**Project #3**

Tyler Perkins

Christopher Ward

Matt Stanfield

Pierre Bonnain

**Section I (Introduction)**

Task 2 was completed by Chris and Tyler using the simple\_wep\_crack instructions. Task 3 was completed by Chris and Tyler using the sshpass program to test all the passwords in the dictionary file. Section 2 and 3 of the report were written by Chris and Tyler. Matt created the brute force password cracking code in order to answer part of task 4 and then answered the questions for task 4 part c, d, and e. Matt and Tyler wrote the introduction and formatted the project report. The group tasks were coordinated via groupme and in-person meetings before and after class.

**Section II (Task II)**

**A.) Show the screen shot when you are running aircrack and obtaining the key.**

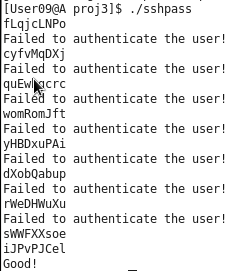
****

**B.) Report how long it takes to crack the WEK key and how many packets are captured in order to crack the key.**

**Time to Crack:** It took ~15 minutes after following the tutorial correctly and opening 8 ping terminals, two of which were similiar to the network we were trying to crack. This is not shown in the picture above as immediatley when we started aircrack-ng the WEP key had already been found.

**Packets Obtained:** 242749 packets

**Section III (Task III)**

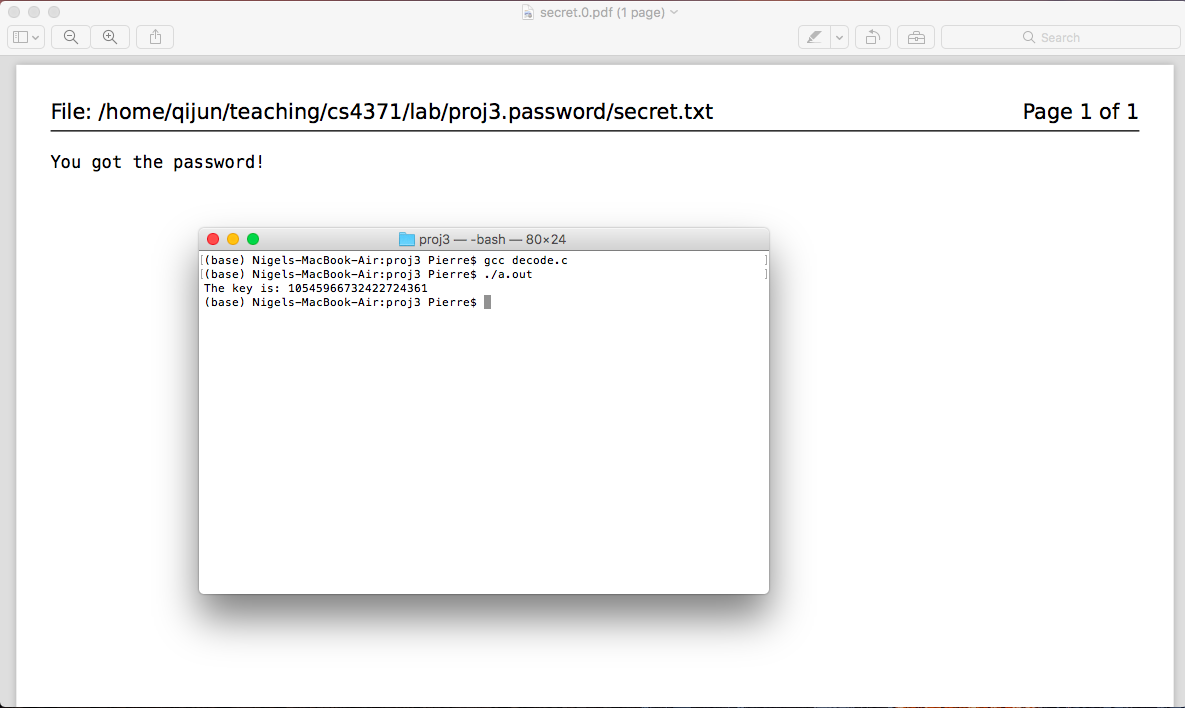
**A.)**

**B.) 9 Passwords => ~15 seconds**

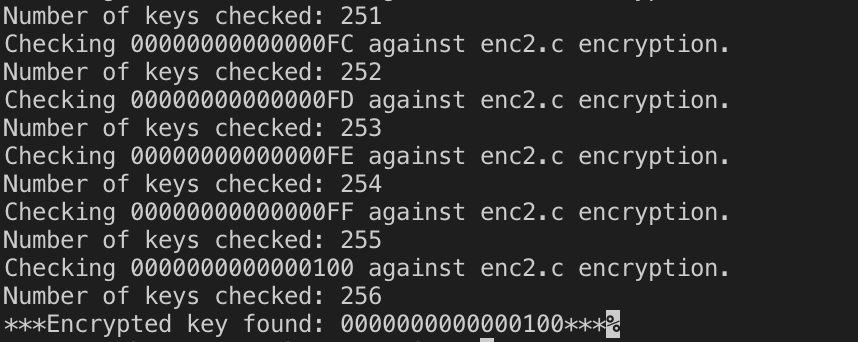
**C.) 479827 Passwords => 719,740 seconds**

**Section IV (Task IV)**

**A.)**

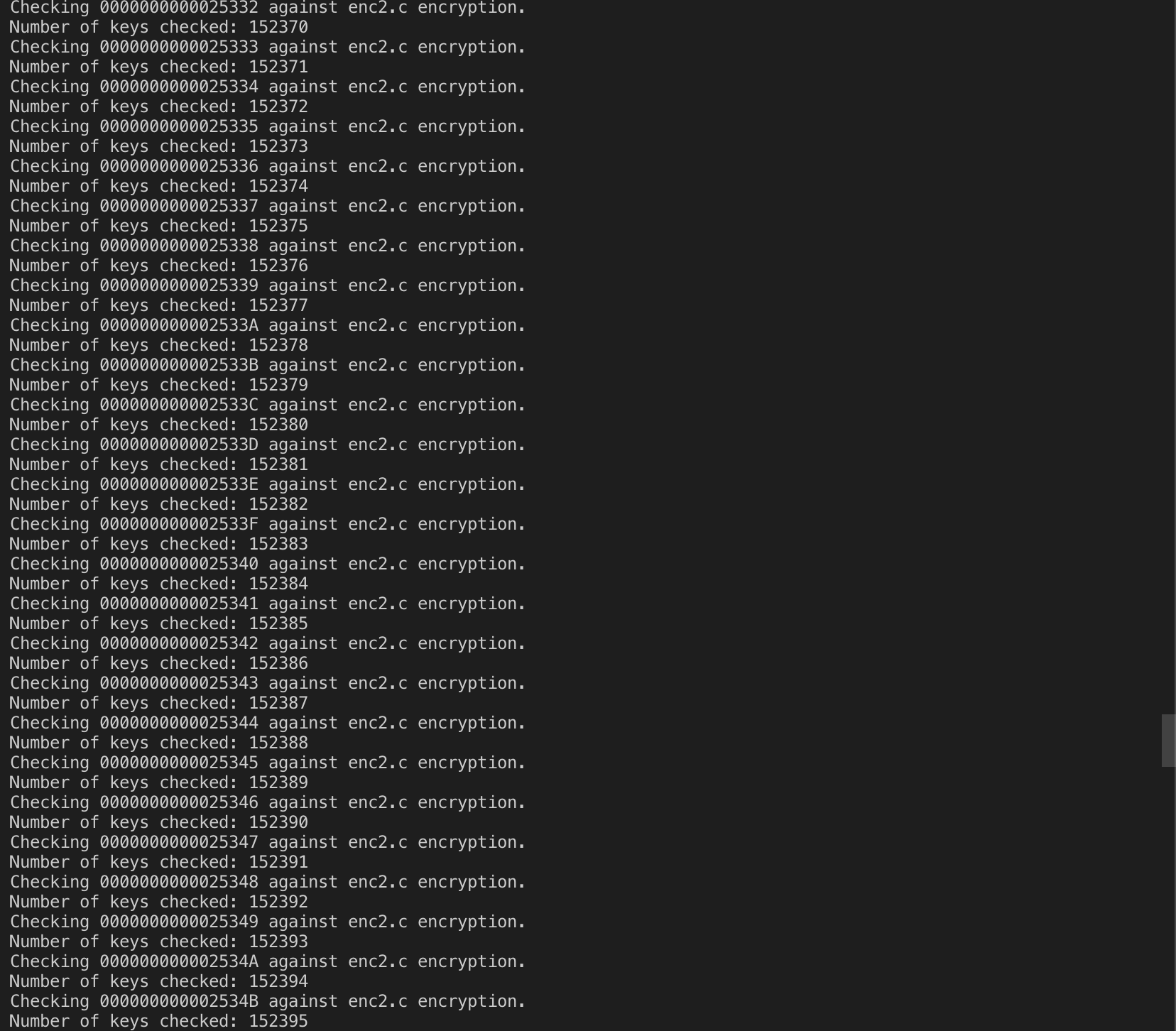
****

**B.) Show the screen shot of your DES program when it deciphers a testing file.**

****

**C.) Show the screen shot of your DES program when you are brute force cracking the key.**

**Program while its running the key checking algorithm**



**D.) Report how many keys were tested in 10 minutes:**

Number of keys tested in 10 minutes: 120,095,792

**E.) Estimate how long it would take to find the key:**

The total possible number of combinations for a DEC-ECB encryption key is 2^56 which is 7.2057594x10^16. A Brute force cracking program like mine which just increments a hexadecimal number by 1 and compares it to the given encryption key (encrypted by enc2.c) from 0x0000000000000000 to 0xFFFFFFFFFFFFFFFF. The security lab computers were able to check ~ 120 million keys in 10 minutes. At that rate it would take the computers roughly 12,401 years to check every possible key in the worst case scenario that the key was 0xFFFFFFFFFFFFFFFF. It would be reasonable to assume that you could find the key in half that amount of time but it all depends on how high the hex number for the key is.