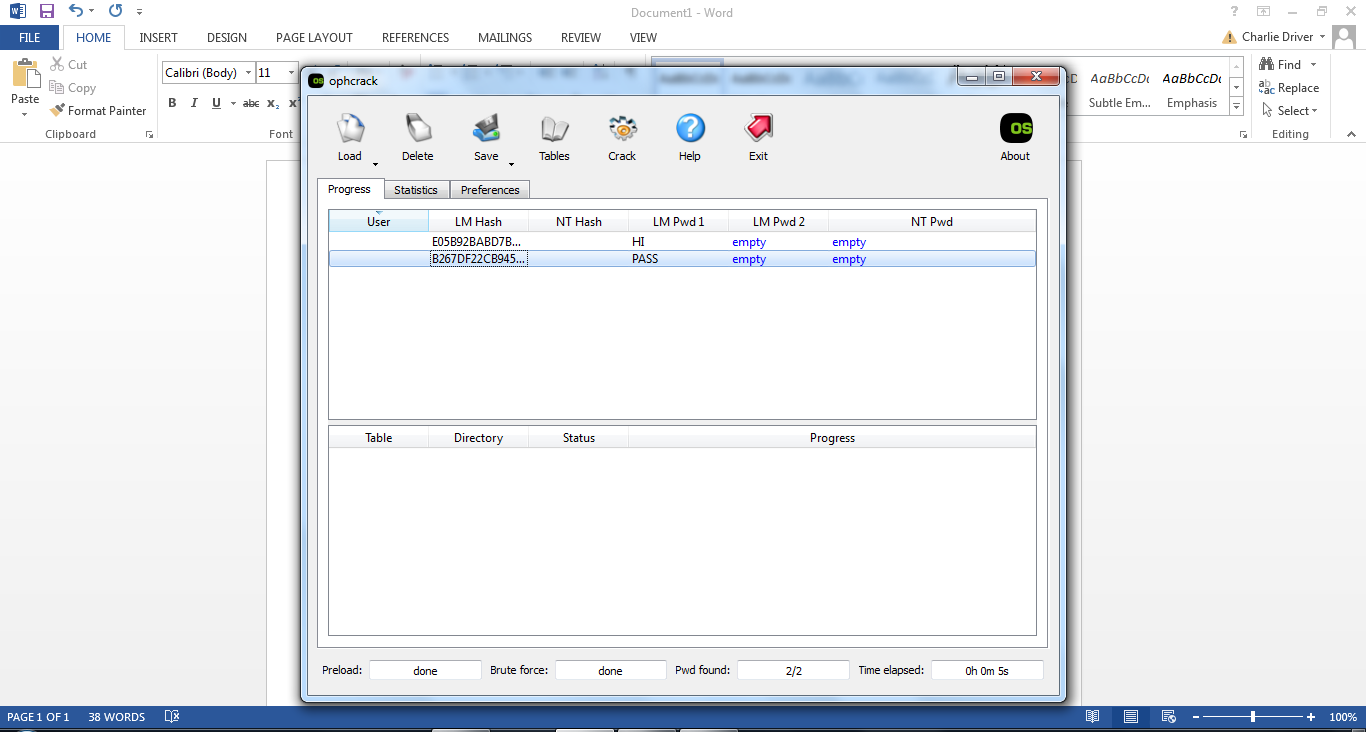
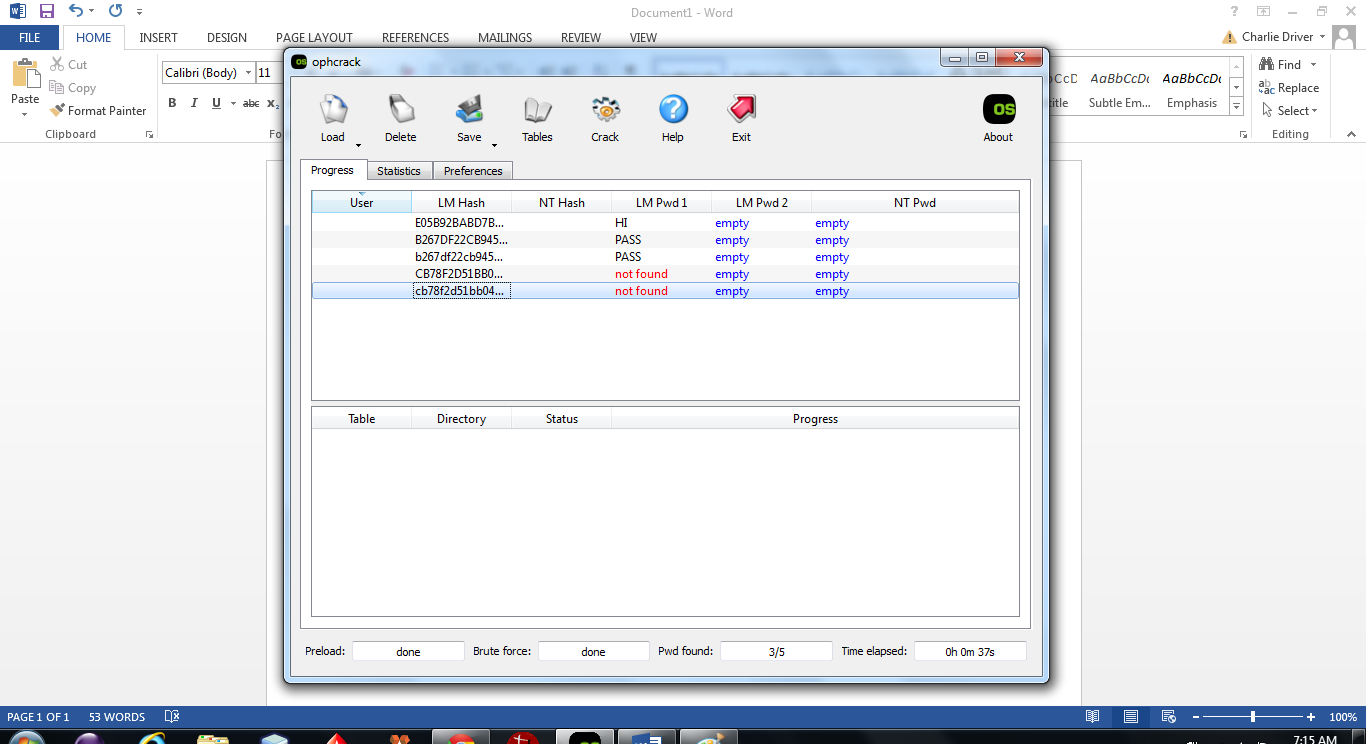
Lab 1 Part 4

Ophcrack initially took about 25 seconds to crack the first password, "hi", using brute force. The password appeared in ophcrack in upper case, due to the algorithm used to encrypt the password converting all letters to upper case.  Entering the hash in lower case, instead of the upper case provided, did not change any results.

Given the hash generated by http://www.asecuritysite.com/Encryption/lmhash, ophcrack could not find the associated password of “hi1234”. After including use of a rainbow table, ophcrack was able to quickly crack this password. It would appear that passwords of 4 or less characters can be cracked without the tables. Larger passwords cannot.



Passwords with similar hashes were cracked much quicker than completely unique passwords. Special characters caused a problem for ophcracker, as it could not find the password “ophcracker1!”.

