

# Cracking Passwords with `hashcat`

Using `hashcat` along with several wordlists obtained from <https://github.com/danielmiessler/SecLists/tree/master/Passwords>, I was able to crack 57 of the 148 hashes.

Running `hashcat` in Hybrid (Wordlist + Brute Force) mode allows us to quickly crack common passwords, and thereafter brute force our way through short passwords.

`hashcat` significantly accelerates the process by making use of available GPUs.

```
Session.....: hashcat
Status.....: Exhausted
Hash.Type.....: MD5
Hash.Target.....: ../hashes.txt
Time.Started.....: Thu Oct 10 23:48:26 2019 (19 secs)
Time.Estimated...: Thu Oct 10 23:48:45 2019 (0 secs)
Guess.Mask.....: ?1?2?2?2?2?2?2 [7]
Guess.Charset....: -1 ?l?d?u, -2 ?l?d, -3 ?l?d*!$@_, -4 Undefined
Guess.Queue.....: 7/15 (46.67%)
Speed.#1.....: 7031.0 MH/s (3.50ms) @ Accel:256 Loops:64 Thr:256 Vec:1
Recovered.....: 64/148 (43.24%) Digests, 0/1 (0.00%) Salts
Progress.....: 134960504832/134960504832 (100.00%)
Rejected.....: 0/134960504832 (0.00%)
Restore.Point....: 1679616/1679616 (100.00%)
Restore.Sub.#1...: Salt:0 Amplifier:80320-80352 Iteration:0-64
Candidates.#1....: 7z7w10y -> Xqxqxqg
Hardware.Mon.#1..: Temp: 62c Fan: 82% Util: 94% Core:1923MHz Mem:4513MHz Bus:8

52b2d1ad30dc855e46a484abb180d325:59873523
72deac1f7a7b70ead34b017fa0676b9b:Chjklm88
cc74c1cf76412cf024b84da7254ecbcd:haw2u521
0c5616c3772c470c9ea847e3ce4079dc:vladkool
8a8ed1d1160152f7656f5e823a8bdffa:tr0mb0n3
```