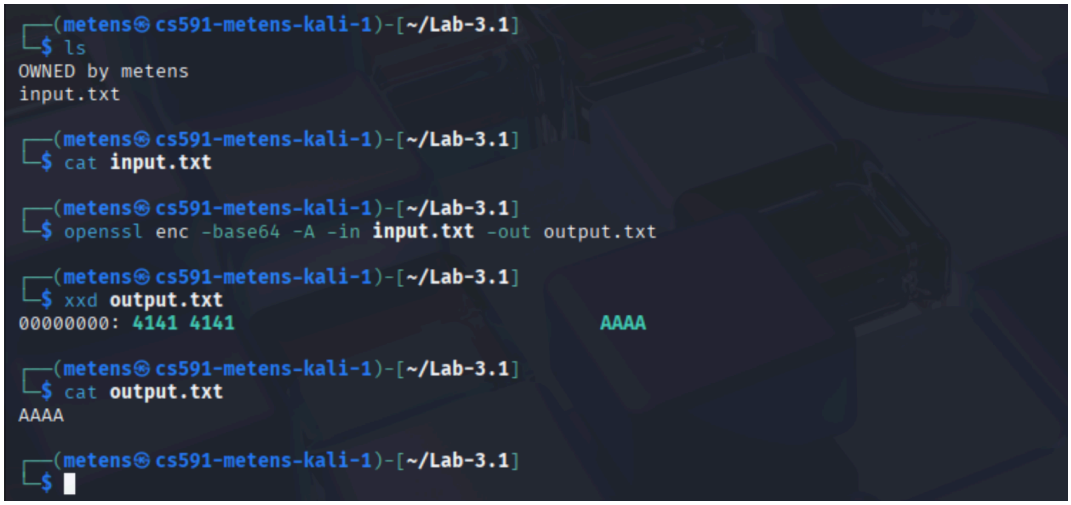
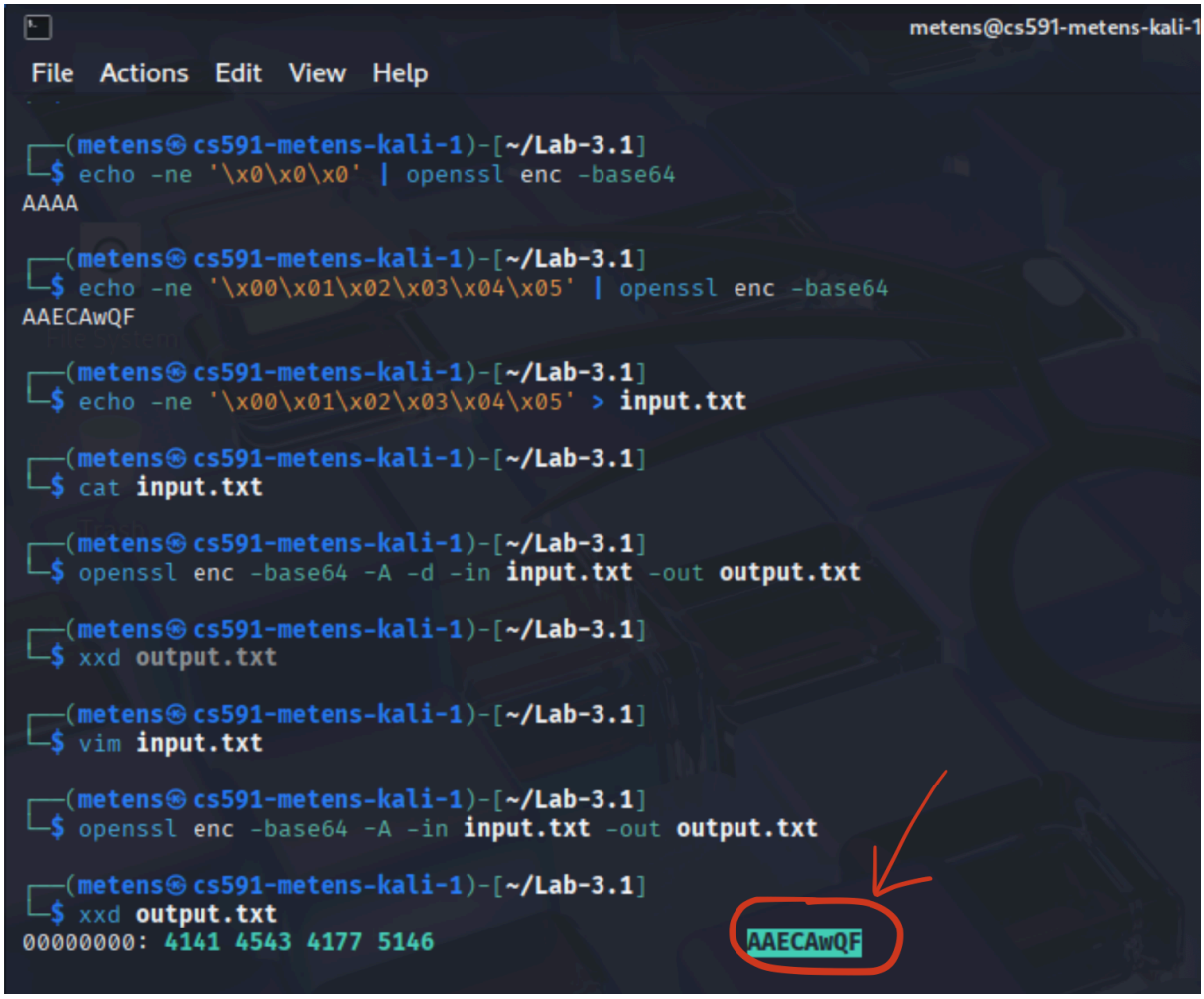
Lab 3.1

By: Nathan Metens (metens@pdx.edu)

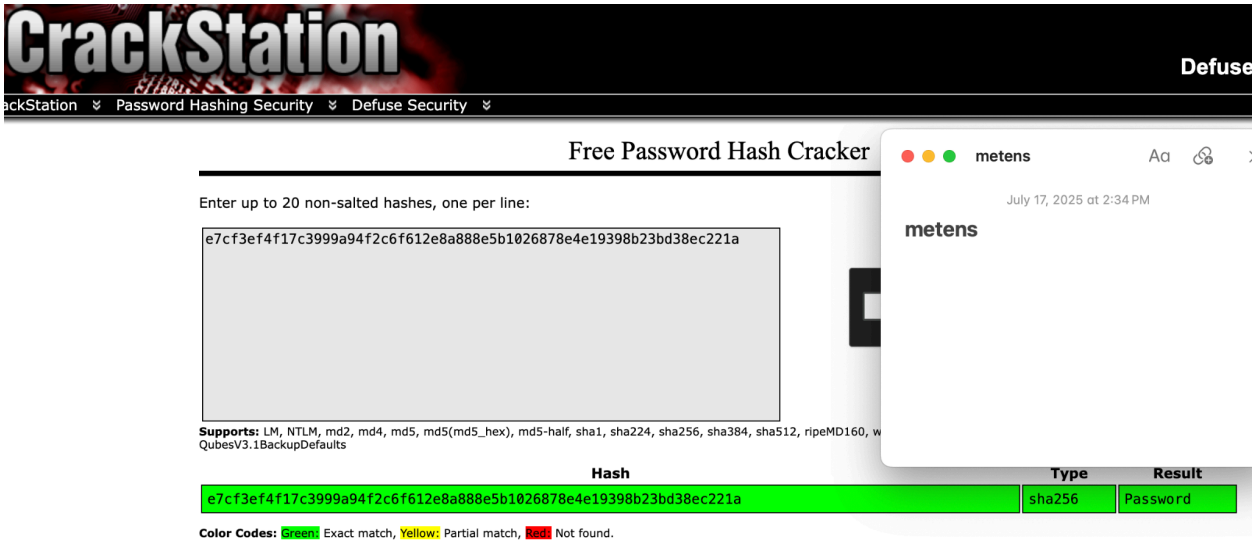
Task 1: Using Base64 and OpenSSL



```
┌──(metens㉿cs591-metens-kali-1)-[~/Lab-3.1]
└─$ openssl enc -base64 -A -d -in output.txt -out decode.txt; xxd decode.txt
00000000: 0000 00                                  ...
```

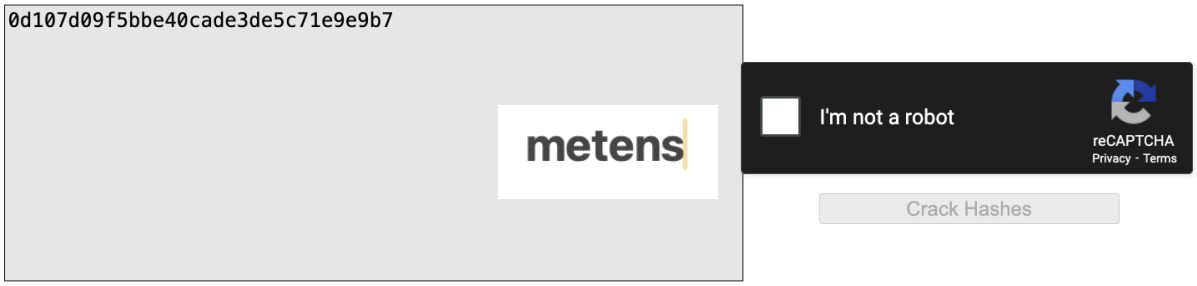


Task 2: Cryptographic hash functions



The most important properties of cryptographic hash functions are their pre-image resistance, collision resistance, and their ability to act as pseudo-random functions. In the case of https://crackstation.net/, the property being attacked is the pre-image resistance. The site stores passwords and their hashes, making it easy to find the output generated from the input. “CrackStation uses massive pre-computed lookup tables to crack password hashes. These tables store a mapping between the hash of a password and the correct password for that hash. The hash values are indexed so that it is possible to quickly search the database for a given hash.”

0d107d09f5bbe40cade3de5c71e9e9b7



Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(sha1_bin)), QubesV3.1BackupDefaults

Hash	Type	Result
0d107d09f5bbe40cade3de5c71e9e9b7	md5	letmein

Color Codes: Green: Exact match, Yellow: Partial match, Red: Not found.

cbfdac6008f9cab4083784cbd1874f76618d2a97

Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(sha1_bin)), QubesV3.1BackupDefaults

Hash	Type	Result
cbfdac6008f9cab4083784cbd1874f76618d2a97	sha1	password123

Color Codes: Green: Exact match, Yellow: Partial match, Red: Not found.

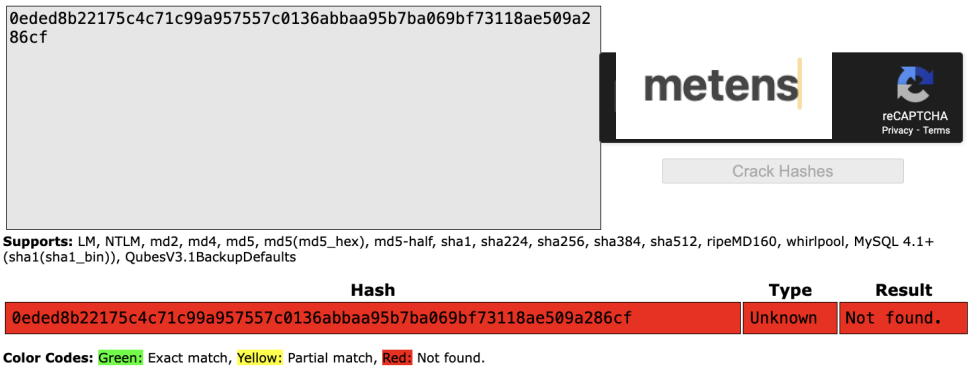
65e84be33532fb784c48129675f9eff3a682b27168c0ea744b2cf58ee02337c5

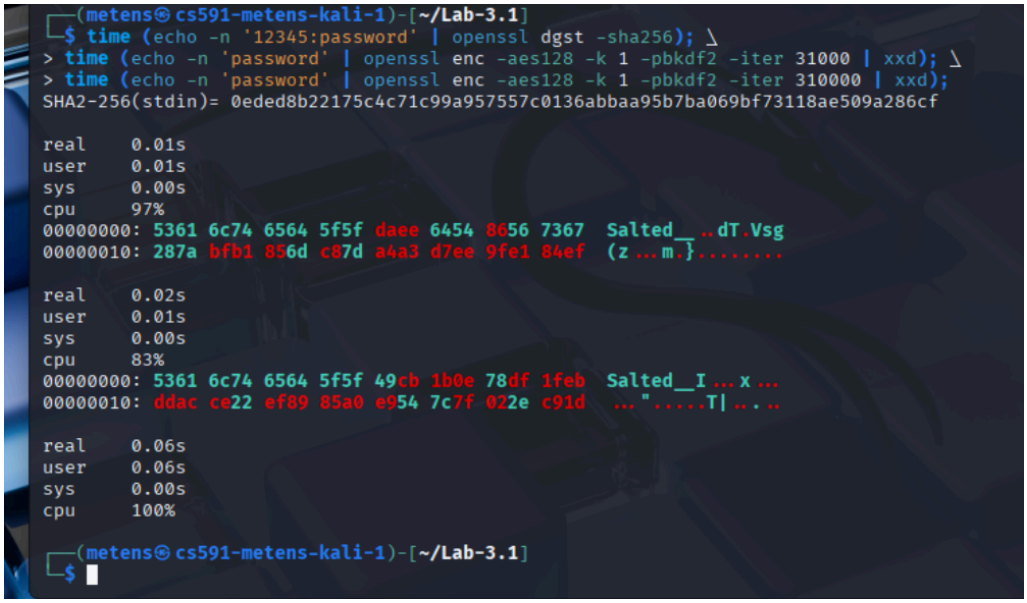
Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(sha1_bin)), QubesV3.1BackupDefaults

Hash	Type	Result
65e84be33532fb784c48129675f9eff3a682b27168c0ea744b2cf58ee02337c5	sha256	qwerty

Color Codes: Green: Exact match, Yellow: Partial match, Red: Not found.

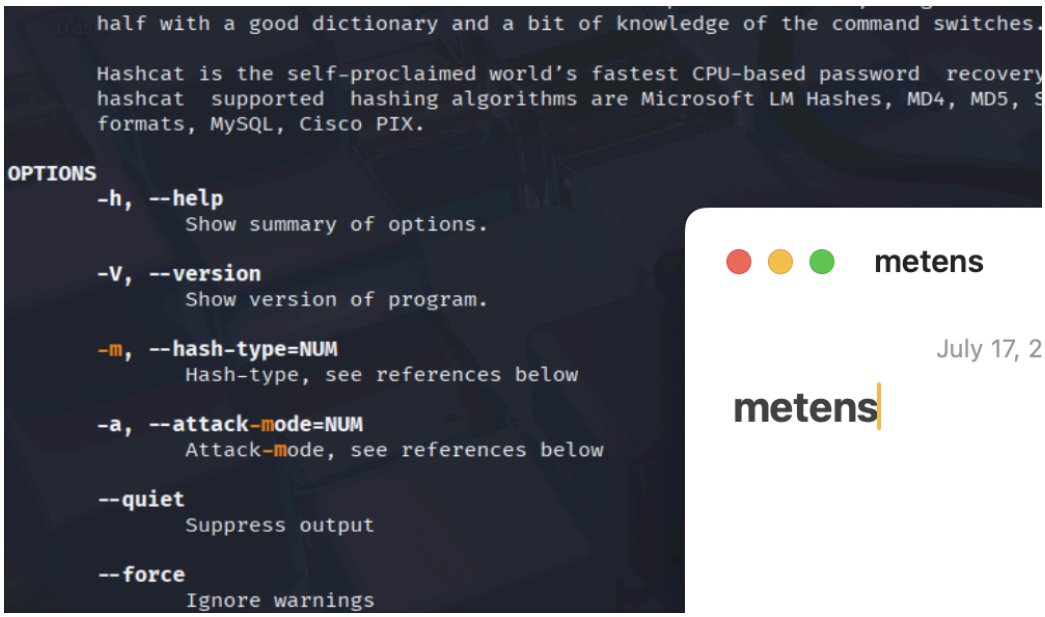
Task 3: Salt & Stretch

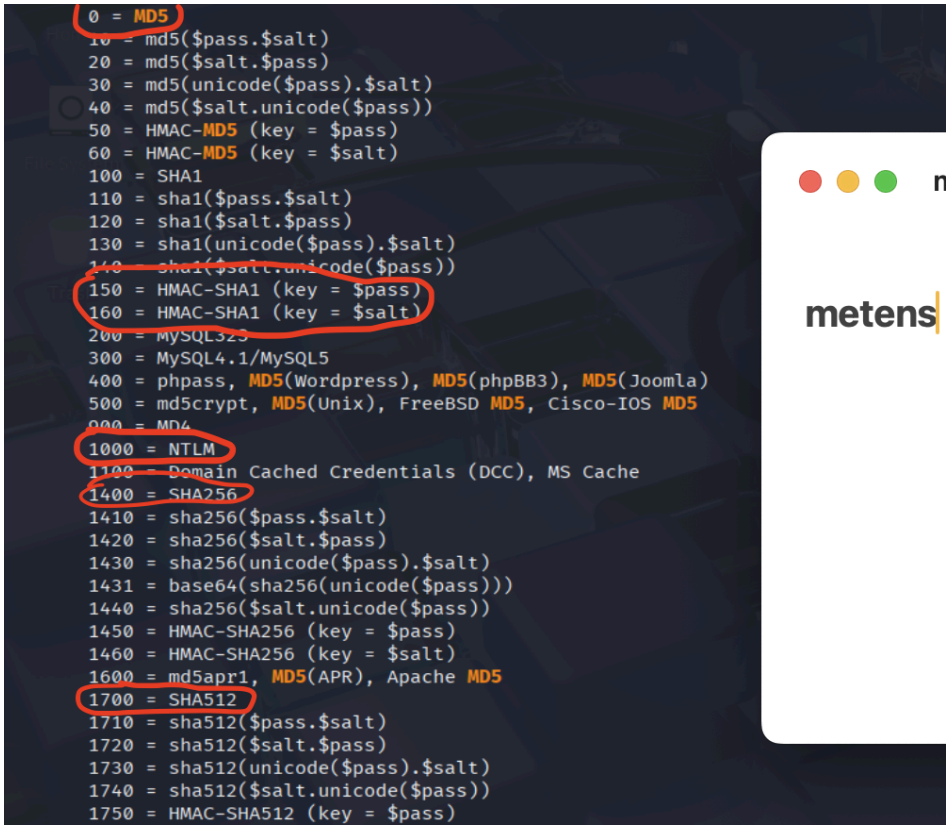




It appears as though the PBKDF with 31000 iterations is 2 times slower, and the PBKDF with 310000 iterations is 6 times slower compared to the SHA-256 hash.

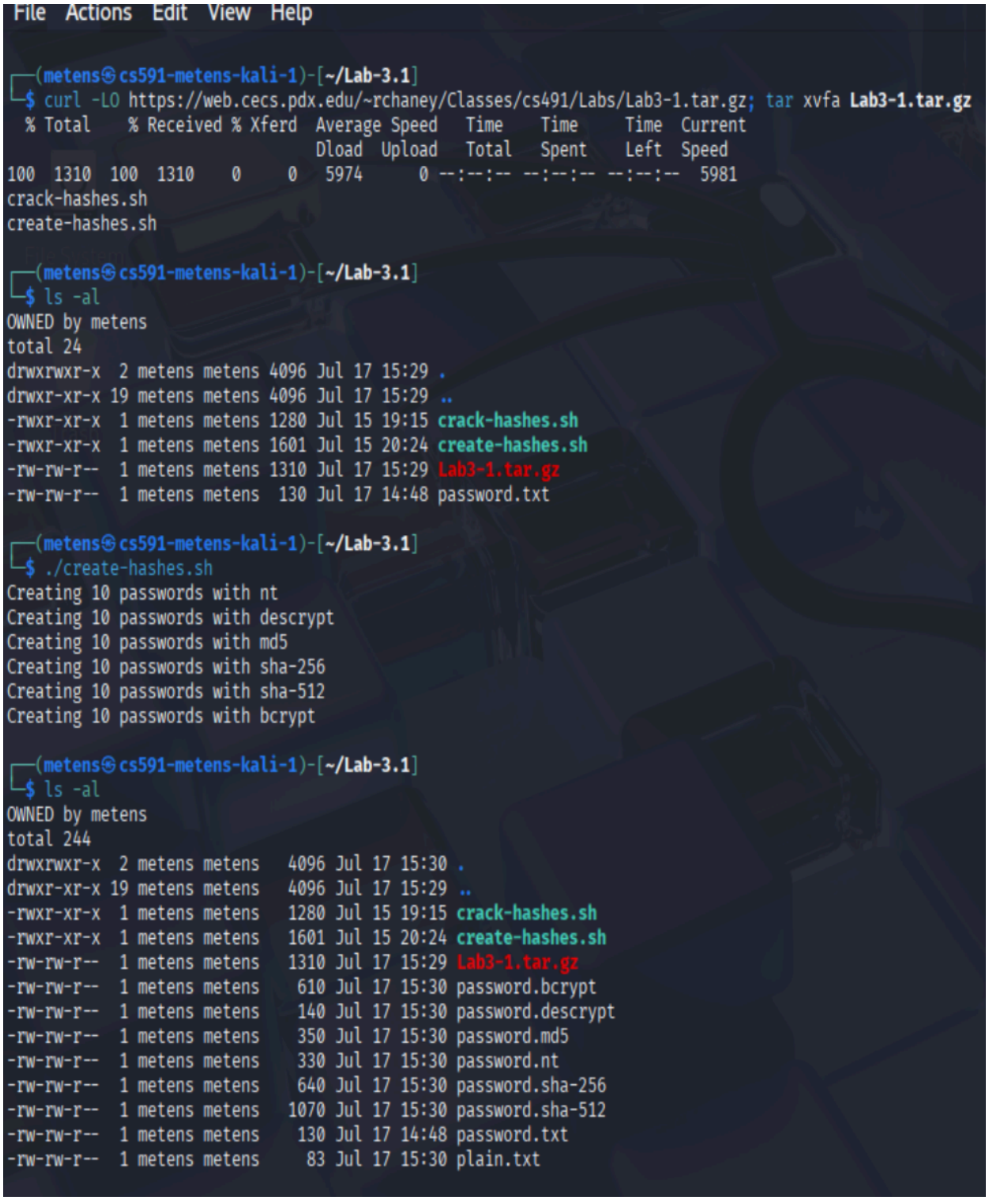
Task 4: Hash types

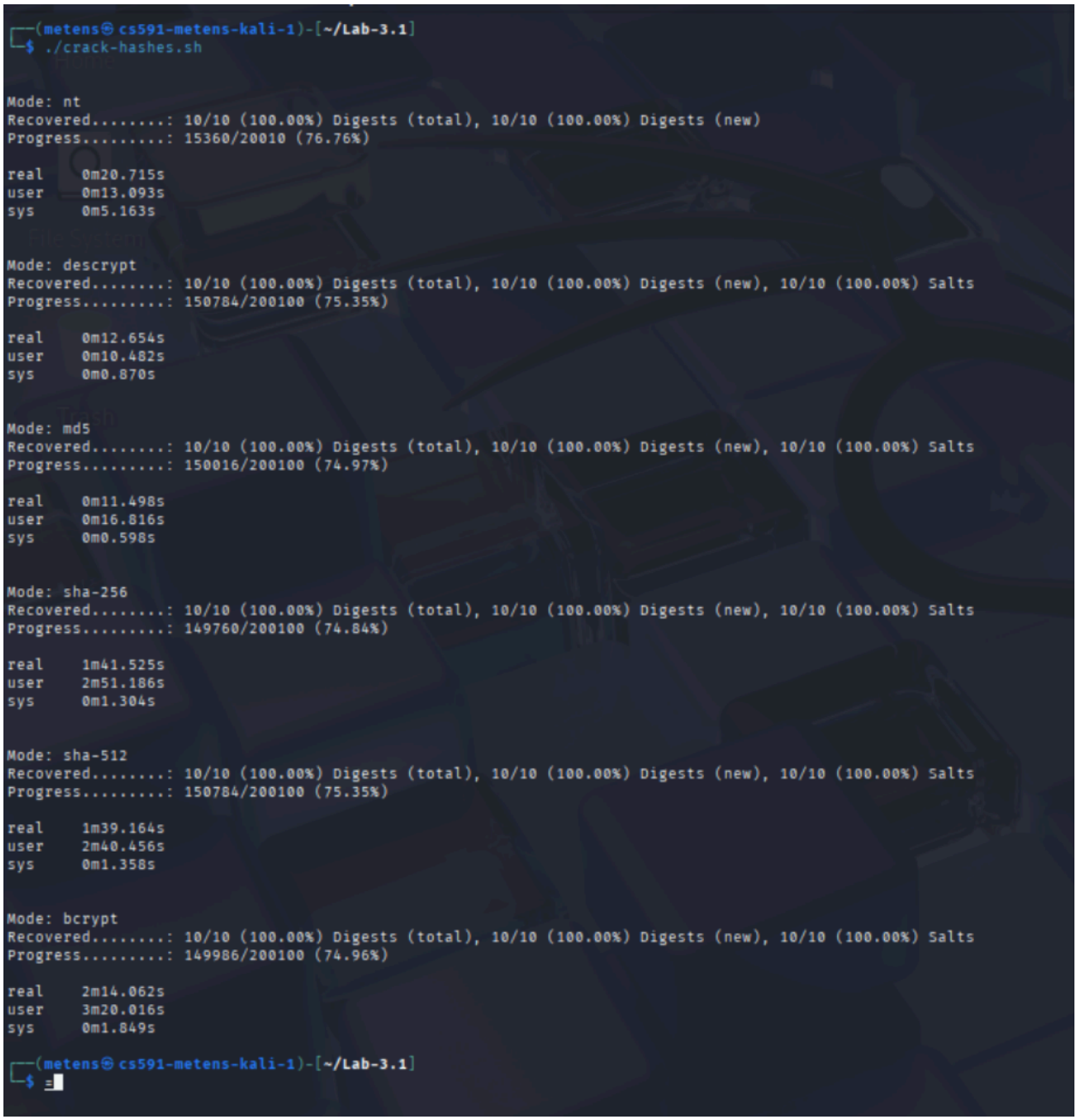




Hash Type numbers: MD5(0), HMAC-SHA1(150/160), NTLM(1000), SHA-256(1400), SHA-512(1700).

Task 5: Cracking passwords with hashcat





The quickest algorithm was MD5 and took about 11 seconds, while the slowest algorithm was BCRYPT which took nearly 2 minutes and 14 seconds.

Task 6: Cracking SSH passphrases

```
┌──(metens㉿cs591-metens-kali-1)-[~/Lab-3.1]
└─$ PASSWORD=$(head -n 500 wordlist.txt | tail -n 1); echo ${PASSWORD}
Derrikus5
```

```
└─$ ssh-keygen -t rsa -f ./id_rsa -b 1024 -N ${PASSWORD}
Generating public/private rsa key pair.
Your identification has been saved in ./id_rsa
Your public key has been saved in ./id_rsa.pub
The key fingerprint is:
SHA256:kNWEGMCgUyhptNjj1C1IwymGbbs+K+crrWjKfhXBRMk metens@cs591-metens-kali-1
The key's randomart image is:
+---[RSA 1024]----+
|o*=+*+oo.+.      |
|BB*+.E.o. .      |
|B+=.o =          |
| +.. o .         |
|  ..  . S        |
|  .  .           |
| o  .            |
|=.=.             |
|BO=+             |
+----[SHA256]-----+

┌──(metens㉿cs591-metens-kali-1)-[~/Lab-3.1]
└─$ ls
OWNED by metens
cracked.bcrypt    cracked.nt       crack-hashes.sh   id_rsa.pub       password.descrypt
cracked.descrypt  cracked.sha-256  create-hashes.sh  Lab3-1.tar.gz    password.md5
cracked.md5       cracked.sha-512  id_rsa            password.bcrypt  password.nt

┌──(metens㉿cs591-metens-kali-1)-[~/Lab-3.1]
└─$ ls | grep "id_rsa"
id_rsa
id_rsa.pub
```

```
┌──(metens㉿cs591-metens-kali-1)-[~/Lab-3.1]
└─$ python3 /usr/share/john/ssh2john.py ./id_rsa > id_rsa.hash

┌──(metens㉿cs591-metens-kali-1)-[~/Lab-3.1]
└─$ cat id_rsa.hash
./id_rsa:$sshng$6$16$81422b56c3678685f45ae2ffdb539896$758$6f70656e7373682d6b65792d7631000000000a6165733235362d637472000000066
263727970740000001800000001081422b56c3678685f45ae2ffdb53989600000018000000010000009700000007737368 2d727361000000030100010000008100c6f117cb1d78d9e7169f1e2536b90f6ff249aed97051614c983eef5f65f36fe04e5e4a1819189cb5213e4377f5c4bd9441577490d1e438503ea52bbb951399b14b8331018f067903b864a5b54c6a7788a47b1600b309dc1e9902bf7f895690f9cd12822ec6016bd896bc03aa9af5f0d7b6f2106d036d413809217de339ca275b00000021098186751e634d6d981d368dfaa5482af34922f90ccf20ffc19608cdfcea50f63cc8aeac854b761802ade51be33759e3b450bd926c1cdc202828d3086b3f76837d82f7aa79f06b6b9fb4c20144f6adbc79d1d00d9ce0caeb677f8fb2ba93767e7ac8c775044157372fb523f6e454b4f0c0169e73b13c1dcfff0c356d953304e5f0bc1ae87d15e03295c7655b10f19c163cc43063a3112ef03c747b83216dc22bd5ffa2057dfbd35f37eaee6833c7b0437e22a6947597c63029b6a9d653199f14e25d8d33be911352f36f36759e1cadfa995544055128420b35151cb757f8a96f6c648e9fe7c36f666e6de67622f70bcb0b5b4d2c87f094be4920e239ab5b1f892b5e900c5f961a162608f81f9fba8eb4da59f122d5753baf6f7225cc06ff9d486e057787f51799ad6ef2ee42c1f183661a61f5c665aeaf1a762c16959f573ccd16790a4530571784d0110253ca1312d0e4e5b869cd85c4befb7f85555915158537b1343eccf7fb88959ec1766ff9668a478d178585d7d97778f19bf31554cd9e28f2bc1aebeafab1cbd55a299a611621d3d3cdadde0c8057b3ee0fea5b3c33c8d08b8f64585745759fab0558f011d20d7676d889dfdd8b2c55cb6e6fafed7a5b87450a0c83a6900184fa33d4a1fc3d7f870a1163ff96401373685c7e5454c1cc3b457d991d83900c1329f72199487bbbe57606a9ba288ebb865206bdeb0dd21a3927633ee21603b0dfbaefca4037f1f06$24$230

┌──(metens㉿cs591-metens-kali-1)-[~/Lab-3.1]
└─$ time john --wordlist=wordlist.txt id_rsa.hash
Created directory: /home/metens/.john
Using default input encoding: UTF-8
Loaded 1 password hash (SSH, SSH private key [RSA/DSA/EC/OPENSSH 32/64])
Cost 1 (KDF/cipher [0=MD5/AES 1=MD5/3DES 2=Bcrypt/AES]) is 2 for all loaded hashes
Cost 2 (iteration count) is 24 for all loaded hashes
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:00:00:09 0.39% (ETA: 17:01:45) 0g/s 6.680p/s 6.680c/s 6.680C/s burri05..08998474260
0g 0:00:00:11 0.45% (ETA: 17:03:18) 0g/s 6.672p/s 6.672c/s 6.672C/s mar1103..romule93
0g 0:00:00:19 0.70% (ETA: 17:08:13) 0g/s 6.659p/s 6.659c/s 6.659C/s geonik..5buckshot
0g 0:00:00:53 1.80% (ETA: 17:11:55) 0g/s 6.620p/s 6.620c/s 6.620C/s chloe_1996..bazzle85
Derrikus5        (./id_rsa)
1g 0:00:01:17 DONE (2025-07-17 16:24) 0.01291g/s 6.614p/s 6.614c/s 6.614C/s hate boys for ever..rachelle!
Use the "--show" option to display all of the cracked passwords reliably
Session completed.

real    83.29s
user    151.36s
sys     0.36s
cpu     182%

┌──(metens㉿cs591-metens-kali-1)-[~/Lab-3.1]
└─$
```