HW04- observations report

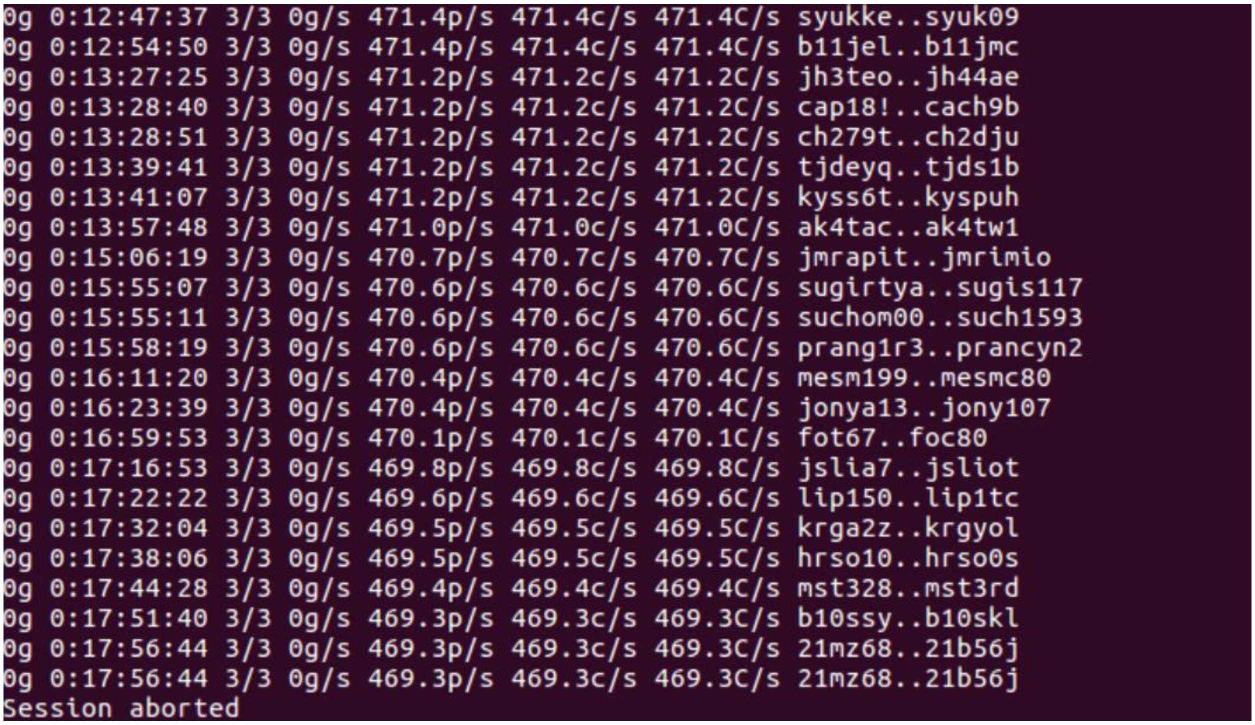
Name: Jihui.Sheng

Course: Cpt_S 427

ID: 11539324

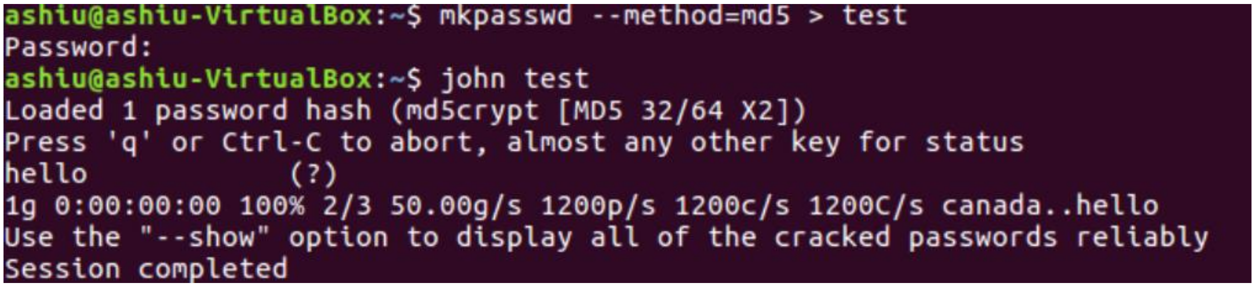
Screenshots proving you did perform the tutorial activities:

When I tried for the first time, I did not define a password. It should use the password that was preset when I entered the system, and that password started with a capital letter, so after 17 hours of operation, I still did not The password is cracked out.



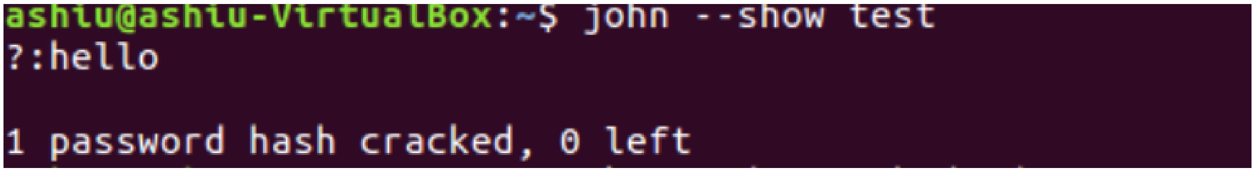
```
0g 0:12:47:37 3/3 0g/s 471.4p/s 471.4c/s 471.4C/s syukke..syuk09
0g 0:12:54:50 3/3 0g/s 471.4p/s 471.4c/s 471.4C/s b11jel..b11jmc
0g 0:13:27:25 3/3 0g/s 471.2p/s 471.2c/s 471.2C/s jh3teo..jh44ae
0g 0:13:28:40 3/3 0g/s 471.2p/s 471.2c/s 471.2C/s cap18!..cach9b
0g 0:13:28:51 3/3 0g/s 471.2p/s 471.2c/s 471.2C/s ch279t..ch2dju
0g 0:13:39:41 3/3 0g/s 471.2p/s 471.2c/s 471.2C/s tjdeyq..tjds1b
0g 0:13:41:07 3/3 0g/s 471.2p/s 471.2c/s 471.2C/s kyss6t..kyspuh
0g 0:13:57:48 3/3 0g/s 471.0p/s 471.0c/s 471.0C/s ak4tac..ak4tw1
0g 0:15:06:19 3/3 0g/s 470.7p/s 470.7c/s 470.7C/s jmrapit..jmrimio
0g 0:15:55:07 3/3 0g/s 470.6p/s 470.6c/s 470.6C/s sugirtya..sugis117
0g 0:15:55:11 3/3 0g/s 470.6p/s 470.6c/s 470.6C/s suchom00..such1593
0g 0:15:58:19 3/3 0g/s 470.6p/s 470.6c/s 470.6C/s prang1r3..prancyn2
0g 0:16:11:20 3/3 0g/s 470.4p/s 470.4c/s 470.4C/s mesm199..mesmc80
0g 0:16:23:39 3/3 0g/s 470.4p/s 470.4c/s 470.4C/s jonya13..jony107
0g 0:16:59:53 3/3 0g/s 470.1p/s 470.1c/s 470.1C/s fot67..foc80
0g 0:17:16:53 3/3 0g/s 469.8p/s 469.8c/s 469.8C/s jslia7..jsliot
0g 0:17:22:22 3/3 0g/s 469.6p/s 469.6c/s 469.6C/s lip150..lip1tc
0g 0:17:32:04 3/3 0g/s 469.5p/s 469.5c/s 469.5C/s krga2z..krgyol
0g 0:17:38:06 3/3 0g/s 469.5p/s 469.5c/s 469.5C/s hrso10..hrso0s
0g 0:17:44:28 3/3 0g/s 469.4p/s 469.4c/s 469.4C/s mst328..mst3rd
0g 0:17:51:40 3/3 0g/s 469.3p/s 469.3c/s 469.3C/s b10ssy..b10skl
0g 0:17:56:44 3/3 0g/s 469.3p/s 469.3c/s 469.3C/s 21mz68..21b56j
0g 0:17:56:44 3/3 0g/s 469.3p/s 469.3c/s 469.3C/s 21mz68..21b56j
Session aborted
```

After that, I started to try **challenge 1**:



```
ashiu@ashiu-VirtualBox:~$ mkpasswd --method=md5 > test
Password:
ashiu@ashiu-VirtualBox:~$ john test
Loaded 1 password hash (md5crypt [MD5 32/64 X2])
Press 'q' or Ctrl-C to abort, almost any other key for status
hello            (?)
1g 0:00:00:00 100% 2/3 50.00g/s 1200p/s 1200c/s 1200C/s canada..hello
Use the "--show" option to display all of the cracked passwords reliably
Session completed
```

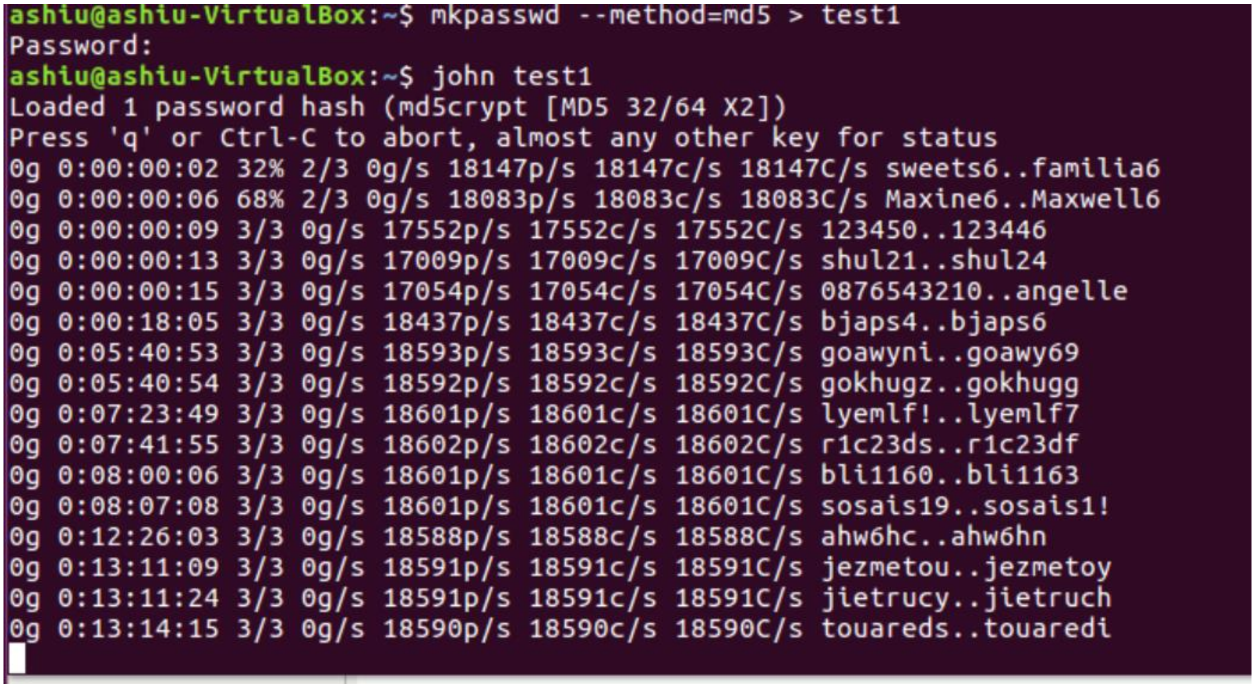
John can easily get the password ‘hello’.



```
ashiu@ashiu-VirtualBox:~$ john --show test
?:hello

1 password hash cracked, 0 left
```

But, when I try to use ";lkjdaf09823471092jlj23" instead of "hello".

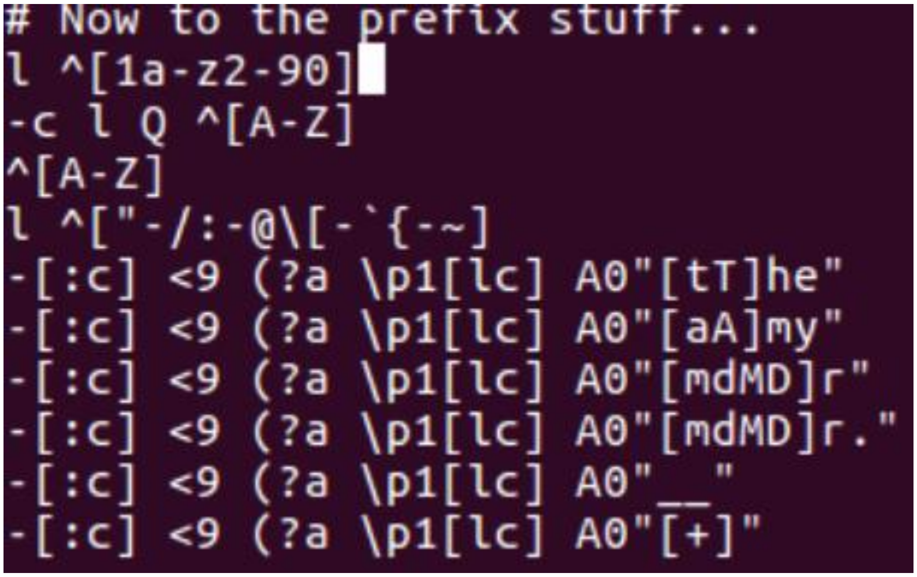


```
ashiu@ashiu-VirtualBox:~$ mkpasswd --method=md5 > test1
Password:
ashiu@ashiu-VirtualBox:~$ john test1
Loaded 1 password hash (md5crypt [MD5 32/64 X2])
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:00:00:02 32% 2/3 0g/s 18147p/s 18147c/s 18147C/s sweets6..familia6
0g 0:00:00:06 68% 2/3 0g/s 18083p/s 18083c/s 18083C/s Maxine6..Maxwell6
0g 0:00:00:09 3/3 0g/s 17552p/s 17552c/s 17552C/s 123450..123446
0g 0:00:00:13 3/3 0g/s 17009p/s 17009c/s 17009C/s shul21..shul24
0g 0:00:00:15 3/3 0g/s 17054p/s 17054c/s 17054C/s 0876543210..angelle
0g 0:00:18:05 3/3 0g/s 18437p/s 18437c/s 18437C/s bjaps4..bjaps6
0g 0:05:40:53 3/3 0g/s 18593p/s 18593c/s 18593C/s goawyni..goawy69
0g 0:05:40:54 3/3 0g/s 18592p/s 18592c/s 18592C/s gokhugz..gokhugg
0g 0:07:23:49 3/3 0g/s 18601p/s 18601c/s 18601C/s lyemlf!..lyemlf7
0g 0:07:41:55 3/3 0g/s 18602p/s 18602c/s 18602C/s r1c23ds..r1c23df
0g 0:08:00:06 3/3 0g/s 18601p/s 18601c/s 18601C/s bli1160..bli1163
0g 0:08:07:08 3/3 0g/s 18601p/s 18601c/s 18601C/s sosais19..sosais1!
0g 0:12:26:03 3/3 0g/s 18588p/s 18588c/s 18588C/s ahw6hc..ahw6hn
0g 0:13:11:09 3/3 0g/s 18591p/s 18591c/s 18591C/s jezmetou..jezmetoy
0g 0:13:11:24 3/3 0g/s 18591p/s 18591c/s 18591C/s jietrucy..jietruch
0g 0:13:14:15 3/3 0g/s 18590p/s 18590c/s 18590C/s touareds..touaredi
```

It took 13 hours and John still could not crack it.

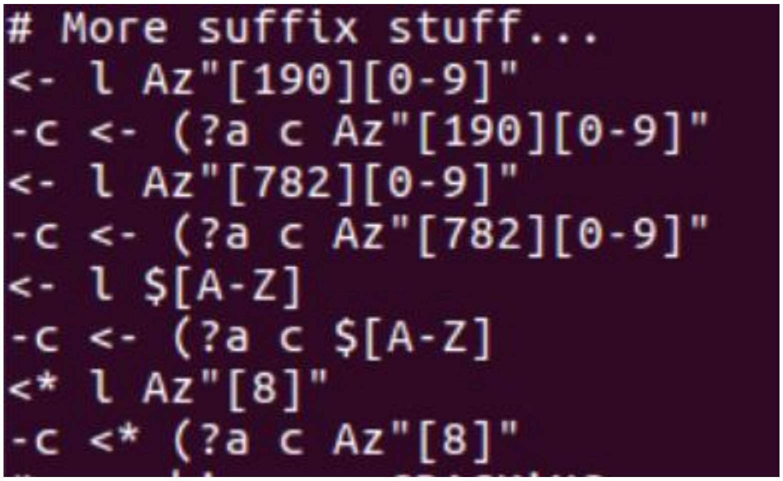
I do not have so much time to wait for a run that may not yield results, so I directly started to **challenge**:

I first add A0"[+]" in prefix stuff part.



```
# Now to the prefix stuff...
l ^[1a-z2-90]
-c l Q ^[A-Z]
^[A-Z]
l ^["-/:-@\[-`{-~]
-[:c] <9 (?a \p1[lc] A0"[tT]he"
-[:c] <9 (?a \p1[lc] A0"[aA]my"
-[:c] <9 (?a \p1[lc] A0"[mdMD]r"
-[:c] <9 (?a \p1[lc] A0"[mdMD]r."
-[:c] <9 (?a \p1[lc] A0"__"
-[:c] <9 (?a \p1[lc] A0"[+]"
```

Then I add Az“[8]” in suffix stuff part.



```
# More suffix stuff...
<- l Az"[190][0-9]"
-c <- (?a c Az"[190][0-9]"
<- l Az"[782][0-9]"
-c <- (?a c Az"[782][0-9]"
<- l $[A-Z]
-c <- (?a c $[A-Z]
<* l Az"[8]"
-c <* (?a c Az"[8]"
```

Trying to change the prefix and suffix separately seems to take more time to find the password. The more important reason for the long time seems to be the absence of a four-letter word dictionary. Since the "-rules" command is not used, it is impossible to determine the main reason.

Report any bugs, typos, broken links etc:

1. Search for the ‘wordlist’ document and find that there is no ‘length4.txt’ document in it. So the command "-wordlist: length4.txt" cannot be used. Similarly, when using the "-rules" command, there will be a prompt that the path cannot be found.
2. I do not know if it is because the password stored in ‘mypasswd.txt’ has not been cracked or other unknown reasons, and the john.pot file was not found.
3. Most of the time in the tutorial is spent on cracking the password. Starting from the "john pass.txt" command, I cannot follow the tutorial. Because it is prompted that the file path cannot be found. I feel that the "pass.txt" document should be a document containing many hashed passwords.

A brief discussion on the skills you've learned from the tutorial (7 lines maximum):

1. The simpler the password, the easier it is for an attacker to crack it. Complex passwords are not unbreakable, but it will take the attacker more time and will not be cracked within a reasonable time.
2. Passwords should not be stored in clear text, and reversible encryption should never be used to store passwords.
3. The use of user id and password is still the most common form of authentication. Although other forms of authentication have emerged, such as biometric authentication and SMS authentication, the use of passwords still dominates.
4. There are several ways to crack the password:
    a. Brute-force attacks: It will increase the difficulty of cracking with the increase of password characters.
    b. Dictionary attacks: In order to make it easier to remember their own passwords, users are likely to use known words.

    c. Precomputed tables: The rainbow table represents a pre-computed dictionary attack. The table stores a large number of passwords and their corresponding hash values. Adding "salt" or a random value before hashing can prevent the password from being cracked by this method.
    d. “Intelligent” brute-force attacks (e.g. Markov chains): Determine the probability of each location of the password by using the previously cracked password.

5. Administrators should help users protect their passwords as much as possible.
   Users should use passwords that are not easy to crack, and even add multiple insurances to their accounts.
6. MD5 is not designed for password hashing, but for low computational cost. Similarly, SHA1 is another hash algorithm that is not suitable for passwords. As a good, slow and computationally expensive hash algorithm, bcrypt is the most suitable for password hashing.
7. In password cracking, one minute is not important. The important thing is to find the best solution based on time and computing resource requirements. A good vocabulary can quickly find common passwords, but if enough time and resources can be provided, the incremental mode can solve random passwords more effectively.