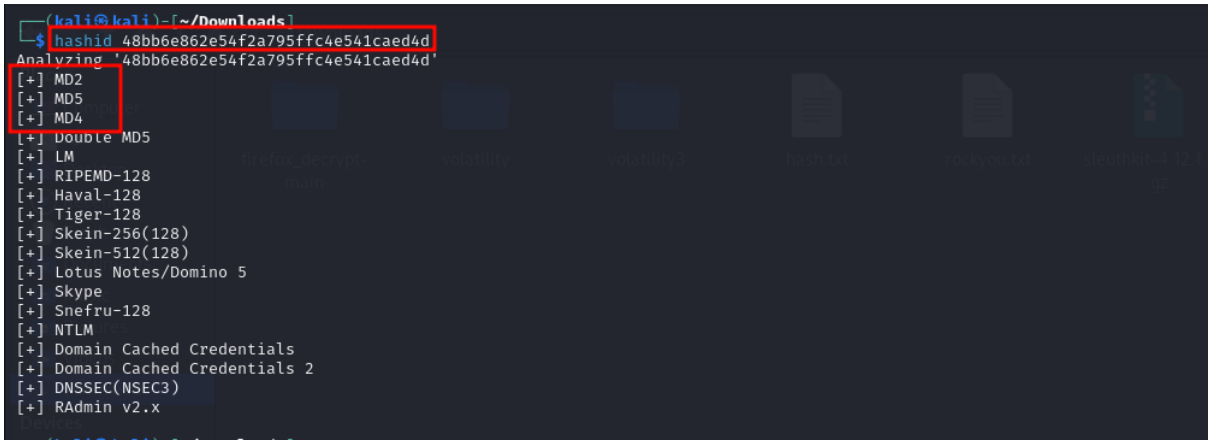
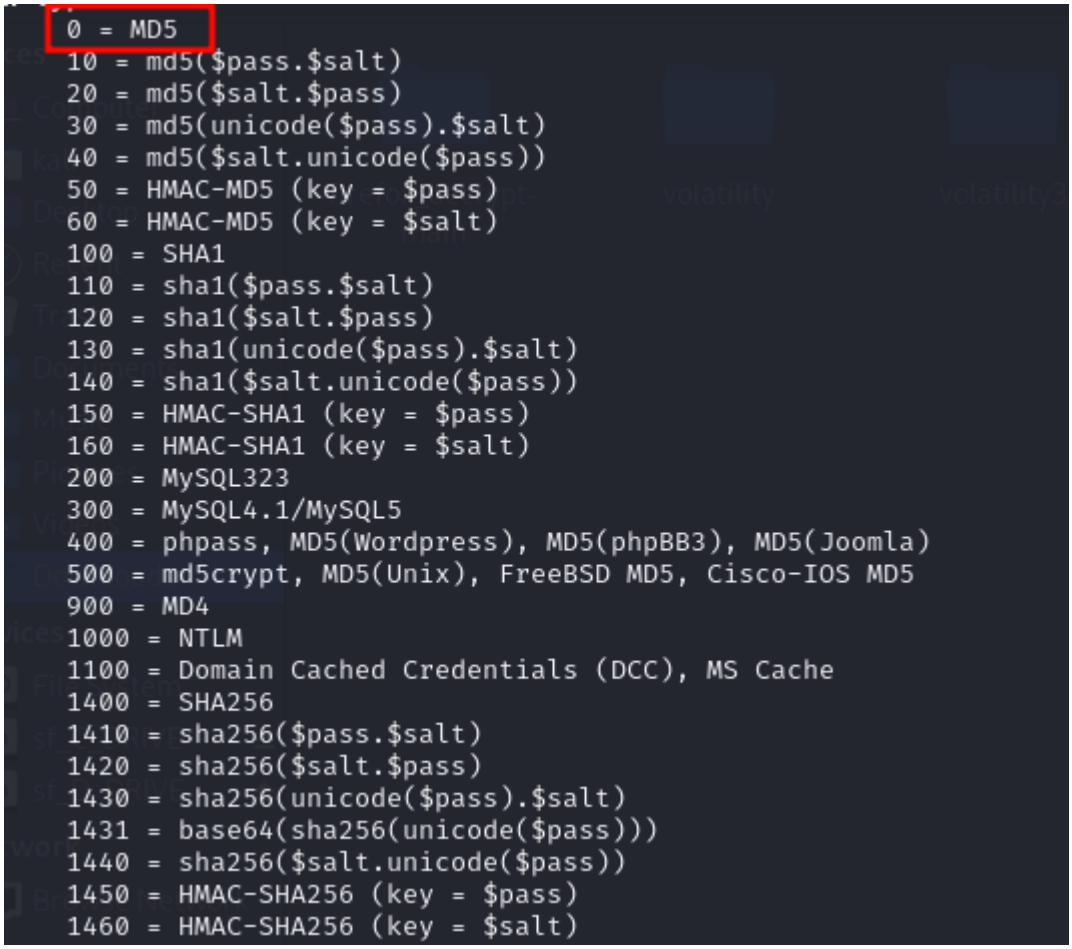
Digital Forensics – Lab#11

Ahmad Abdullah (i22-1609)

1. Hashid gave MD5 hash family



Using man hashcat it gave the number that we need to use for md5 which is 0.

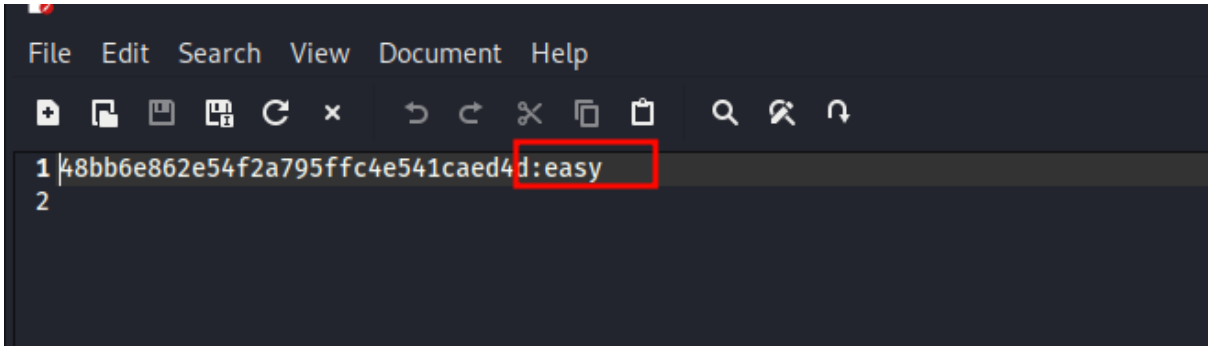


```
1700 = SHA512
1710 = sha512($pass.$salt)
1720 = sha512($salt.$pass)
1730 = sha512(unicode($pass).$salt)
1740 = sha512($salt.unicode($pass))
1750 = HMAC-SHA512 (key = $pass)
1760 = HMAC-SHA512 (key = $salt)
1800 = SHA-512(Unix)
2400 = Cisco-PIX MD5
2410 = Cisco-ASA MD5
2500 = WPA/WPA2
2600 = Double MD5
3200 = bcrypt, Blowfish(OpenBSD)
3300 = MD5(Sun)
3500 = md5(md5(md5($pass)))
3610 = md5(md5($salt).$pass)
3710 = md5($salt.md5($pass))
3720 = md5($pass.md5($salt))
3800 = md5($salt.$pass.$salt)
3910 = md5(md5($pass).md5($salt))
4010 = md5($salt.md5($salt.$pass))
```

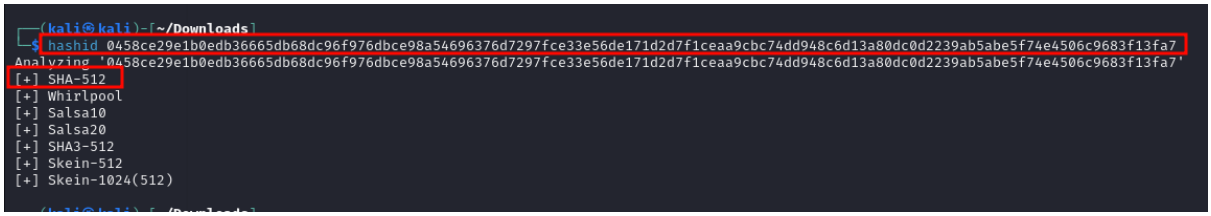
Using the command and giving some seconds, it gave us

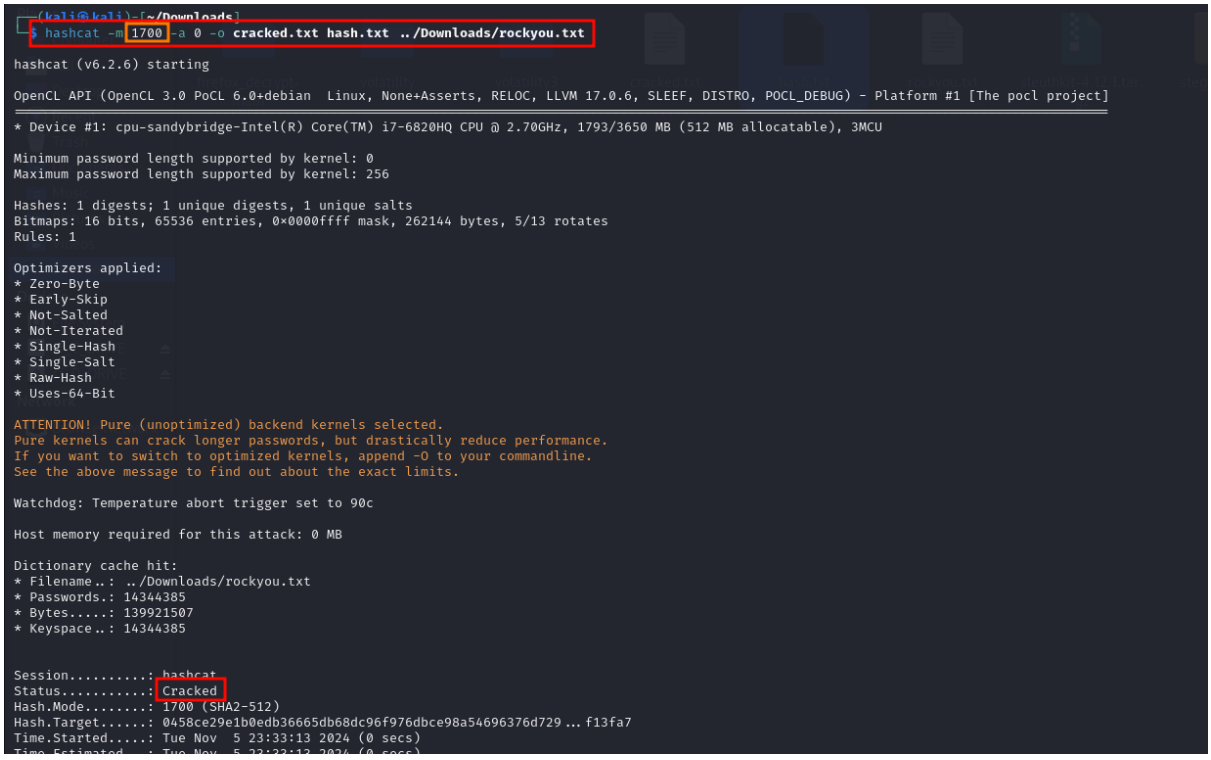
```
┌──(kali㉿kali)-[~/Downloads]
└─$ hashcat -m 0 -a 0 -o cracked.txt hash.txt ../Downloads/rockyou.txt

hashcat (v6.2.6) starting

OpenCL API (OpenCL 3.0 PoCL 6.0+debian  Linux, None+Asserts, RELOC, LLVM 17.0.6, SLEEF, DISTRO, POCL_DEBUG) - Platform #1 [The
═══════════════════════════════════════════════════════════════════════════════════════════════════════════════════════════
* Device #1: cpu-sandybridge-Intel(R) Core(TM) i7-6820HQ CPU @ 2.70GHz, 1793/3650 MB (512 MB allocatable), 3MCU

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

Hashes: 1 digests; 1 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0×0000ffff mask, 262144 bytes, 5/13 rotates
Rules: 1

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

Host memory required for this attack: 0 MB

Dictionary cache hit:
* Filename..: ../Downloads/rockyou.txt
* Passwords.: 14344385
* Bytes.....: 139921507
* Keyspace..: 14344385


Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 0 (MD5)
Hash.Target......: 48bb6e862e54f2a795ffc4e541caed4d
```

I used the command -o cracked.txt to output it in the file rather than showing the password in the terminal. The password is *'easy'*.

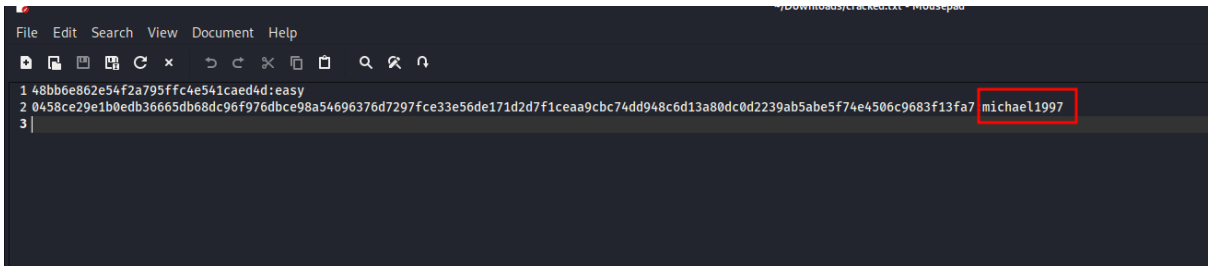


2. Hashid identified this hash as SHA-512 so we used 1700 number for this and rest of the command was same.

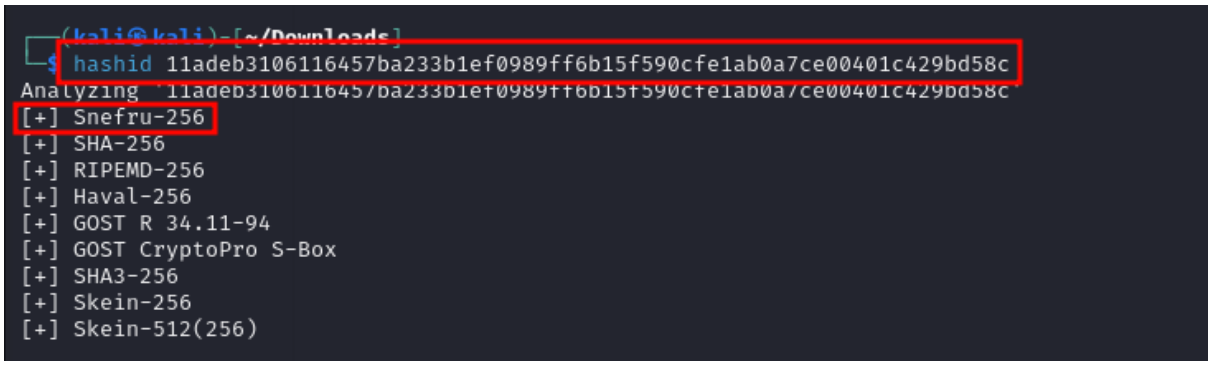


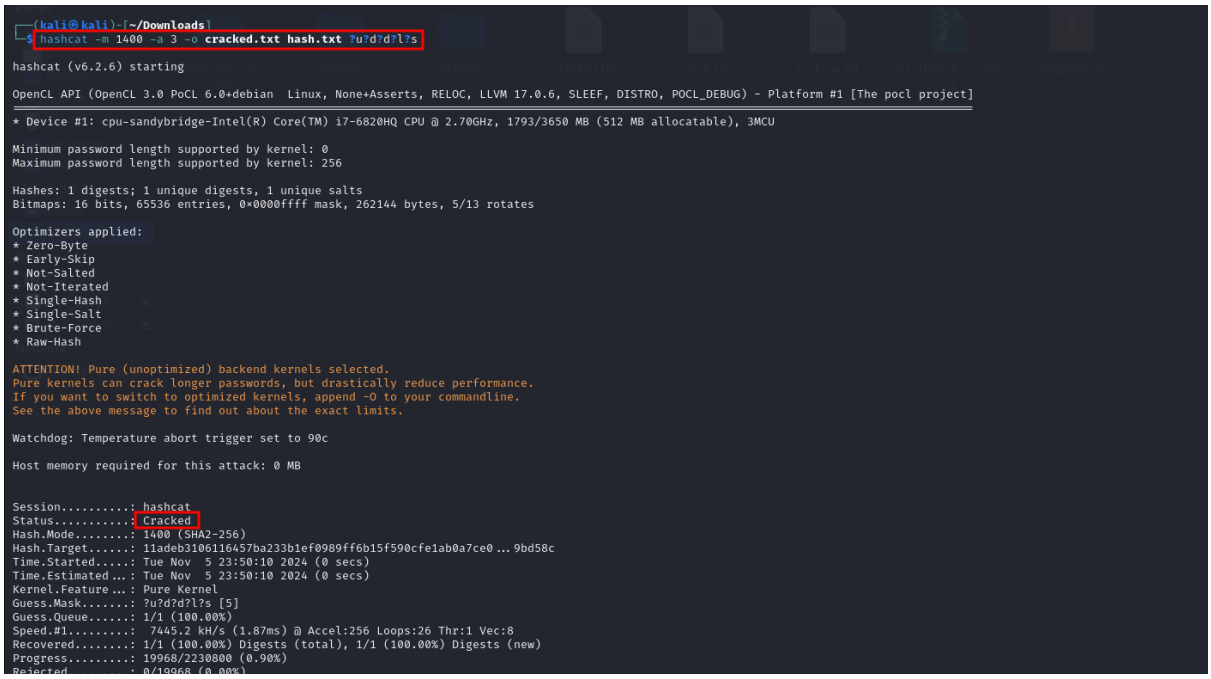


Password is: michael1997

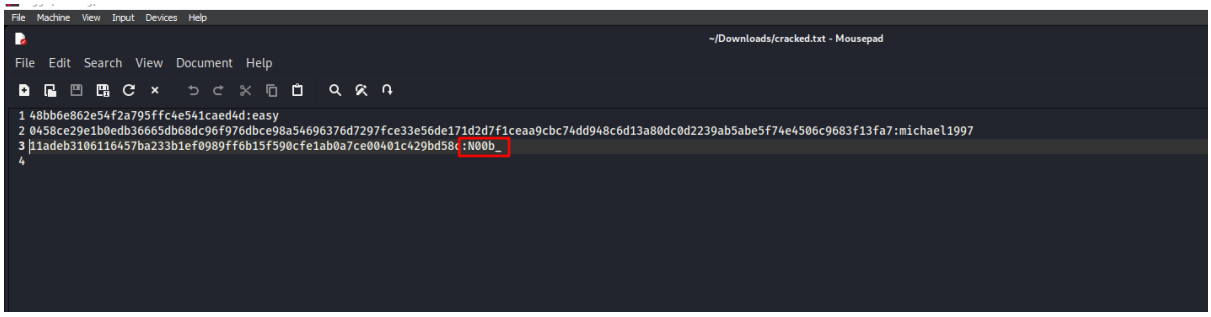


3. Hashid gave Snefru-256 which did not work so instead I used SHA-256 code 1400 in hashcat to crack the hash.

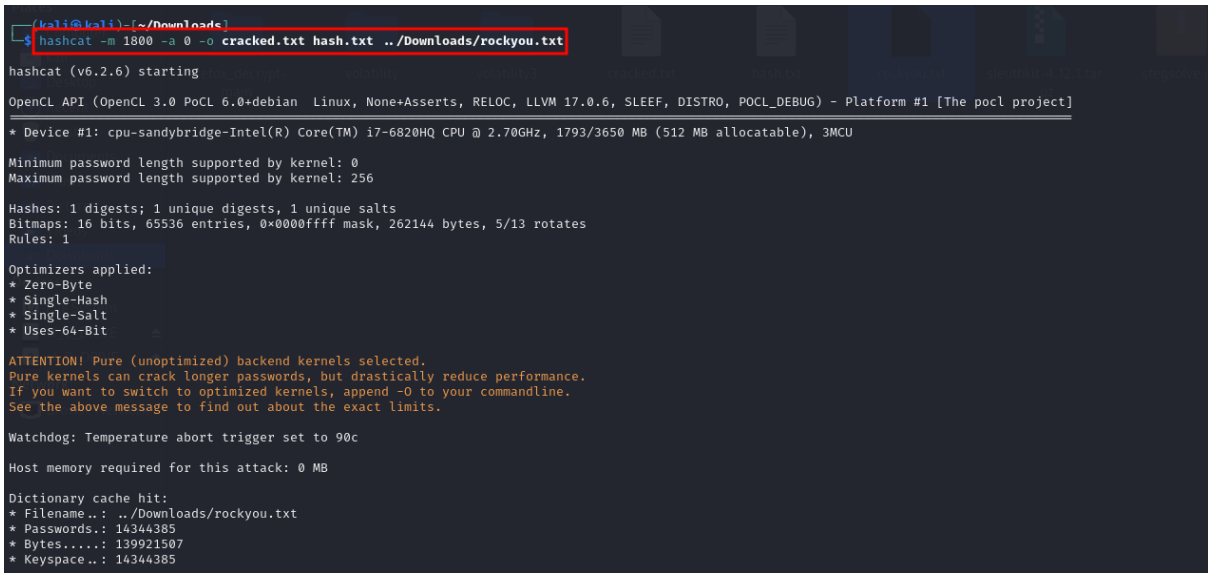


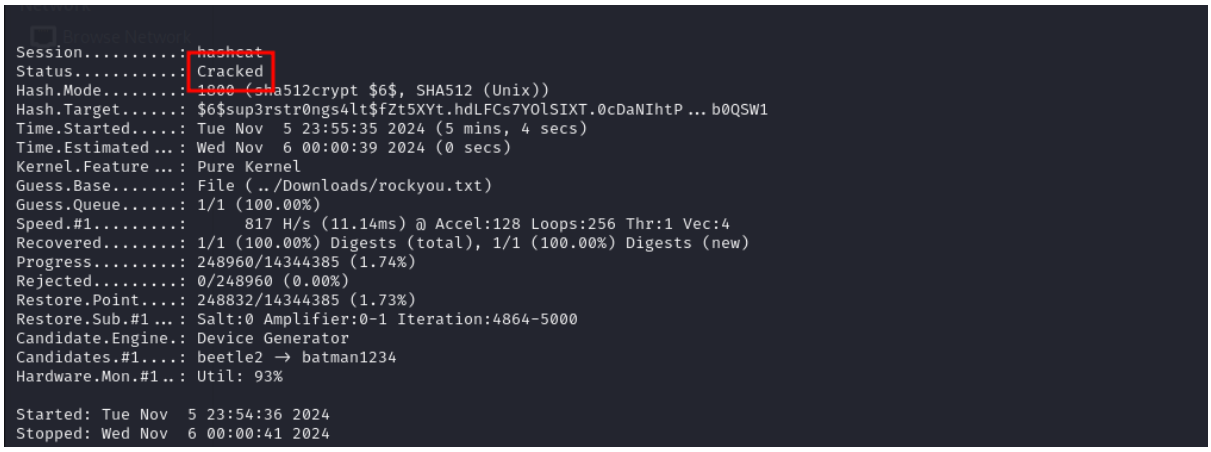


Password: N00b_



4. Hashid could not identify so I used GPT to see which type of hash has 6 at the beginning and it said SHA-512 and the number for that is 1800.





It takes about 4 minutes, and it cracked.