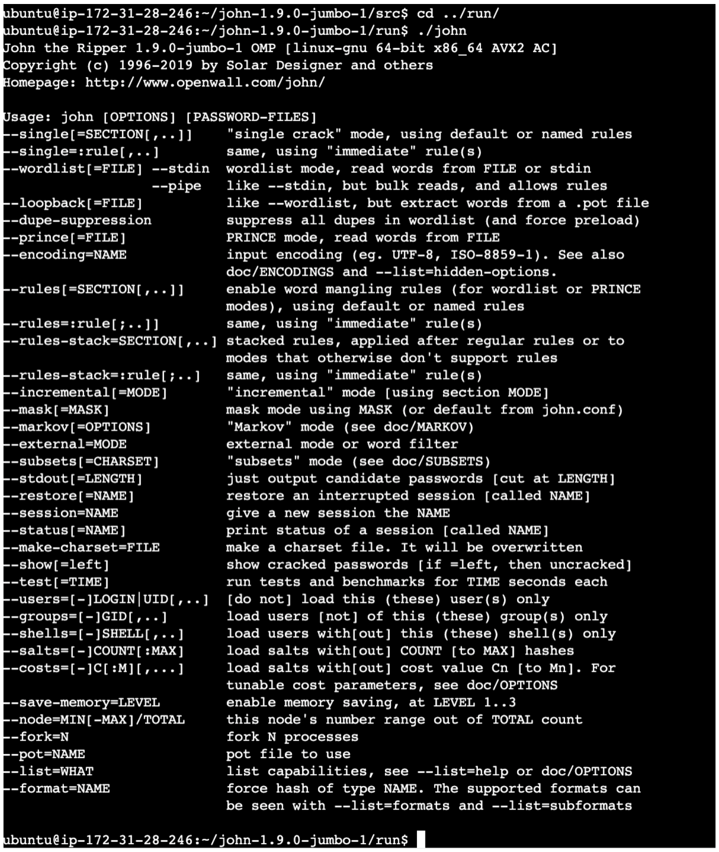
CSCI180 Lab4 Report

Xiaoming Huang

Task 1: Installing John the Ripper

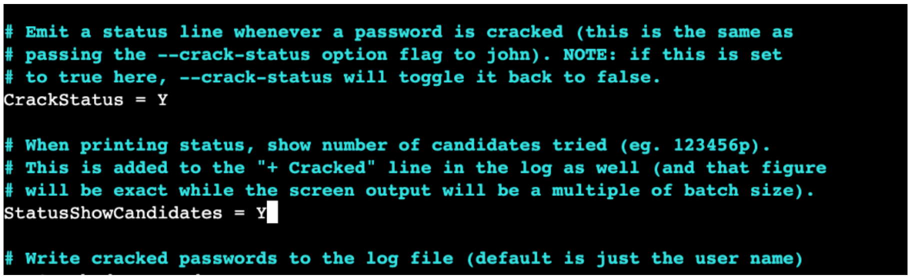
Result:



```
ubuntu@ip-172-31-28-246:~/john-1.9.0-jumbo-1/src$ cd ../run/
ubuntu@ip-172-31-28-246:~/john-1.9.0-jumbo-1/run$ ./john
John the Ripper 1.9.0-jumbo-1 OMP [linux-gnu 64-bit x86_64 AVX2 AC]
Copyright (c) 1996-2019 by Solar Designer and others
Homepage: http://www.openwall.com/john/

Usage: john [OPTIONS] [PASSWORD-FILES]
--single[=SECTION[,..]]    "single crack" mode, using default or named rules
--single=:rule[,..]        same, using "immediate" rule(s)
--wordlist[=FILE] --stdin  wordlist mode, read words from FILE or stdin
                  --pipe   like --stdin, but bulk reads, and allows rules
--loopback[=FILE]          like --wordlist, but extract words from a .pot file
--dupe-suppression         suppress all dupes in wordlist (and force preload)
--prince[=FILE]            PRINCE mode, read words from FILE
--encoding=NAME            input encoding (eg. UTF-8, ISO-8859-1). See also
                           doc/ENCODINGS and --list=hidden-options.
--rules[=SECTION[,..]]     enable word mangling rules (for wordlist or PRINCE
                           modes), using default or named rules
--rules=:rule[;..]]        same, using "immediate" rule(s)
--rules-stack=SECTION[,..] stacked rules, applied after regular rules or to
                           modes that otherwise don't support rules
--rules-stack=:rule[;..]   same, using "immediate" rule(s)
--incremental[=MODE]       "incremental" mode [using section MODE]
--mask[=MASK]              mask mode using MASK (or default from john.conf)
--markov[=OPTIONS]         "Markov" mode (see doc/MARKOV)
--external=MODE            external mode or word filter
--subsets[=CHARSET]        "subsets" mode (see doc/SUBSETS)
--stdout[=LENGTH]          just output candidate passwords [cut at LENGTH]
--restore[=NAME]           restore an interrupted session [called NAME]
--session=NAME             give a new session the NAME
--status[=NAME]            print status of a session [called NAME]
--make-charset=FILE        make a charset file. It will be overwritten
--show[=left]              show cracked passwords [if =left, then uncracked]
--test[=TIME]              run tests and benchmarks for TIME seconds each
--users=[-]LOGIN|UID[,..]  [do not] load this (these) user(s) only
--groups=[-]GID[,..]       load users [not] of this (these) group(s) only
--shells=[-]SHELL[,..]     load users with[out] this (these) shell(s) only
--salts=[-]COUNT[:MAX]     load salts with[out] COUNT [to MAX] hashes
--costs=[-]C[:M][,...]     load salts with[out] cost value Cn [to Mn]. For
                           tunable cost parameters, see doc/OPTIONS
--save-memory=LEVEL        enable memory saving, at LEVEL 1..3
--node=MIN[-MAX]/TOTAL     this node's number range out of TOTAL count
--fork=N                   fork N processes
--pot=NAME                 pot file to use
--list=WHAT                list capabilities, see --list=help or doc/OPTIONS
--format=NAME              force hash of type NAME. The supported formats can
                           be seen with --list=formats and --list=subformats

ubuntu@ip-172-31-28-246:~/john-1.9.0-jumbo-1/run$
```



```
# Emit a status line whenever a password is cracked (this is the same as
# passing the --crack-status option flag to john). NOTE: if this is set
# to true here, --crack-status will toggle it back to false.
CrackStatus = Y

# When printing status, show number of candidates tried (eg. 123456p).
# This is added to the "+ Cracked" line in the log as well (and that figure
# will be exact while the screen output will be a multiple of batch size).
StatusShowCandidates = Y

# Write cracked passwords to the log file (default is just the user name)
```

Changing:

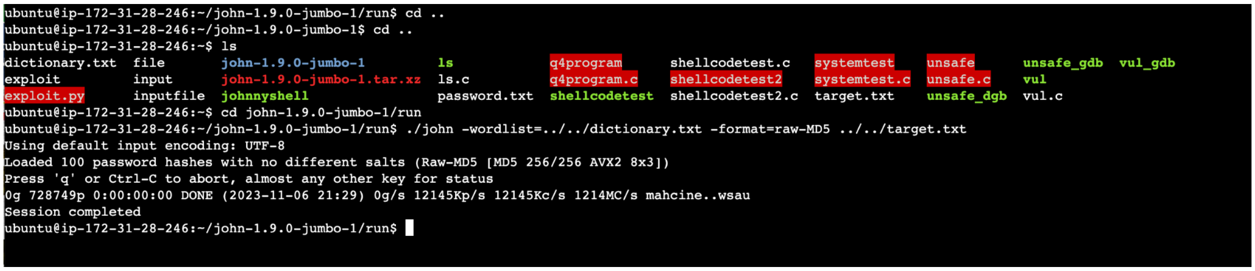
CrackStatus = Y

StatusShowCandidates = Y

Task 2: Cracking a set of passwords

1) *./john -wordlist=../../dictionary.txt -format=raw-MD5 ../../target.txt*

This is the standard wordlist mode only, and it just check the words from dictionary.txt to see if they match, but without any other setting, no password is cracked

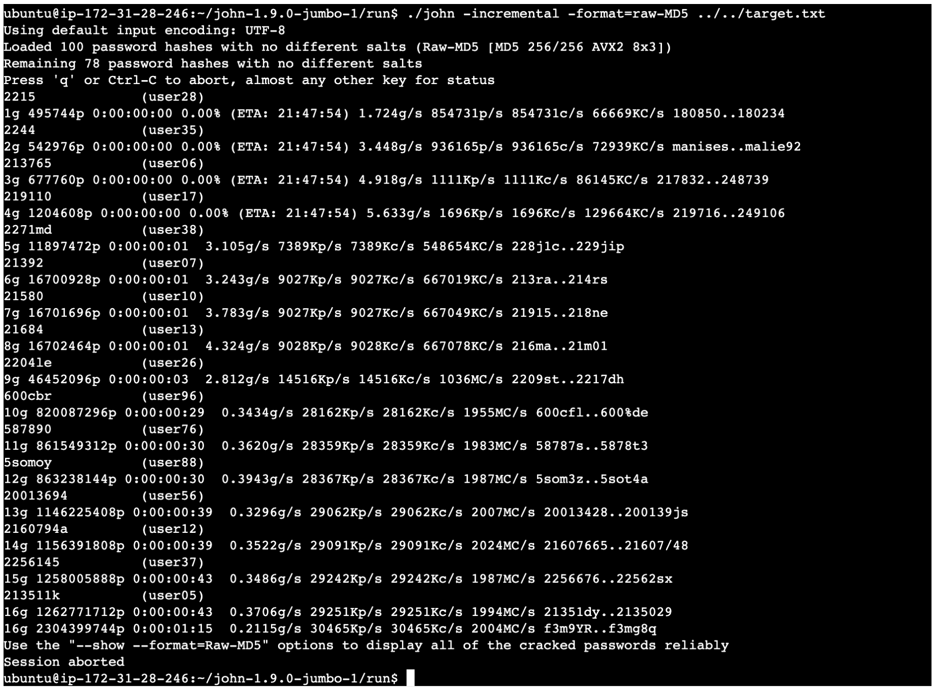


```
ubuntu@ip-172-31-28-246:~/john-1.9.0-jumbo-1/run$ cd ..
ubuntu@ip-172-31-28-246:~/john-1.9.0-jumbo-1$ cd ..
ubuntu@ip-172-31-28-246:~$ ls
dictionary.txt  file       john-1.9.0-jumbo-1         ls           q4program      shellcodetest.c    systemtest     unsafe       unsafe_gdb  vul_gdb
exploit         input      john-1.9.0-jumbo-1.tar.xz  ls.c         q4program.c    shellcodetest2     systemtest.c   unsafe.c     vul
exploit.py      inputfile  johnnyshell                password.txt shellcodetest  shellcodetest2.c   target.txt     unsafe_dgb   vul.c
ubuntu@ip-172-31-28-246:~$ cd john-1.9.0-jumbo-1/run
ubuntu@ip-172-31-28-246:~/john-1.9.0-jumbo-1/run$ ./john -wordlist=../../dictionary.txt -format=raw-MD5 ../../target.txt
Using default input encoding: UTF-8
Loaded 100 password hashes with no different salts (Raw-MD5 [MD5 256/256 AVX2 8x3])
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 728749p 0:00:00:00 DONE (2023-11-06 21:29) 0g/s 12145Kp/s 12145Kc/s 1214MC/s mahcine..wsau
Session completed
ubuntu@ip-172-31-28-246:~/john-1.9.0-jumbo-1/run$ █
```

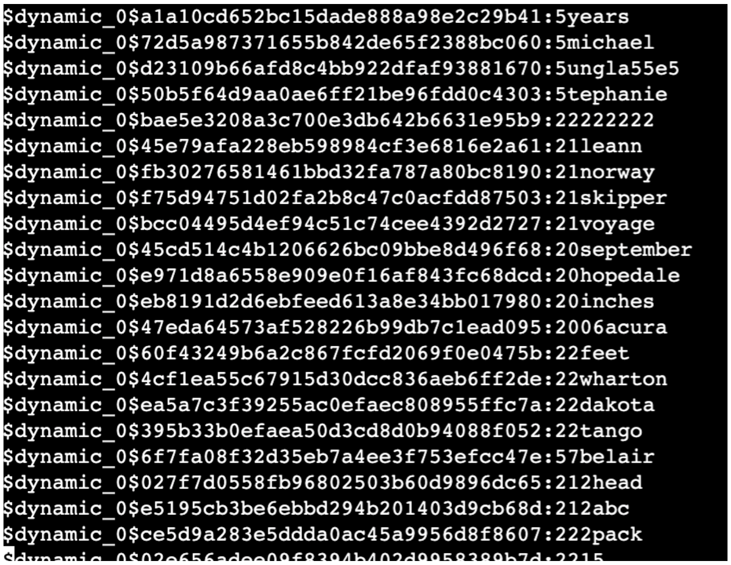
Result is John.pot is empty

2) *./john -wordlist=../../dictionary.txt -rules=dive -format=raw-MD5 ../../target.txt*

Based on the wordlist mode, I also use "*-rules=dive*" to expand the search range, and generate various password combinations.



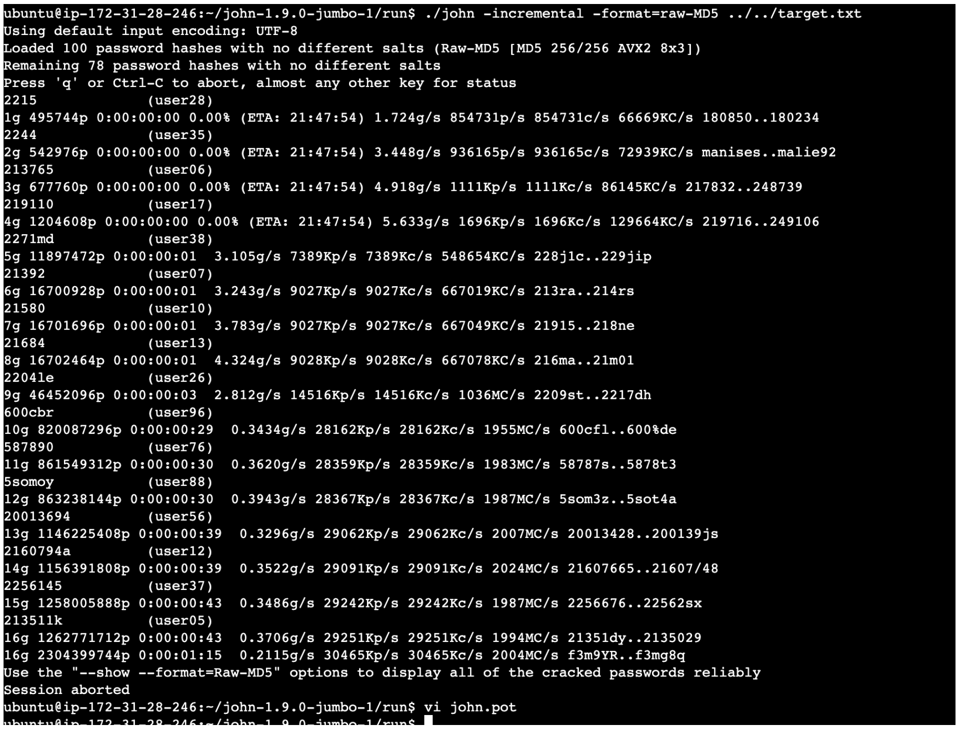
```
ubuntu@ip-172-31-28-246:~/john-1.9.0-jumbo-1/run$ ./john -incremental -format=raw-MD5 ../../target.txt
Using default input encoding: UTF-8
Loaded 100 password hashes with no different salts (Raw-MD5 [MD5 256/256 AVX2 8x3])
Remaining 78 password hashes with no different salts
Press 'q' or Ctrl-C to abort, almost any other key for status
2215             (user28)
1g 495744p 0:00:00:00 0.00% (ETA: 21:47:54) 1.724g/s 854731p/s 854731c/s 66669KC/s 180850..180234
2244             (user35)
2g 542976p 0:00:00:00 0.00% (ETA: 21:47:54) 3.448g/s 936165p/s 936165c/s 72939KC/s manises..malie92
213765           (user06)
3g 677760p 0:00:00:00 0.00% (ETA: 21:47:54) 4.918g/s 1111Kp/s 1111Kc/s 86145KC/s 217832..248739
219110           (user17)
4g 1204608p 0:00:00:00 0.00% (ETA: 21:47:54) 5.633g/s 1696Kp/s 1696Kc/s 129664KC/s 219716..249106
2271md           (user38)
5g 11897472p 0:00:00:01  3.105g/s 7389Kp/s 7389Kc/s 548654KC/s 228j1c..229jip
21392            (user07)
6g 16700928p 0:00:00:01  3.243g/s 9027Kp/s 9027Kc/s 667019KC/s 213ra..214rs
21580            (user10)
7g 16701696p 0:00:00:01  3.783g/s 9027Kp/s 9027Kc/s 667049KC/s 21915..218ne
21684            (user13)
8g 16702464p 0:00:00:01  4.324g/s 9028Kp/s 9028Kc/s 667078KC/s 216ma..21m01
2204le           (user26)
9g 46452096p 0:00:00:03  2.812g/s 14516Kp/s 14516Kc/s 1036MC/s 2209st..2217dh
600cbr           (user96)
10g 820087296p 0:00:00:29  0.3434g/s 28162Kp/s 28162Kc/s 1955MC/s 600cfl..600%de
587890           (user76)
11g 861549312p 0:00:00:30  0.3620g/s 28359Kp/s 28359Kc/s 1983MC/s 58787s..5878t3
5somoy           (user88)
12g 863238144p 0:00:00:30  0.3943g/s 28367Kp/s 28367Kc/s 1987MC/s 5som3z..5sot4a
20013694         (user56)
13g 1146225408p 0:00:00:39  0.3296g/s 29062Kp/s 29062Kc/s 2007MC/s 20013428..200139js
2160794a         (user12)
14g 1156391808p 0:00:00:39  0.3522g/s 29091Kp/s 29091Kc/s 2024MC/s 21607665..21607/48
2256145          (user37)
15g 1258005888p 0:00:00:43  0.3486g/s 29242Kp/s 29242Kc/s 1987MC/s 2256676..22562sx
213511k          (user05)
16g 1262771712p 0:00:00:43  0.3706g/s 29251Kp/s 29251Kc/s 1994MC/s 21351dy..2135029
16g 2304399744p 0:00:01:15  0.2115g/s 30465Kp/s 30465Kc/s 2004MC/s f3m9YR..f3mg8q
Use the "--show --format=Raw-MD5" options to display all of the cracked passwords reliably
Session aborted
ubuntu@ip-172-31-28-246:~/john-1.9.0-jumbo-1/run$
```



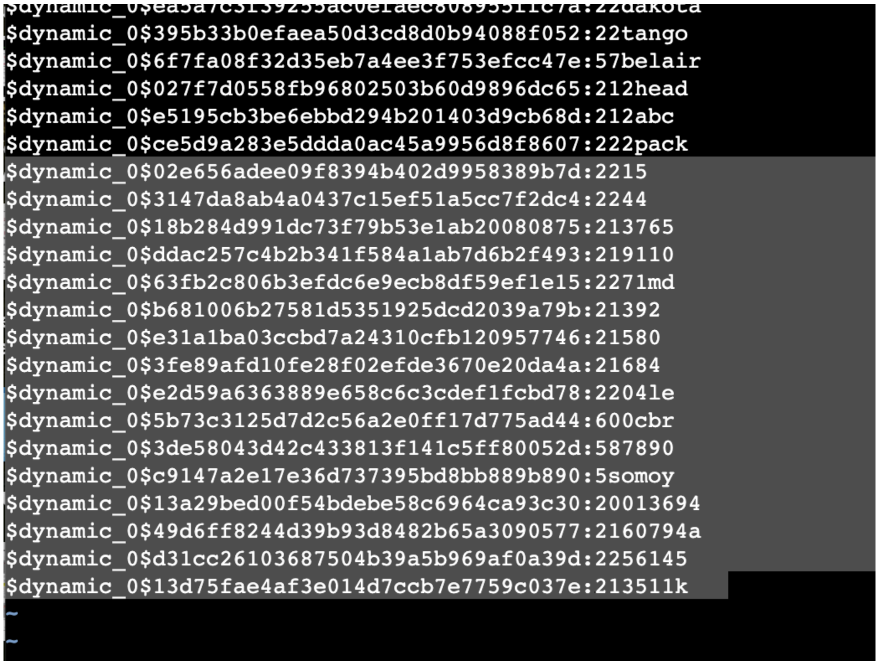
```
$dynamic_0$a1a10cd652bc15dade888a98e2c29b41:5years
$dynamic_0$72d5a987371655b842de65f2388bc060:5michael
$dynamic_0$d23109b66afd8c4bb922dfaf93881670:5ungla55e5
$dynamic_0$50b5f64d9aa0ae6ff21be96fdd0c4303:5tephanie
$dynamic_0$bae5e3208a3c700e3db642b6631e95b9:22222222
$dynamic_0$45e79afa228eb598984cf3e6816e2a61:21leann
$dynamic_0$fb30276581461bbd32fa787a80bc8190:21norway
$dynamic_0$f75d94751d02fa2b8c47c0acfdd87503:21skipper
$dynamic_0$bcc04495d4ef94c51c74cee4392d2727:21voyage
$dynamic_0$45cd514c4b1206626bc09bbe8d496f68:20september
$dynamic_0$e971d8a6558e909e0f16af843fc68dcd:20hopedale
$dynamic_0$eb8191d2d6ebfeed613a8e34bb017980:20inches
$dynamic_0$47eda64573af528226b99db7c1ead095:2006acura
$dynamic_0$60f43249b6a2c867fcfd2069f0e0475b:22feet
$dynamic_0$4cf1ea55c67915d30dcc836aeb6ff2de:22wharton
$dynamic_0$ea5a7c3f39255ac0efaec808955ffc7a:22dakota
$dynamic_0$395b33b0efaea50d3cd8d0b94088f052:22tango
$dynamic_0$6f7fa08f32d35eb7a4ee3f753efcc47e:57belair
$dynamic_0$027f7d0558fb96802503b60d9896dc65:212head
$dynamic_0$e5195cb3be6ebbd294b201403d9cb68d:212abc
$dynamic_0$ce5d9a283e5ddda0ac45a9956d8f8607:222pack
$dynamic_0$02e656adee09f8394b402d9958389b7d:2215
```

3) *./john -incremental -format=raw-MD5 ../../target.txt*

Directly using “incremental” mode, and use the default setting (the ASCII) for most hash types, and systematically generates and tests all possible password combinations within a given character set and length range. Similar to a brute-force.



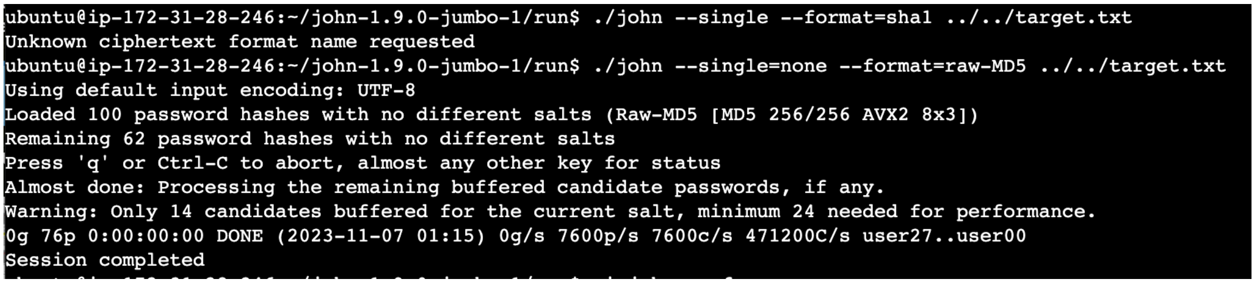
```
ubuntu@ip-172-31-28-246:~/john-1.9.0-jumbo-1/run$ ./john -incremental -format=raw-MD5 ../../target.txt
Using default input encoding: UTF-8
Loaded 100 password hashes with no different salts (Raw-MD5 [MD5 256/256 AVX2 8x3])
Remaining 78 password hashes with no different salts
Press 'q' or Ctrl-C to abort, almost any other key for status
2215             (user28)
1g 495744p 0:00:00:00 0.00% (ETA: 21:47:54) 1.724g/s 854731p/s 854731c/s 66669KC/s 180850..180234
2244             (user35)
2g 542976p 0:00:00:00 0.00% (ETA: 21:47:54) 3.448g/s 936165p/s 936165c/s 72939KC/s manises..malie92
213765           (user06)
3g 677760p 0:00:00:00 0.00% (ETA: 21:47:54) 4.918g/s 1111Kp/s 1111Kc/s 86145KC/s 217832..248739
219110           (user17)
4g 1204608p 0:00:00:00 0.00% (ETA: 21:47:54) 5.633g/s 1696Kp/s 1696Kc/s 129664KC/s 219716..249106
2271md           (user38)
5g 11897472p 0:00:00:01  3.105g/s 7389Kp/s 7389Kc/s 548654KC/s 228j1c..229jip
21392            (user07)
6g 16700928p 0:00:00:01  3.243g/s 9027Kp/s 9027Kc/s 667019KC/s 213ra..214rs
21580            (user10)
7g 16701696p 0:00:00:01  3.783g/s 9027Kp/s 9027Kc/s 667049KC/s 21915..218ne
21684            (user13)
8g 16702464p 0:00:00:01  4.324g/s 9028Kp/s 9028Kc/s 667078KC/s 216ma..21m01
2204le           (user26)
9g 46452096p 0:00:00:03  2.812g/s 14516Kp/s 14516Kc/s 1036MC/s 2209st..2217dh
600cbr           (user96)
10g 820087296p 0:00:00:29  0.3434g/s 28162Kp/s 28162Kc/s 1955MC/s 600cfl..600%de
587890           (user76)
11g 861549312p 0:00:00:30  0.3620g/s 28359Kp/s 28359Kc/s 1983MC/s 58787s..5878t3
5somoy           (user88)
12g 863238144p 0:00:00:30  0.3943g/s 28367Kp/s 28367Kc/s 1987MC/s 5som3z..5sot4a
20013694         (user56)
13g 1146225408p 0:00:00:39  0.3296g/s 29062Kp/s 29062Kc/s 2007MC/s 20013428..200139js
2160794a         (user12)
14g 1156391808p 0:00:00:39  0.3522g/s 29091Kp/s 29091Kc/s 2024MC/s 21607665..21607/48
2256145          (user37)
15g 1258005888p 0:00:00:43  0.3486g/s 29242Kp/s 29242Kc/s 1987MC/s 2256676..22562sx
213511k          (user05)
16g 1262771712p 0:00:00:43  0.3706g/s 29251Kp/s 29251Kc/s 1994MC/s 21351dy..2135029
16g 2304399744p 0:00:01:15  0.2115g/s 30465Kp/s 30465Kc/s 2004MC/s f3m9YR..f3mg8q
Use the "--show --format=Raw-MD5" options to display all of the cracked passwords reliably
Session aborted
ubuntu@ip-172-31-28-246:~/john-1.9.0-jumbo-1/run$ vi john.pot
ubuntu@ip-172-31-28-246:~/john-1.9.0-jumbo-1/run$
```



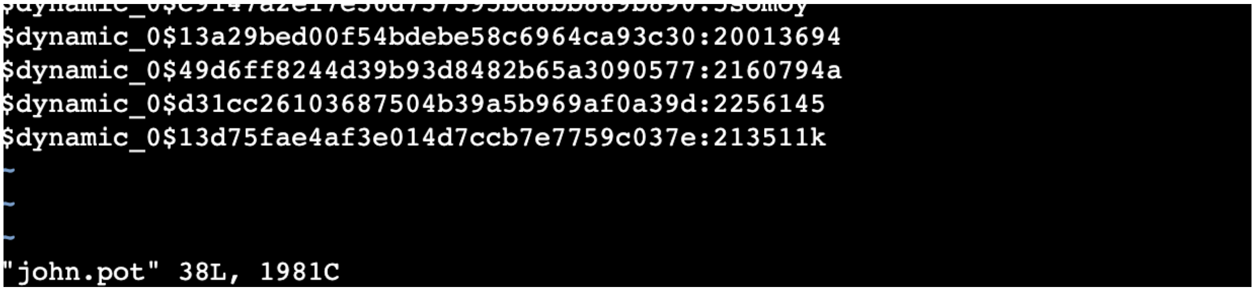
```
$dynamic_0$ea5a7c3139255ac0e1aec8089551fc7a:22dakota
$dynamic_0$395b33b0efaea50d3cd8d0b94088f052:22tango
$dynamic_0$6f7fa08f32d35eb7a4ee3f753efcc47e:57belair
$dynamic_0$027f7d0558fb96802503b60d9896dc65:212head
$dynamic_0$e5195cb3be6ebbd294b201403d9cb68d:212abc
$dynamic_0$ce5d9a283e5ddda0ac45a9956d8f8607:222pack
$dynamic_0$02e656adee09f8394b402d9958389b7d:2215
$dynamic_0$3147da8ab4a0437c15ef51a5cc7f2dc4:2244
$dynamic_0$18b284d991dc73f79b53e1ab20080875:213765
$dynamic_0$ddac257c4b2b341f584a1ab7d6b2f493:219110
$dynamic_0$63fb2c806b3efdc6e9ecb8df59ef1e15:2271md
$dynamic_0$b681006b27581d5351925dcd2039a79b:21392
$dynamic_0$e31a1ba03ccbd7a24310cfb120957746:21580
$dynamic_0$3fe89afd10fe28f02efde3670e20da4a:21684
$dynamic_0$e2d59a6363889e658c6c3cdef1fcbd78:2204le
$dynamic_0$5b73c3125d7d2c56a2e0ff17d775ad44:600cbr
$dynamic_0$3de58043d42c433813f141c5ff80052d:587890
$dynamic_0$c9147a2e17e36d737395bd8bb889b890:5somoy
$dynamic_0$13a29bed00f54bdebe58c6964ca93c30:20013694
$dynamic_0$49d6ff8244d39b93d8482b65a3090577:2160794a
$dynamic_0$d31cc26103687504b39a5b969af0a39d:2256145
$dynamic_0$13d75fae4af3e014d7ccb7e7759c037e:213511k
~
~
```

4) *./john --single --format=raw-MD5 ../../target.txt*

Using the “single=none” will crack passwords by using a combination of techniques such as using words from dictionaries, common passwords, and permutations of usernames. And this is the default "single crack" mode.



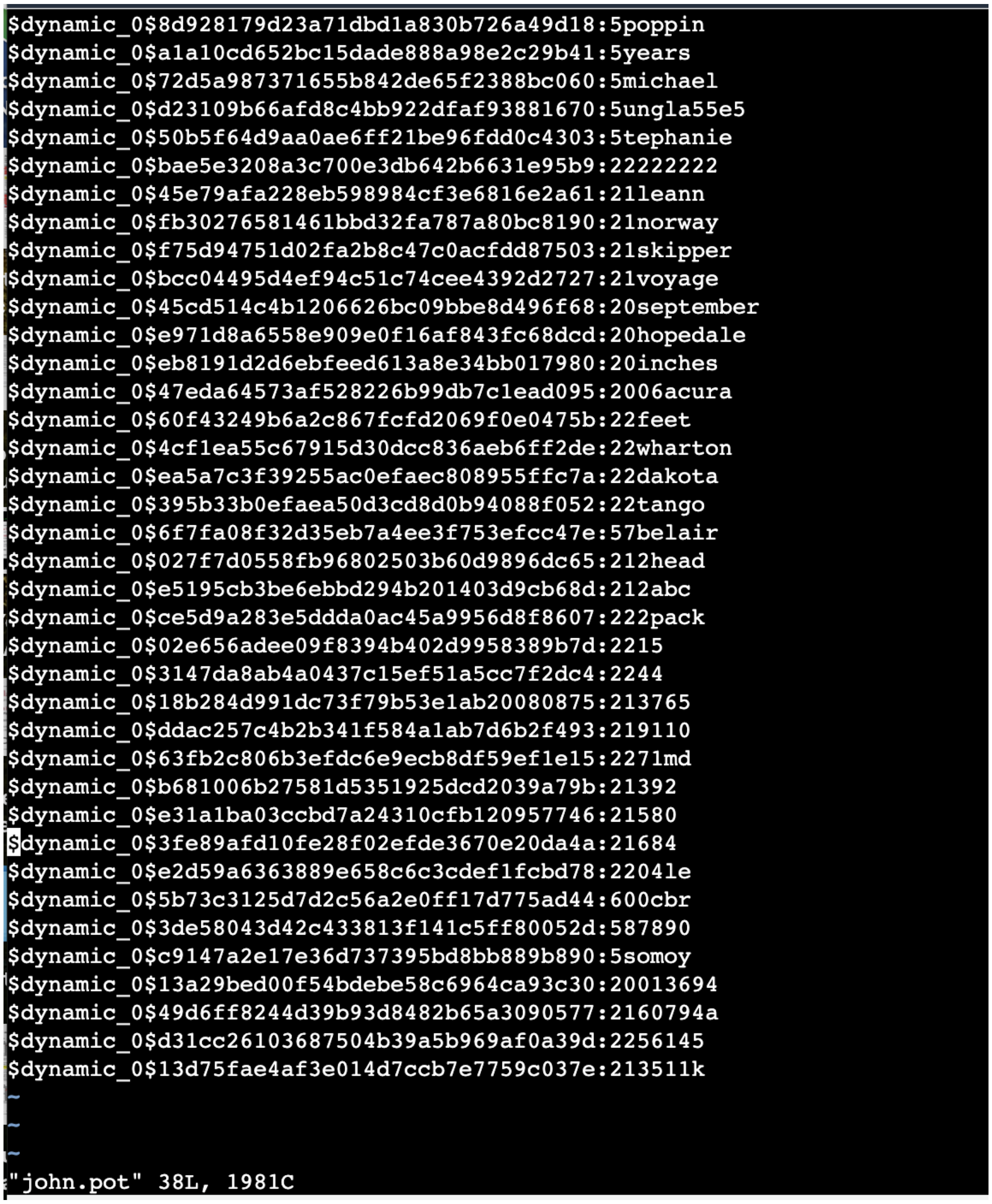
```
ubuntu@ip-172-31-28-246:~/john-1.9.0-jumbo-1/run$ ./john --single --format=sha1 ../../target.txt
Unknown ciphertext format name requested
ubuntu@ip-172-31-28-246:~/john-1.9.0-jumbo-1/run$ ./john --single=none --format=raw-MD5 ../../target.txt
Using default input encoding: UTF-8
Loaded 100 password hashes with no different salts (Raw-MD5 [MD5 256/256 AVX2 8x3])
Remaining 62 password hashes with no different salts
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Warning: Only 14 candidates buffered for the current salt, minimum 24 needed for performance.
0g 76p 0:00:00:00 DONE (2023-11-07 01:15) 0g/s 7600p/s 7600c/s 471200C/s user27..user00
Session completed
```



```
$dynamic_0$13a29bed00f54bdebe58c6964ca93c30:20013694
$dynamic_0$49d6ff8244d39b93d8482b65a3090577:2160794a
$dynamic_0$d31cc26103687504b39a5b969af0a39d:2256145
$dynamic_0$13d75fae4af3e014d7ccb7e7759c037e:213511k
~
~
~
"john.pot" 38L, 1981C
```

No password cracked, as no new passwords are added to the file.

Conclusion on all password cracked for four methods:

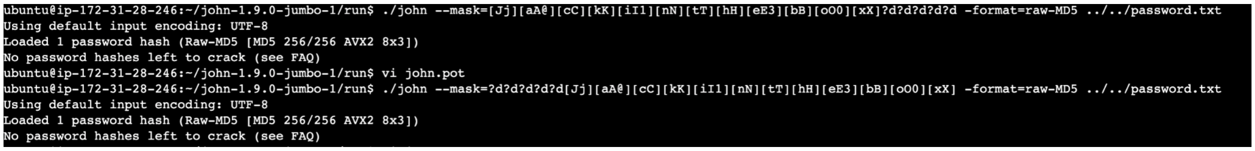


```
$dynamic_0$8d928179d23a71dbd1a830b726a49d18:5poppin
$dynamic_0$a1a10cd652bc15dade888a98e2c29b41:5years
$dynamic_0$72d5a987371655b842de65f2388bc060:5michael
$dynamic_0$d23109b66afd8c4bb922dfaf93881670:5ungla55e5
$dynamic_0$50b5f64d9aa0ae6ff21be96fdd0c4303:5tephanie
$dynamic_0$bae5e3208a3c700e3db642b6631e95b9:22222222
$dynamic_0$45e79afa228eb598984cf3e6816e2a61:21leann
$dynamic_0$fb30276581461bbd32fa787a80bc8190:21norway
$dynamic_0$f75d94751d02fa2b8c47c0acfdd87503:21skipper
$dynamic_0$bcc04495d4ef94c51c74cee4392d2727:21voyage
$dynamic_0$45cd514c4b1206626bc09bbe8d496f68:20september
$dynamic_0$e971d8a6558e909e0f16af843fc68dcd:20hopedale
$dynamic_0$eb8191d2d6ebfeed613a8e34bb017980:20inches
$dynamic_0$47eda64573af528226b99db7c1ead095:2006acura
$dynamic_0$60f43249b6a2c867fcfd2069f0e0475b:22feet
$dynamic_0$4cf1ea55c67915d30dcc836aeb6ff2de:22wharton
$dynamic_0$ea5a7c3f39255ac0efaec808955ffc7a:22dakota
$dynamic_0$395b33b0efaea50d3cd8d0b94088f052:22tango
$dynamic_0$6f7fa08f32d35eb7a4ee3f753efcc47e:57belair
$dynamic_0$027f7d0558fb96802503b60d9896dc65:212head
$dynamic_0$e5195cb3be6ebbd294b201403d9cb68d:212abc
$dynamic_0$ce5d9a283e5ddda0ac45a9956d8f8607:222pack
$dynamic_0$02e656adee09f8394b402d9958389b7d:2215
$dynamic_0$3147da8ab4a0437c15ef51a5cc7f2dc4:2244
$dynamic_0$18b284d991dc73f79b53e1ab20080875:213765
$dynamic_0$ddac257c4b2b341f584a1ab7d6b2f493:219110
$dynamic_0$63fb2c806b3efdc6e9ecb8df59ef1e15:2271md
$dynamic_0$b681006b27581d5351925dcd2039a79b:21392
$dynamic_0$e31a1ba03ccbd7a24310cfb120957746:21580
$dynamic_0$3fe89afd10fe28f02efde3670e20da4a:21684
$dynamic_0$e2d59a6363889e658c6c3cdef1fcbd78:2204le
$dynamic_0$5b73c3125d7d2c56a2e0ff17d775ad44:600cbr
$dynamic_0$3de58043d42c433813f141c5ff80052d:587890
$dynamic_0$c9147a2e17e36d737395bd8bb889b890:5somoy
$dynamic_0$13a29bed00f54bdebe58c6964ca93c30:20013694
$dynamic_0$49d6ff8244d39b93d8482b65a3090577:2160794a
$dynamic_0$d31cc26103687504b39a5b969af0a39d:2256145
$dynamic_0$13d75fae4af3e014d7ccb7e7759c037e:213511k
~
~
~
"john.pot" 38L, 1981C
```

Task 3: Find the password with the provided information:

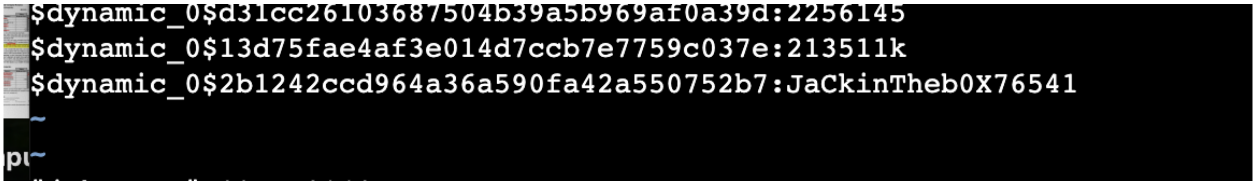
<u>Code:</u>

1) *./john --mask=[Jj][aA@][cC][kK][iI1][nN][tT][hH][eE3][bB][oO0][xX]?d?d?d?d?d -format=raw-MD5 ../../password.txt*
2) *./john --mask=?d?d?d?d?d [Jj][aA@][cC][kK][iI1][nN][tT][hH][eE3][bB][oO0][xX] -format=raw-MD5 ../../password.txt*



```
ubuntu@ip-172-31-28-246:~/john-1.9.0-jumbo-1/run$ ./john --mask=[Jj][aA@][cC][kK][iI1][nN][tT][hH][eE3][bB][oO0][xX]?d?d?d?d?d -format=raw-MD5 ../../password.txt
Using default input encoding: UTF-8
Loaded 1 password hash (Raw-MD5 [MD5 256/256 AVX2 8x3])
No password hashes left to crack (see FAQ)
ubuntu@ip-172-31-28-246:~/john-1.9.0-jumbo-1/run$ vi john.pot
ubuntu@ip-172-31-28-246:~/john-1.9.0-jumbo-1/run$ ./john --mask=?d?d?d?d?d[Jj][aA@][cC][kK][iI1][nN][tT][hH][eE3][bB][oO0][xX] -format=raw-MD5 ../../password.txt
Using default input encoding: UTF-8
Loaded 1 password hash (Raw-MD5 [MD5 256/256 AVX2 8x3])
No password hashes left to crack (see FAQ)
```

Result:



```
$dynamic_0$d31cc26103687504b39a5b969af0a39d:2256145
$dynamic_0$13d75fae4af3e014d7ccb7e7759c037e:213511k
$dynamic_0$2b1242ccd964a36a590fa42a550752b7:JaCkinTheb0X76541
~
~
```

I use the mask method, in the documentation, it says that "Mask mode have custom placeholders ?1..?9 that look similar to user classes # but are a different thing. They are merely defaults for the -1..-9 command # line options. As delivered, they resemble hashcat's defaults." And I think it matches with our description where we can potentially change from a to @, also potentially some additional characters at the end or at the beginning, which is also allowed with the mask mode.

We also keep

I have a [ ] for each character, and also include possible upper-lower shift for each character, and at the end, the password is cracked, and is "***<u>JaCkinTheb0X76541</u>***"