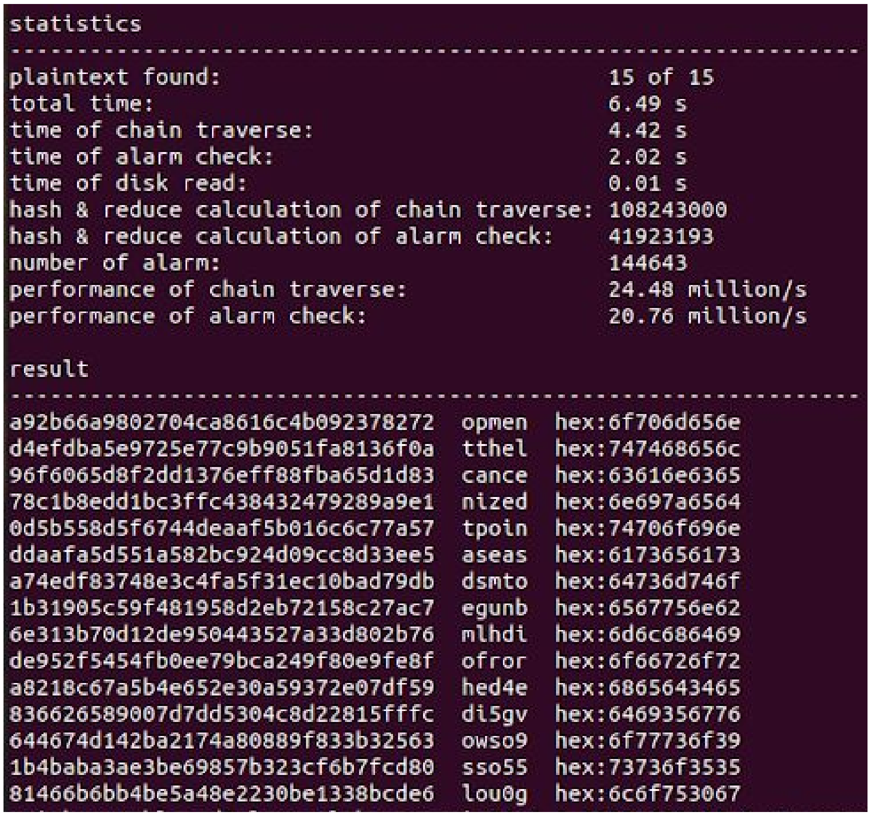
Lab 3

MD5 and Rainbow Tables

5 Salting

For both salted and unsalted passwords, we made use of RainbowCrack to crack the passwords. RainbowCrack uses rainbow tables to crack hashes.

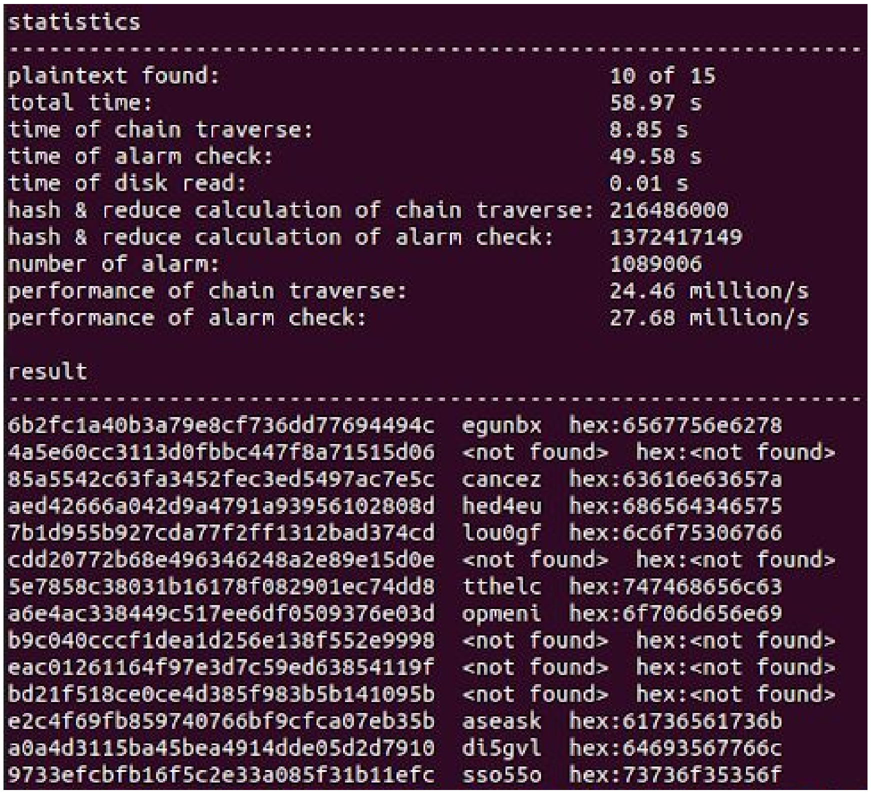
For unsalted passwords, it takes 6.49s in total to crack all 15 passwords, while for salted passwords, it takes 58.97s in total to crack only 10 out of 15 passwords.



```
statistics
----------------------------------------------------------------
plaintext found:                             15 of 15
total time:                                  6.49 s
time of chain traverse:                      4.42 s
time of alarm check:                         2.02 s
time of disk read:                           0.01 s
hash & reduce calculation of chain traverse: 108243000
hash & reduce calculation of alarm check:    41923193
number of alarm:                             144643
performance of chain traverse:               24.48 million/s
performance of alarm check:                  20.76 million/s

result
----------------------------------------------------------------
a92b66a9802704ca8616c4b092378272  opmen  hex:6f706d656e
d4efdba5e9725e77c9b9051fa8136f0a  tthel  hex:747468656c
96f6065d8f2dd1376eff88fba65d1d83  cance  hex:63616e6365
78c1b8edd1bc3ffc438432479289a9e1  nized  hex:6e697a6564
0d5b558d5f6744deaaf5b016c6c77a57  tpoin  hex:74706f696e
ddaafa5d551a582bc924d09cc8d33ee5  aseas  hex:6173656173
a74edf83748e3c4fa5f31ec10bad79db  dsmto  hex:64736d746f
1b31905c59f481958d2eb72158c27ac7  egunb  hex:6567756e62
6e313b70d12de950443527a33d802b76  mlhdi  hex:6d6c686469
de952f5454fb0ee79bca249f80e9fe8f  ofror  hex:6f66726f72
a8218c67a5b4e652e30a59372e07df59  hed4e  hex:6865643465
836626589007d7dd5304c8d22815fffc  di5gv  hex:6469356776
644674d142ba2174a80889f833b32563  owso9  hex:6f77736f39
1b4baba3ae3be69857b323cf6b7fcd80  sso55  hex:73736f3535
81466b6bb4be5a48e2230be1338bcde6  lou0g  hex:6c6f753067
```

Fig 1: Statistics for Cracking Unsalted Passwords



```
statistics
--------------------------------------------------------------
plaintext found:                             10 of 15
total time:                                  58.97 s
time of chain traverse:                      8.85 s
time of alarm check:                         49.58 s
time of disk read:                           0.01 s
hash & reduce calculation of chain traverse: 216486000
hash & reduce calculation of alarm check:    1372417149
number of alarm:                             1089006
performance of chain traverse:               24.46 million/s
performance of alarm check:                  27.68 million/s

result
--------------------------------------------------------------
6b2fc1a40b3a79e8cf736dd77694494c  egunbx  hex:6567756e6278
4a5e60cc3113d0fbbc447f8a71515d06  <not found>  hex:<not found>
85a5542c63fa3452fec3ed5497ac7e5c  cancez  hex:63616e63657a
aed42666a042d9a4791a93956102808d  hed4eu  hex:686564346575
7b1d955b927cda77f2ff1312bad374cd  lou0gf  hex:6c6f75306766
cdd20772b68e496346248a2e89e15d0e  <not found>  hex:<not found>
5e7858c38031b16178f082901ec74dd8  tthelc  hex:747468656c63
a6e4ac338449c517ee6df0509376e03d  opmeni  hex:6f706d656e69
b9c040cccf1dea1d256e138f552e9998  <not found>  hex:<not found>
eac01261164f97e3d7c59ed63854119f  <not found>  hex:<not found>
bd21f518ce0ce4d385f983b5b141095b  <not found>  hex:<not found>
e2c4f69fb859740766bf9cfca07eb35b  aseask  hex:61736561736b
a0a4d3115ba45bea4914dde05d2d7910  di5gvl  hex:64693567766c
9733efcbfb16f5c2e33a085f31b11efc  sso55o  hex:73736f35356f
```

Fig 2: Statistics for Cracking Salted Passwords

As the rainbow table's charset is loweralpha-numeric, addition of 1 character as salt means that there are 36^6 = 2,176,782,336 more possible guesses compared to the unsalted password of length 5.

In the rainbow table, although the unsalted passwords were identified to be more common and can be easily cracked by the table, the addition of the salt meant completely different hashes, and guessed would need to be recomputed again, even when there are repeat passwords. Out of these 15 salted passwords, we can then see that only 10 of them are common enough to be stored in the rainbow table to be looked up easily and cracked.

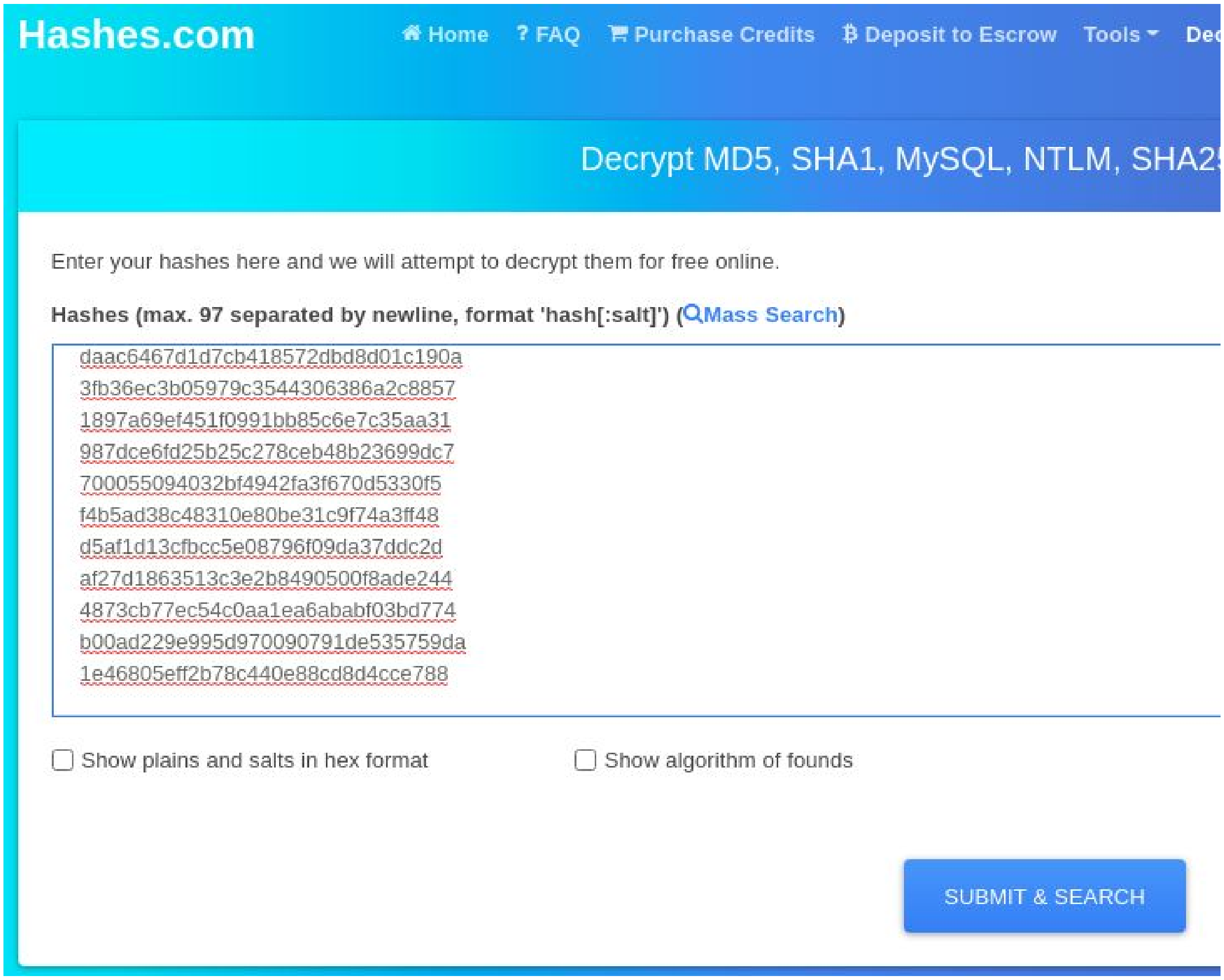
6 Hash breaking competition

To crack the hashes, I made use of hashes.com to crack the hashes.

Hashes.com does not crack the hashes in real-time, but instead is a lookup service which searches its own database, with MD5 hashes among others, of already cracked hashes to find a possible password for collision. It indexes hashes to plaintext to allow for searching. While this is very space consuming, it is almost instantaneous in time.

This database was started in August 2007, and the hashes cracked over the years by enthusiasts have been cached.

The website has a User Interface (UI) through which we can search through the database. In the home page, we can input the hashes into the input box as shown below. Due to the limit, we have to split the hashes to be entered in 2 batches.



Enter your hashes here and we will attempt to decrypt them for free online.

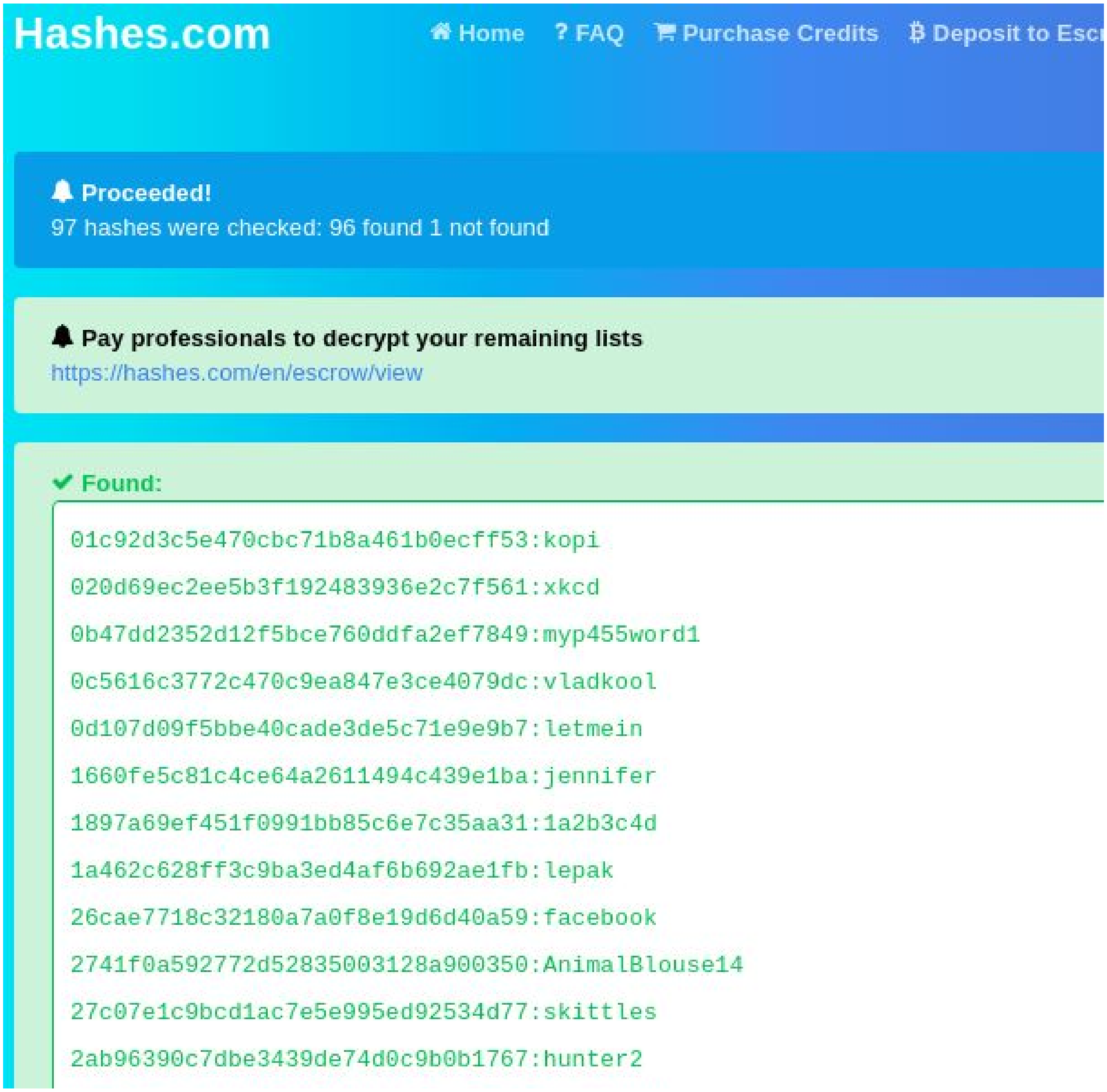
Hashes (max. 97 separated by newline, format 'hash[:salt]') (Mass Search)

```
daac6467d1d7cb418572dbd8d01c190a
3fb36ec3b05979c3544306386a2c8857
1897a69ef451f0991bb85c6e7c35aa31
987dce6fd25b25c278ceb48b23699dc7
700055094032bf4942fa3f670d5330f5
f4b5ad38c48310e80be31c9f74a3ff48
d5af1d13cfbcc5e08796f09da37ddc2d
af27d1863513c3e2b8490500f8ade244
4873cb77ec54c0aa1ea6ababf03bd774
b00ad229e995d970090791de535759da
1e46805eff2b78c440e88cd8d4cce788
```

☐ Show plains and salts in hex format ☐ Show algorithm of founds

Fig 3: Hashes.com input box for hashes

After the hashes are entered, click the “SUBMIT & SEARCH” button. The hashes’ corresponding plaintexts would then be searched through the database, and the results would be displayed, as shown below.



Proceeded!
97 hashes were checked: 96 found 1 not found

Pay professionals to decrypt your remaining lists
https://hashes.com/en/escrow/view

✓ **Found:**

```
01c92d3c5e470cbc71b8a461b0ecff53:kopi
020d69ec2ee5b3f192483936e2c7f561:xkcd
0b47dd2352d12f5bce760ddfa2ef7849:myp455word1
0c5616c3772c470c9ea847e3ce4079dc:vladkool
0d107d09f5bbe40cade3de5c71e9e9b7:letmein
1660fe5c81c4ce64a2611494c439e1ba:jennifer
1897a69ef451f0991bb85c6e7c35aa31:1a2b3c4d
1a462c628ff3c9ba3ed4af6b692ae1fb:lepak
26cae7718c32180a7a0f8e19d6d40a59:facebook
2741f0a592772d52835003128a900350:AnimalBlouse14
27c07e1c9bcd1ac7e5e995ed92534d77:skittles
2ab96390c7dbe3439de74d0c9b0b1767:hunter2
```

Fig 4: Results from hashes.com Hash Lookup

Hashes.com is also able to identify the type of MD5 encryption done on the plain texts, such as if it is a standard MD5 encryption, MD5PLAIN, or MD5X2.

Repeat the process until collisions to all hashes have been found.

Although most passwords can be cracked by hashes.com (145 out of 148), there are 3 which could not be cracked, namely:

- 4698e7ab9c06649f06f3bbc8fcb20360
- daac6467d1d7cb418572dbd8d01c190a
- d768d3b271ba9faaab0141600a47b221

To crack these, I tried to use hashcat as well, with the help of common password lists found here.

Unfortunately, I did not manage to crack the passwords with the help of these.

How hashcat works is that it takes in password lists and hashes them based on the mode, which in our case is MD5. After hashing them, the password hashes are compared to the hashes provided, and if there is a collision, it would show up. This is known as a dictionary attack.

I tried the dictionary attack with the following password lists:

- Rockyou
- John the Ripper
- Cain & Abel
- 500 worst passwords
- 370 Banned Twitter
- English words
- Fuzzing strings
- Hotmail
- Facebook Full names

Other than the dictionary attack, hashcat has other attack modes as well, such as combinator attack, mask attack, rule-based attack and brute force attack.