One-way function (B. Schneier, Applied Cryptography: Protocols, Algorithms and Source Code in C, 20th Anniversary Edition: https://learning.oreilly.com/library/view/applied-cryptography-protocols/9781119096726/10\_chap02.html#chap02-sec003)

* Easy to compute but hard (nearly impossible) to reverse
* No secret parts so it can be public
* It cannot be used for encryptions as-is because encrypted message cannot be decrypted
* Trapdoor one-way function has a secret that helps to decode one way function which leaves us with the problem of sharing secrets between parties
* One-way functions have a lot of use, e.g. checksum of downloaded file to validate that the file is original and not modified

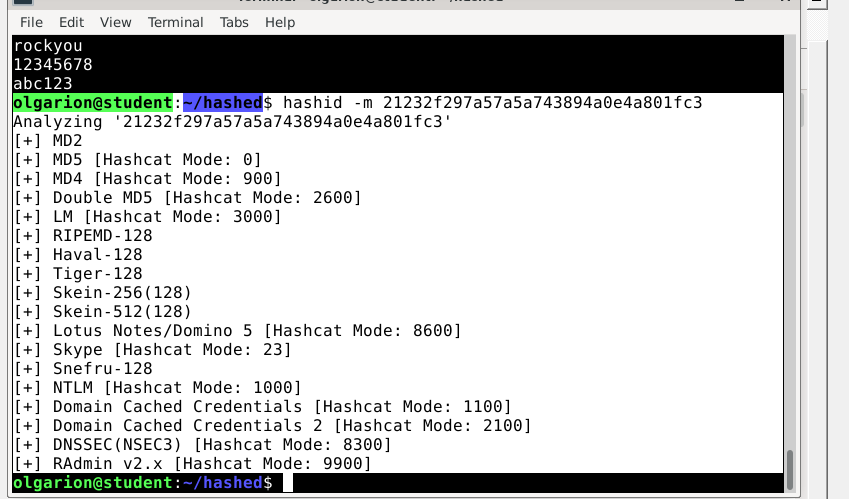
‘A hash function is a function, mathematical or otherwise, that takes a variable-length input string (called a pre-image) and converts it to a fixed-length (generally smaller) output string (called a hash value).’(B. Schneier, Applied Cryptography: Protocols, Algorithms and Source Code in C, 20th Anniversary Edition)

A one-way hash function is a hash function that works in one way only, it is easy to generate a hash value but it is hard to re-create the pre-image that leads to a particular values.

<https://terokarvinen.com/2022/cracking-passwords-with-hashcat/>

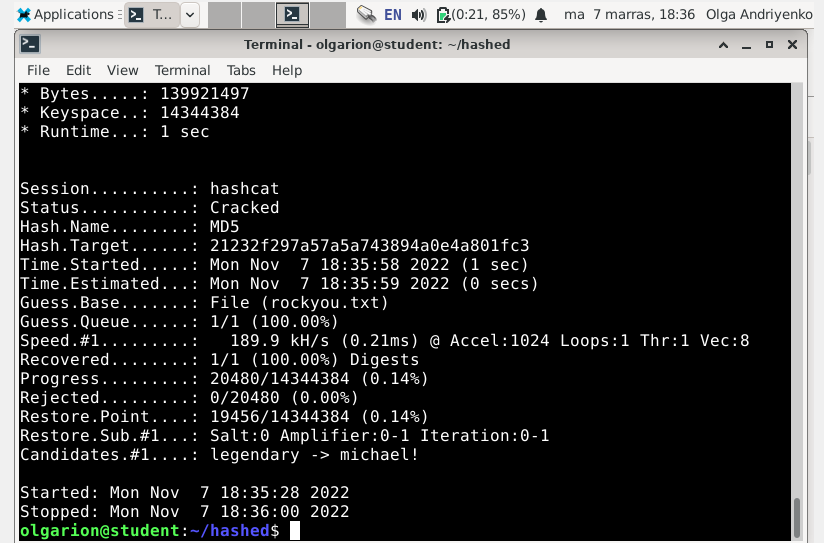
b) Crack this hash: 21232f297a57a5a743894a0e4a801fc3

Identify Hash Types of the 21232f297a57a5a743894a0e4a801fc3



I used hash type MD5 as in the exercise

$ hashcat -m 0 '21232f297a57a5a743894a0e4a801fc3' rockyou.txt -o solved

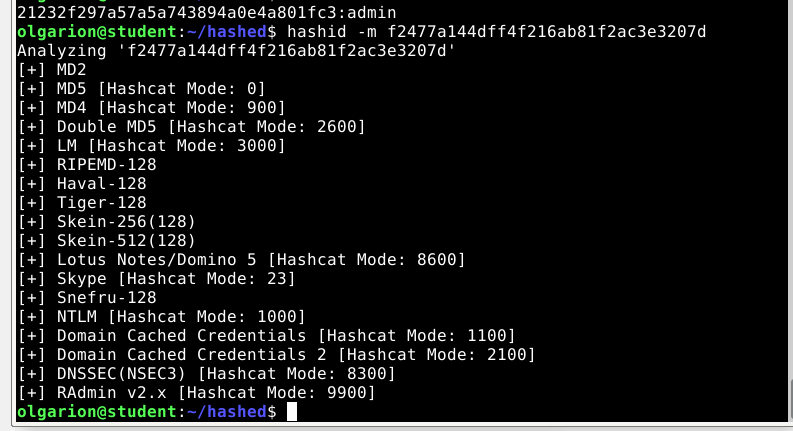




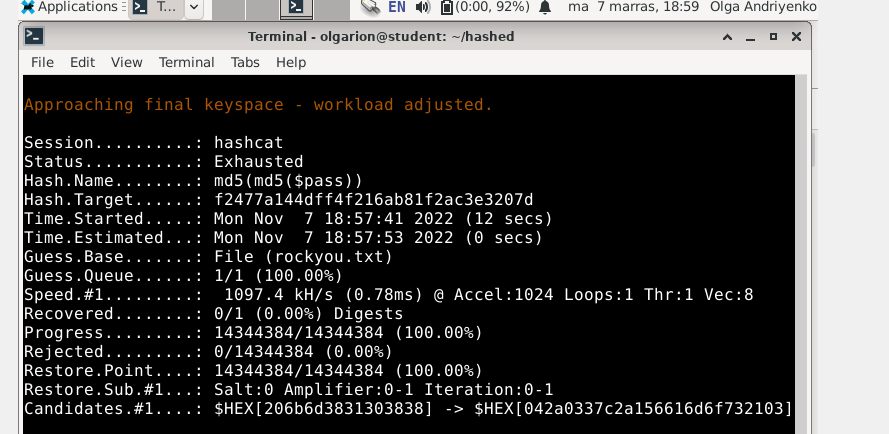
Password: admin

c) Crack this Windows NTLM hash: f2477a144dff4f216ab81f2ac3e3207d

Hash types:

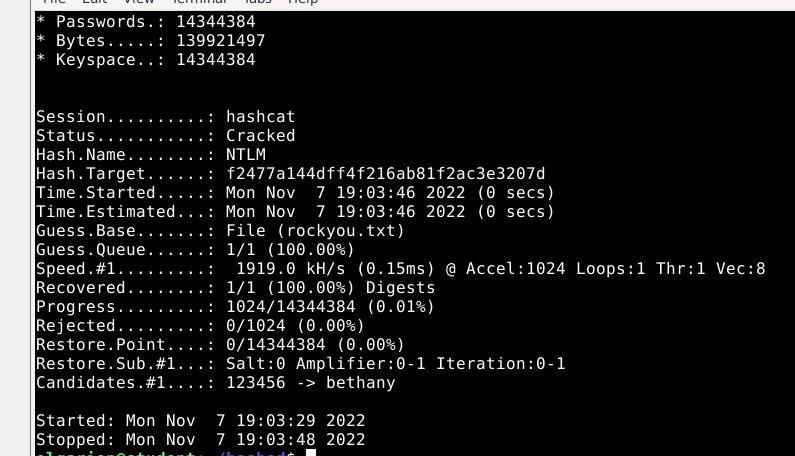


I used hash type Double MD5 and I got exhausted:



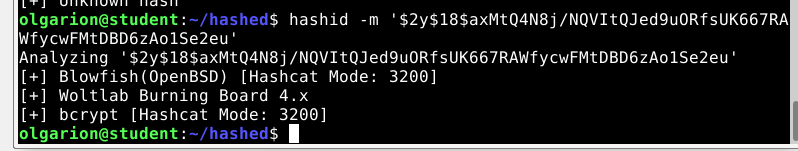
*Exhausted* simply means hashcat has tried every possible password combination in the attack you have provided, and failed to crack 100% of all hashes given. In other words, hashcat has finished doing everything you told it to do – it has *exhausted* its search to crack the hashes. You should run hashcat again with a different attack/word list/mask etc. (https://hashcat.net/wiki/doku.php?id=frequently\_asked\_questions#i\_may\_have\_the\_wrong\_driver\_installed\_what\_should\_i\_do)

When I chose type NTLM: 1000 it got cracked:

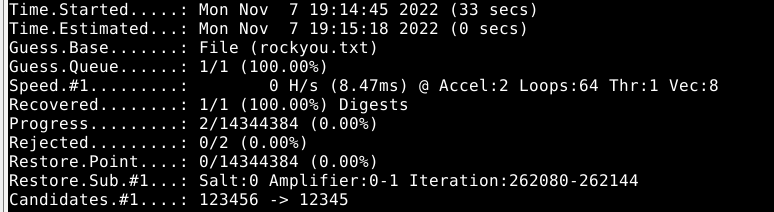


Password: monkey

d) Try cracking this hash and comment on your hash rate $2y$18$axMtQ4N8j/NQVItQJed9uORfsUK667RAWfycwFMtDBD6zAo1Se2eu . This subtask does not require actually cracking the hash, just trying it and commenting on the hash rate.



It took 3 sec to crack



I understand that it is the 2nd password it processed from the list.

f) Voluntary bonus: create some hashes of your own, then crack them with hashcat.

Generated at https://www.md5hashgenerator.com/

62a8119bc71653262e915983550b1885f80e2e3d

