# Hashcat -- Crack Passwords in Minutes

Hashcat is an advanced free (License: MIT) multi-threaded password recovery tool and it is world's fastest password cracker and recovery utility, which supports multiple unique attack modes of attacks for more than 200 highly optimized hashing algorithms. Hashcat currently supports CPUs and GPUs and other hardware accelerators on Linux, Windows, and OSX, and has facilities to help enable distributed password cracking.

[**Hashcat**](https://hashcat.net/hashcat/) comes pre-installed on our Kali Linux system, So we don't need to install it, but if installation is required we can use **sudo apt install hashcat** command.

# Features of Hashcat

* World's fastest password cracker.
* World's first and only in-kernel rule engine.
* Free and open source.
* Multi-OS (Linux, Windows and macOS).
* Multi-Hash (Cracking multiple hashes at the same time).
* Multi-Device-Types (Utilizing mixed device types in same system).
* Supports password candidate brain functionality.
* Supports distributed cracking networks (using overlay).
* ... and much more.

Hashcat offers multiple unique attack modes for cracking passwords. Those are following:

* Brute-Force attack
* Combinator attack
* Dictionary attack
* Fingerprint attack
* Hybrid attack

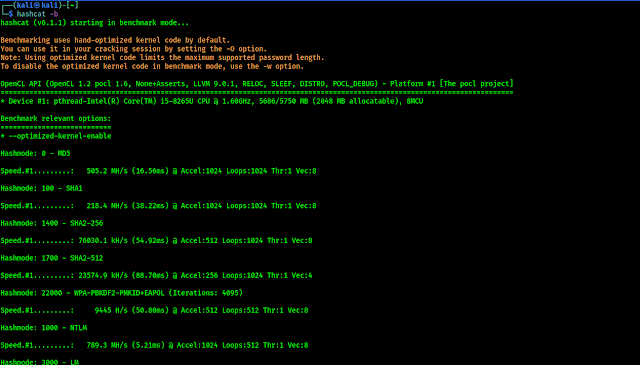
Now without wasting any more time lets dive into Hashcat.

# Hashcat on Kali Linux

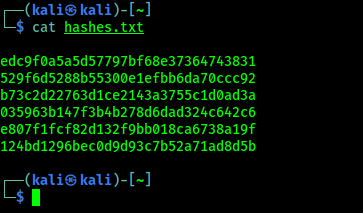
As we told Hashcat comes pre-installed with a Kali Linux and it is multi-threaded so first let we benchmark our system by using following command:

hashcat -b

In the following screenshot we can see the benchmark of our system and get an idea how it can perform while cracking various types of hashes.

[](https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEh0GlVJWqD3_qor6Ak-lKNcb9QSM8-gHvt-Cu1wyaYOXgGXq5t2Jq-YhS4RPCmnA-8q_Gp3mYGjIelkZWJ-jmixA21Ub0lViPxHapZ9Hqnsxjv9UpjXzcdYPosrwbwJKZUSofOjDZDzEY4/s1248/benchmark+hashcat.png)

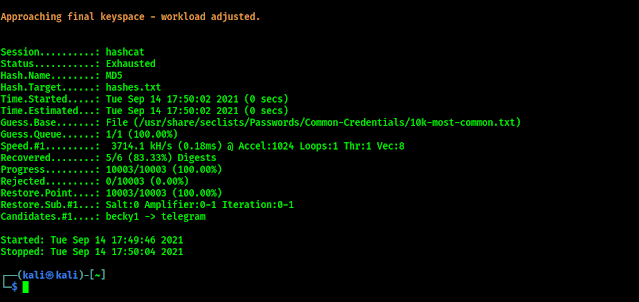
Here we can get an idea about the performance of our system. Let's run this tool to crack some hashes. Here we have collected some hashed on a text file. For educational purposes we just generated these hashed not collected from any website's database.

[](https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEiaYQhnBllnKmDA07DL1AzqbqYRgcDdxG8FdMc8xxG1nB4EMtzhARQKnKb_4IWbppBMdn-afv2cTOyTO8RU6XUD_KlVP3utWlccB74Uynf0-8Uh4cNPbwY4wh_kXrH4ypmxcdK2jnxToGA/s363/hashes.png)

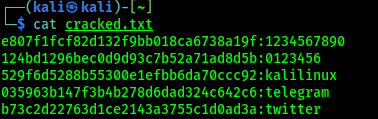
Now we can crack these using Hashcat, and store the output in a craced.txt file by applying following command:

hashcat -m 0 -a 0 -o cracked.txt hashes.txt /usr/share/seclists/Passwords/Common-Credentials/10k-most-common.txt

Let's discuss about the above command, in this command we have used **-m** flag to specify the hash type, **-a** for attack mode and **-o** for output file, here we named our output file 'cracked.txt', then we give the target hash file to crack named 'hashes.txt', at last we specify the wordlist file to be used. In the following screenshot we can see that hashcat finishes the cracking job.

[](https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEijl2TRaKeSUWCun9nBgQa8gJcrufjzcUjHMTRqUwgP6mABJRjyEbfttzTvCjKzqtomlfuT__2_2LogXzS2TSdG173O8S9w1BYeP4yN20xGR0312GlnNd8rwYSRW8oiOMY_p4e3VcsTxCA/s924/hashcat+work+done.png)

Let's see our output file (cracked.txt).

[](https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEhI0XLaFZ0xuWcDwKXpvHvOcPLde4HZ17MShifuleTi-zWkv7FyWHXbu0zqWaqsccfi6lrVvITK1z7qlcyF_BrhnCgduePs64FCYpJRPrE3M0aNlMEElnun5Om-R_qhCRwcinMQizVQFGQ/s378/hashcat+password+recovered.png)

In the above screenshot we can see that hashcat cracked the hashes. Here for the new readers, in this attack mode we can crack those password hashes if the plaintext of the hashes is available in the wordlist file. Using bigger wordlist file will increase the chance to crack hashes.

# Hashcat & Type of Hashes & Attacks

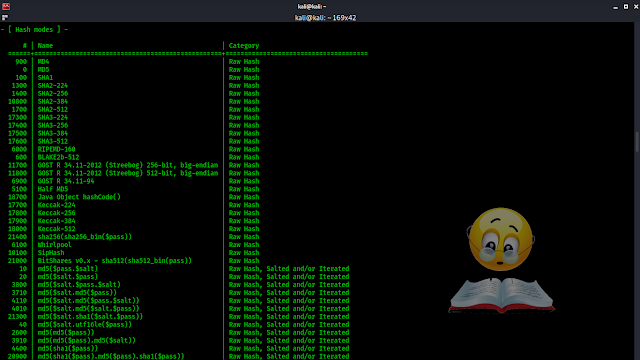
In the above we saw that we need to specify our attack modes and type of hashes we want to crack. These attack modes and hashes are refereed by numbers. Here we are giving hashcat supported all numbers that referees to the attack modes and the type of hashes (as Sep 2021, update of Hashcat tool may include some new things).

## Attack Types of Hashcat

  0 | Straight  
  1 | Combination  
  3 | Brute-force  
  6 | Hybrid Wordlist + Mask  
  7 | Hybrid Mask + Wordlist

## Hash types in Hashcat

Hashcat supports so much types of hashes if we include all them here then this article will very lengthy. We encourage to use **hashcat - h** command on our Kali Linux system to get all the numbers corresponding to the hash type (Uff.. It's really large 😫).

[](https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEgQ3QzRInbon7kZ9msdNkNbyAcNYxToVcXLEJa5-qkCF06z_OBNAK-Sb1YO7chcKZcho_O_Om7vqoel4KbGtl6q-P7ZuRB7rKYaPBp4nV-WWuHMvV9kgbTT53MuKy1ZIs-IPl7Pz5ajwY0/s1366/hash+types+in+hashcat.png)

Whenever we are trying to crack a hash we have to know the type of the hash. We can use [**hash-id**](https://www.kalilinux.in/2019/03/hash-id-hash-identifier.html) tool to know the type of hash. Then we need to choose our attack type and wordlist. That's all it's not hard.

This is all about Hashcat, and how we can use Hashcat to crack passwords on our Kali Linux. Hashcat (#🐈) is really a very widely used tool for cracking passwords.