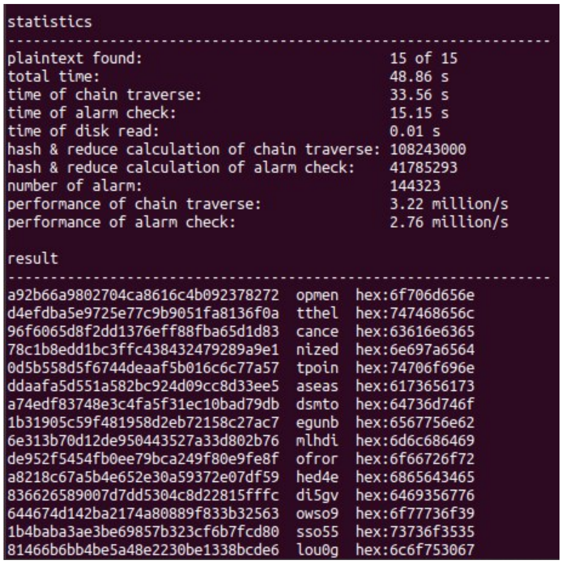
**Summary Table:**

| **No. of characters** | **Five-character** | | **Six-character** | |
|---|---|---|---|---|
| **Method** | **Brute force** | **Rainbow table** | | |
| | | **Chain length:** 3800<br>**Chain number:** 600000 | | **Chain length:** 7600<br>**Chain number:** 2000000 |
| **Time in s (2d.p.)** | 387.27 | 48.86 | 366.31* | 132.64** |

*9 out of 15 hashes broken

**14 out of 15 hashes broken

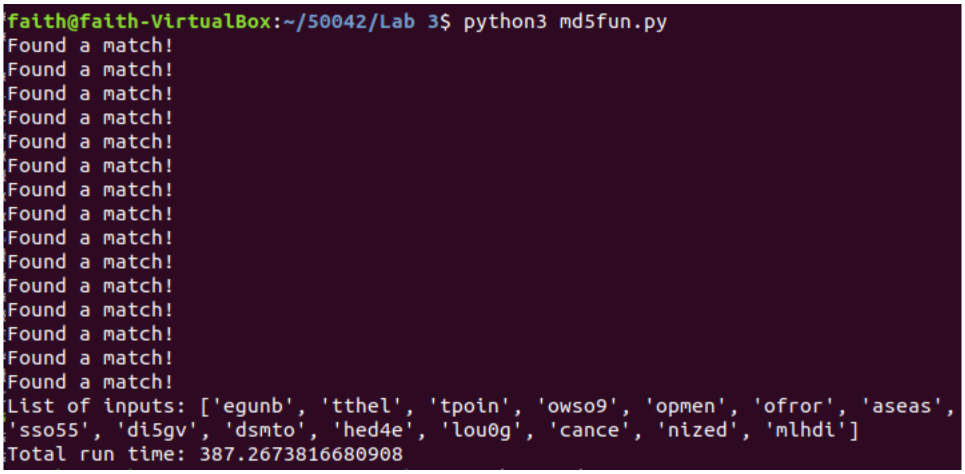
**Using rainbow table for five-character input:**



```
statistics
-------------------------------------------------------------------
plaintext found:                              15 of 15
total time:                                   48.86 s
time of chain traverse:                       33.56 s
time of alarm check:                          15.15 s
time of disk read:                            0.01 s
hash & reduce calculation of chain traverse: 108243000
hash & reduce calculation of alarm check:    41785293
number of alarm:                              144323
performance of chain traverse:                3.22 million/s
performance of alarm check:                   2.76 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
```

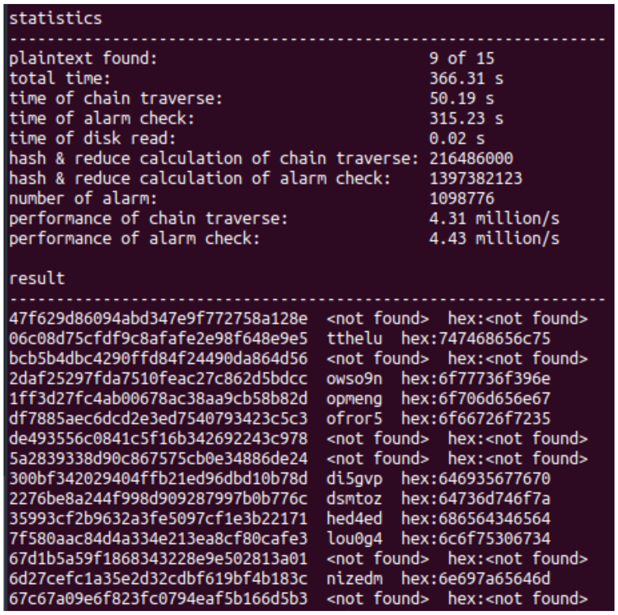
As compared to the brute forcing which took almost 8 times longer, we can see that using rainbow table to break hashes is much more efficient.



```
faith@faith-VirtualBox:~/50042/Lab 3$ python3 md5fun.py
Found a match!
Found a match!
Found a match!
Found a match!
Found a match!
Found a match!
Found a match!
Found a match!
Found a match!
Found a match!
Found a match!
Found a match!
Found a match!
Found a match!
Found a match!
List of inputs: ['egunb', 'tthel', 'tpoin', 'owso9', 'opmen', 'ofror', 'aseas',
'sso55', 'di5gv', 'dsmto', 'hed4e', 'lou0g', 'cance', 'nized', 'mlhdi']
Total run time: 387.2673816680908
```

### Using rainbow table for six-character input: (Salted hashes)

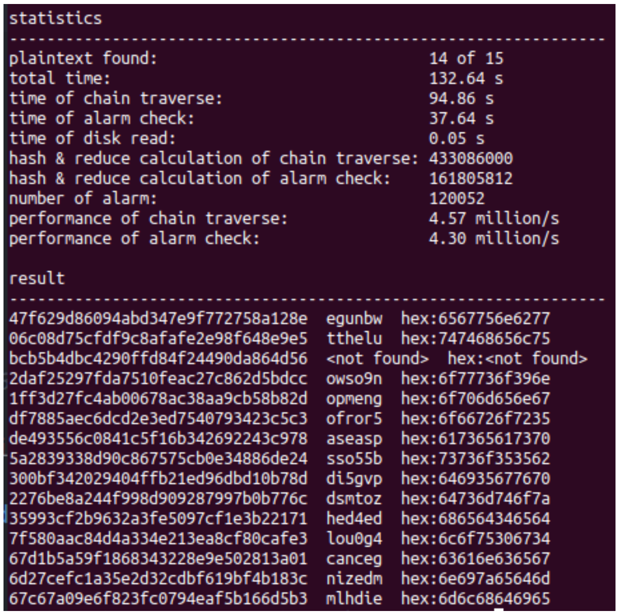
By increasing the length of the password by 1, the input space is now $36^6$ instead of $36^5$. Without increasing the chain length and chain number, not all the salted hashes can be broken as only 9 out of 15 can be broken.



```
statistics
--------------------------------------------------------------
plaintext found:                             9 of 15
total time:                                  366.31 s
time of chain traverse:                      50.19 s
time of alarm check:                         315.23 s
time of disk read:                           0.02 s
hash & reduce calculation of chain traverse: 216486000
hash & reduce calculation of alarm check:    1397382123
number of alarm:                             1098776
performance of chain traverse:               4.31 million/s
performance of alarm check:                  4.43 million/s

result
--------------------------------------------------------------
47f629d86094abd347e9f772758a128e  <not found>  hex:<not found>
06c08d75cfdf9c8afafe2e98f648e9e5  tthelu  hex:747468656c75
bcb5b4dbc4290ffd84f24490da864d56  <not found>  hex:<not found>
2daf25297fda7510feac27c862d5bdcc  owso9n  hex:6f77736f396e
1ff3d27fc4ab00678ac38aa9cb58b82d  opmeng  hex:6f706d656e67
df7885aec6dcd2e3ed7540793423c5c3  ofror5  hex:6f66726f7235
de493556c0841c5f16b342692243c978  <not found>  hex:<not found>
5a2839338d90c867575cb0e34886de24  <not found>  hex:<not found>
300bf342029404ffb21ed96dbd10b78d  di5gvp  hex:646935677670
2276be8a244f998d909287997b0b776c  dsmtoz  hex:64736d746f7a
35993cf2b9632a3fe5097cf1e3b22171  hed4ed  hex:686564346564
7f580aac84d4a334e213ea8cf80cafe3  lou0g4  hex:6c6f75306734
67d1b5a59f1868343228e9e502813a01  <not found>  hex:<not found>
6d27cefc1a35e2d32cdbf619bf4b183c  nizedm  hex:6e697a65646d
67c67a09e6f823fc0794eaf5b166d5b3  <not found>  hex:<not found>
```

Even after increasing the chain length to 7600 and the chain number to 2000000, only 14 out of 15 hashes could be broken. The increase in input space, chain length and chain number also means that the size of the rainbow table is significantly larger.  We can see that the time required to crack the passwords is higher along with a larger rainbow table with a six-character input.



```
statistics
--------------------------------------------------------------
plaintext found:                             14 of 15
total time:                                  132.64 s
time of chain traverse:                      94.86 s
time of alarm check:                         37.64 s
time of disk read:                           0.05 s
hash & reduce calculation of chain traverse: 433086000
hash & reduce calculation of alarm check:    161805812
number of alarm:                             120052
performance of chain traverse:               4.57 million/s
performance of alarm check:                  4.30 million/s

result
--------------------------------------------------------------
47f629d86094abd347e9f772758a128e  egunbw  hex:6567756e6277
06c08d75cfdf9c8afafe2e98f648e9e5  tthelu  hex:747468656c75
bcb5b4dbc4290ffd84f24490da864d56  <not found>  hex:<not found>
2daf25297fda7510feac27c862d5bdcc  owso9n  hex:6f77736f396e
1ff3d27fc4ab00678ac38aa9cb58b82d  opmeng  hex:6f706d656e67
df7885aec6dcd2e3ed7540793423c5c3  ofror5  hex:6f66726f7235
de493556c0841c5f16b342692243c978  aseasp  hex:617365617370
5a2839338d90c867575cb0e34886de24  sso55b  hex:73736f353562
300bf342029404ffb21ed96dbd10b78d  di5gvp  hex:646935677670
2276be8a244f998d909287997b0b776c  dsmtoz  hex:64736d746f7a
35993cf2b9632a3fe5097cf1e3b22171  hed4ed  hex:686564346564
7f580aac84d4a334e213ea8cf80cafe3  lou0g4  hex:6c6f75306734
67d1b5a59f1868343228e9e502813a01  canceg  hex:63616e636567
6d27cefc1a35e2d32cdbf619bf4b183c  nizedm  hex:6e697a65646d
67c67a09e6f823fc0794eaf5b166d5b3  mlhdie  hex:6d6c68646965
```

Using the online hash lookup service, https://hashkiller.co.uk/Cracker/MD5, I was able to crack all except 4 of the moderate hashes given. The md5 hash of the password and the corresponding plain text password is available in the attached *"part6.csv"*.