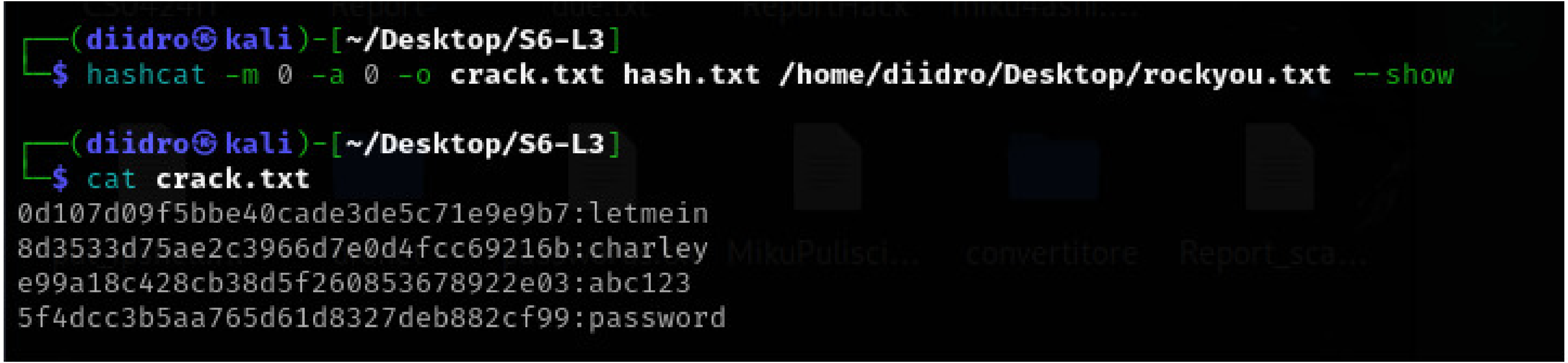
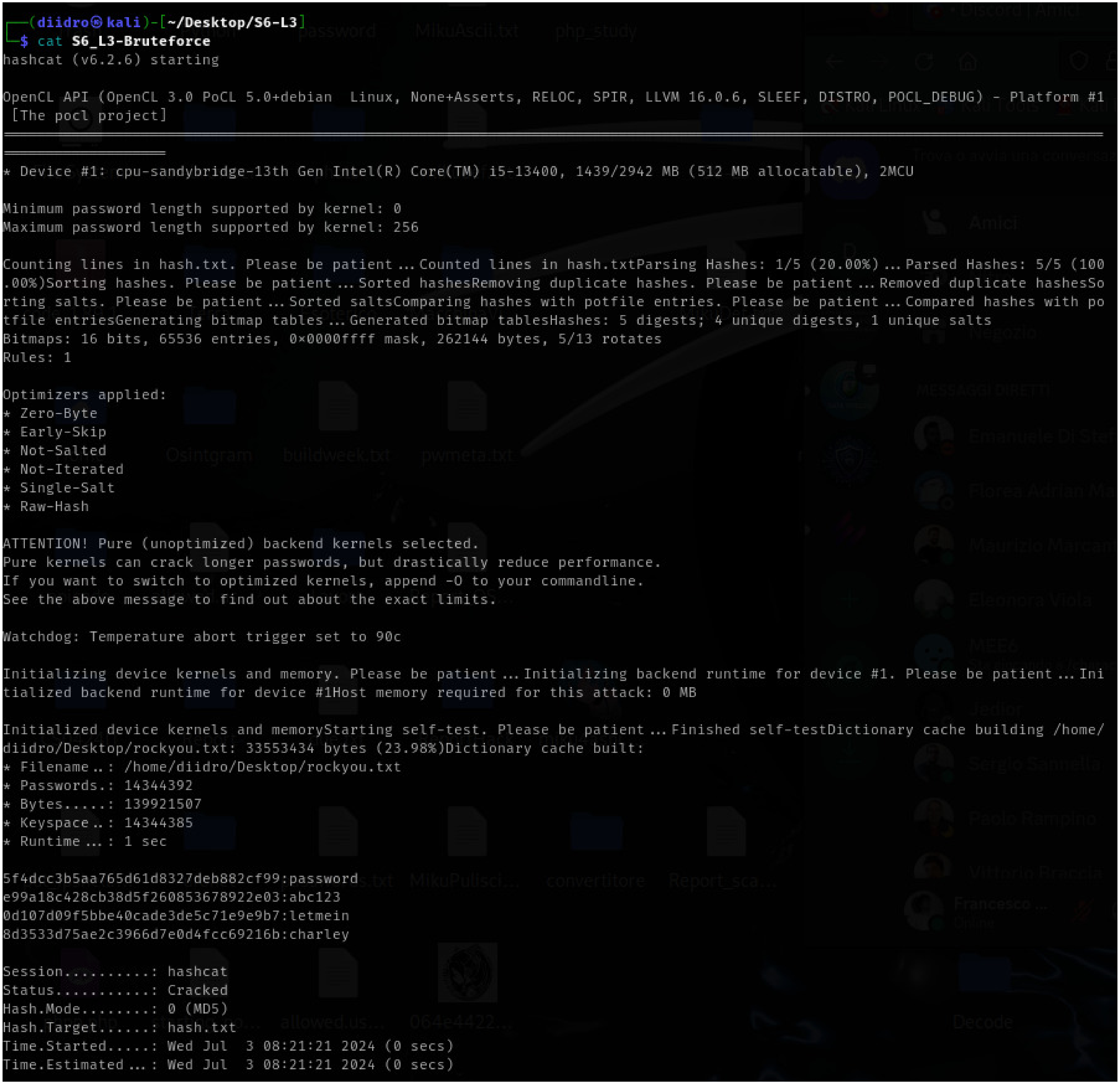
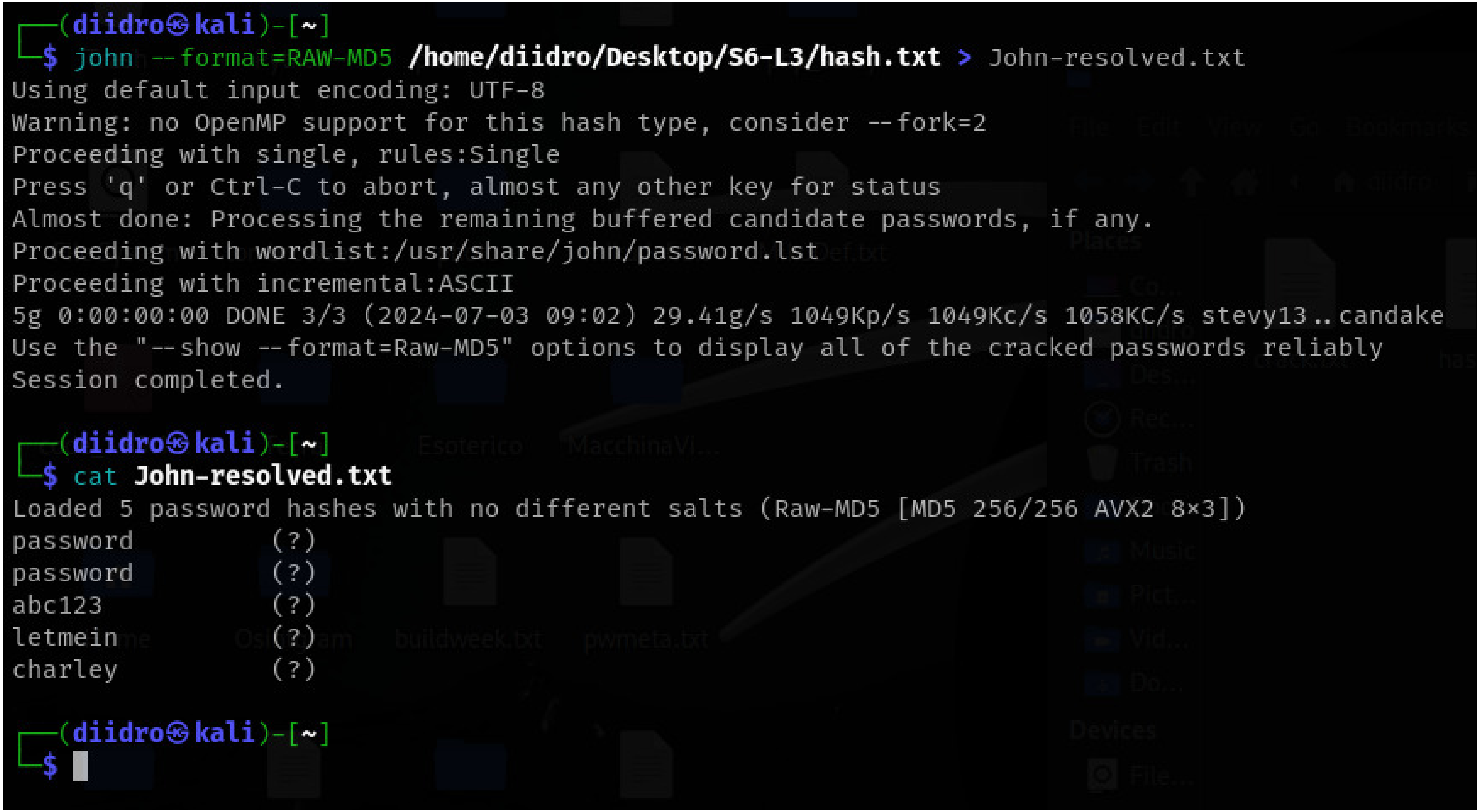


```
┌──(diidro㉿kali)-[~/Desktop/S6-L3]
└─$ hashcat -m 0 -a 0 -o crack.txt hash.txt /home/diidro/Desktop/rockyou.txt --show

┌──(diidro㉿kali)-[~/Desktop/S6-L3]
└─$ cat crack.txt
0d107d09f5bbe40cade3de5c71e9e9b7:letmein
8d3533d75ae2c3966d7e0d4fcc69216b:charley
e99a18c428cb38d5f260853678922e03:abc123
5f4dcc3b5aa765d61d8327deb882cf99:password
```



```
┌──(diidro㉿kali)-[~/Desktop/S6-L3]
└─$ cat S6_L3-Bruteforce
hashcat (v6.2.6) starting

OpenCL API (OpenCL 3.0 PoCL 5.0+debian  Linux, None+Asserts, RELOC, SPIR, LLVM 16.0.6, SLEEF, DISTRO, POCL_DEBUG) - Platform #1
 [The pocl project]
================================================================================================================================
===================
* Device #1: cpu-sandybridge-13th Gen Intel(R) Core(TM) i5-13400, 1439/2942 MB (512 MB allocatable), 2MCU

Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 256

Counting lines in hash.txt. Please be patient...Counted lines in hash.txtParsing Hashes: 1/5 (20.00%)...Parsed Hashes: 5/5 (100
.00%)Sorting hashes. Please be patient...Sorted hashesRemoving duplicate hashes. Please be patient...Removed duplicate hashesSo
rting salts. Please be patient...Sorted saltsComparing hashes with potfile entries. Please be patient...Compared hashes with po
tfile entriesGenerating bitmap tables...Generated bitmap tablesHashes: 5 digests; 4 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates
Rules: 1

Optimizers applied:
* Zero-Byte
* Early-Skip
* Not-Salted
* Not-Iterated
* Single-Salt
* Raw-Hash

ATTENTION! Pure (unoptimized) backend kernels selected.
Pure kernels can crack longer passwords, but drastically reduce performance.
If you want to switch to optimized kernels, append -O to your commandline.
See the above message to find out about the exact limits.

Watchdog: Temperature abort trigger set to 90c

Initializing device kernels and memory. Please be patient...Initializing backend runtime for device #1. Please be patient...Ini
tialized backend runtime for device #1Host memory required for this attack: 0 MB

Initialized device kernels and memoryStarting self-test. Please be patient...Finished self-testDictionary cache building /home/
diidro/Desktop/rockyou.txt: 33553434 bytes (23.98%)Dictionary cache built:
* Filename..: /home/diidro/Desktop/rockyou.txt
* Passwords.: 14344392
* Bytes.....: 139921507
* Keyspace..: 14344385
* Runtime...: 1 sec

5f4dcc3b5aa765d61d8327deb882cf99:password
e99a18c428cb38d5f260853678922e03:abc123
0d107d09f5bbe40cade3de5c71e9e9b7:letmein
8d3533d75ae2c3966d7e0d4fcc69216b:charley

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 0 (MD5)
Hash.Target......: hash.txt
Time.Started.....: Wed Jul  3 08:21:21 2024 (0 secs)
Time.Estimated...: Wed Jul  3 08:21:21 2024 (0 secs)
```



```
┌──(diidro㉿kali)-[~]
└─$ john --format=RAW-MD5 /home/diidro/Desktop/S6-L3/hash.txt > John-resolved.txt
Using default input encoding: UTF-8
Warning: no OpenMP support for this hash type, consider --fork=2
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
Proceeding with incremental:ASCII
5g 0:00:00:00 DONE 3/3 (2024-07-03 09:02) 29.41g/s 1049Kp/s 1049Kc/s 1058KC/s stevy13..candake
Use the "--show --format=Raw-MD5" options to display all of the cracked passwords reliably
Session completed.

┌──(diidro㉿kali)-[~]
└─$ cat John-resolved.txt
Loaded 5 password hashes with no different salts (Raw-MD5 [MD5 256/256 AVX2 8×3])
password         (?)
password         (?)
abc123           (?)
letmein          (?)
charley          (?)

┌──(diidro㉿kali)-[~]
└─$ 
```