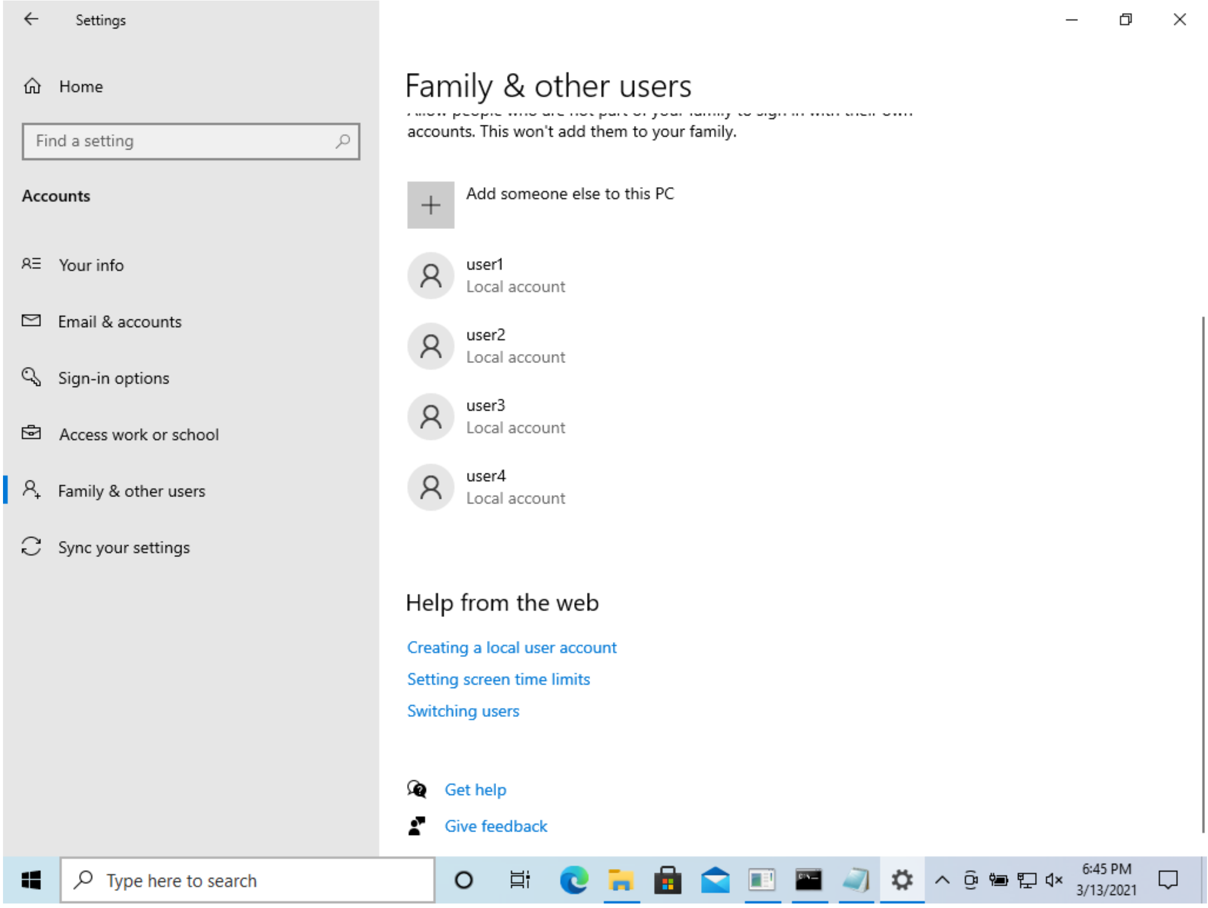
CIS4204.01 **Brandon Thompson**

Dr. Ashokkumar Patel Due: 3/13/21

Lab Homework 5: Offline Password Cracking

In this lab we will be doing an offline password attack using a rainbow table. Passwords are gathered from a Windows 10 VM using PwDump v8.2

First we create new user accounts with simple passwords.



Settings

Home

Find a setting

Accounts

Your info

Email & accounts

Sign-in options

Access work or school

Family & other users

Sync your settings

Family & other users

Allow people who are not part of your family to sign in with their own accounts. This won't add them to your family.

Add someone else to this PC

user1
Local account

user2
Local account

user3
Local account

user4
Local account

Help from the web

Creating a local user account

Setting screen time limits

Switching users

Get help

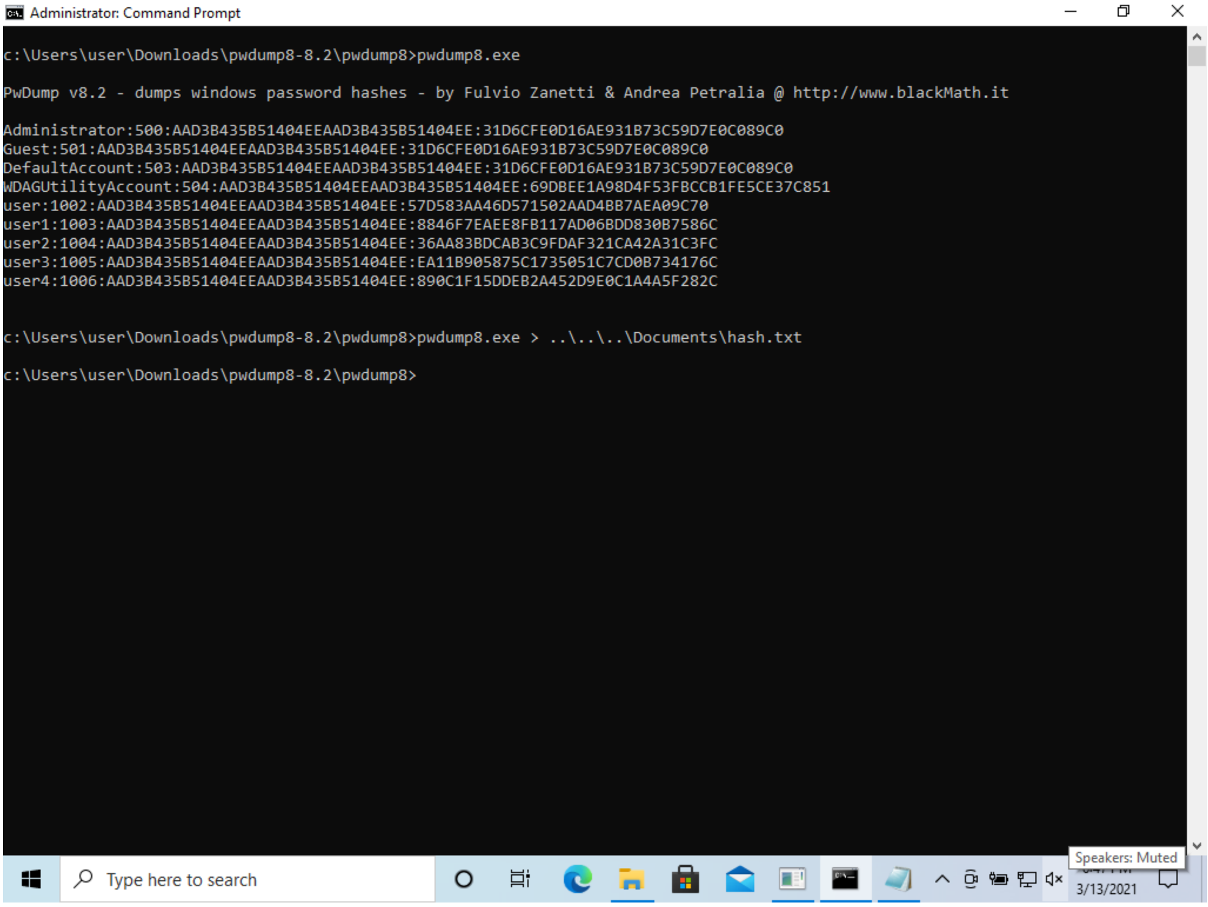
Give feedback

Type here to search

6:45 PM
3/13/2021

Figure 1: List of users whose passwords will be cracked.

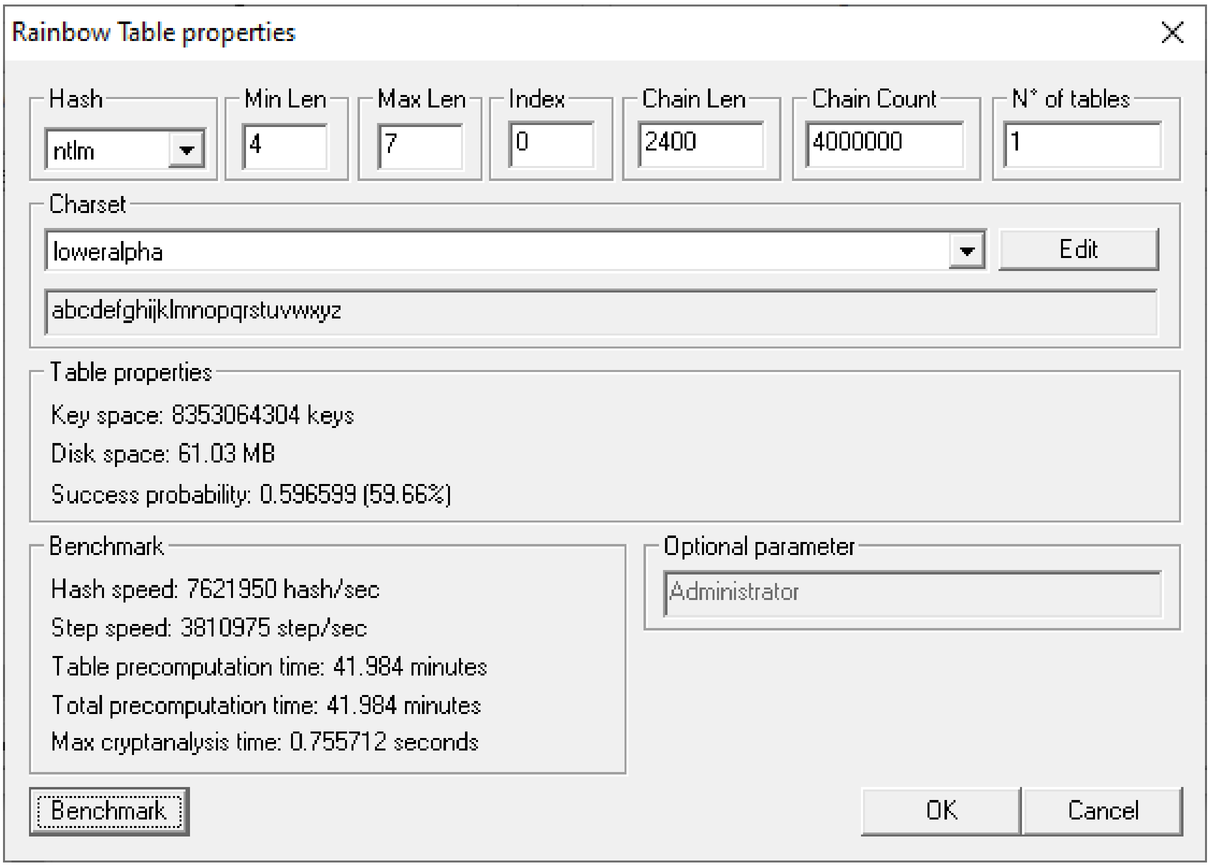
Next we install and run PwDump to retrieve the passwords hashes from the system files.



```
c:\Users\user\Downloads\pwdump8-8.2\pwdump8>pwdump8.exe

PwDump v8.2 - dumps windows password hashes - by Fulvio Zanetti & Andrea Petralia @ http://www.blackMath.it

Administrator:500:AAD3B435B51404EEAAD3B435B51404EE:31D6CFE0D16AE931B73C59D7E0C089C0
Guest:501:AAD3B435B51404EEAAD3B435B51404EE:31D6CFE0D16AE931B73C59D7E0C089C0
DefaultAccount:503:AAD3B435B51404EEAAD3B435B51404EE:31D6CFE0D16AE931B73C59D7E0C089C0
WDAGUtilityAccount:504:AAD3B435B51404EEAAD3B435B51404EE:69DBEE1A98D4F53FBCCB1FE5CE37C851
user:1002:AAD3B435B51404EEAAD3B435B51404EE:57D583AA46D571502AAD4BB7AEA09C70
user1:1003:AAD3B435B51404EEAAD3B435B51404EE:8846F7EAEE8FB117AD06BDD830B7586C
user2:1004:AAD3B435B51404EEAAD3B435B51404EE:36AA83BDCAB3C9FDAF321CA42A31C3FC
user3:1005:AAD3B435B51404EEAAD3B435B51404EE:EA11B905875C1735051C7CD0B734176C
user4:1006:AAD3B435B51404EEAAD3B435B51404EE:890C1F15DDEB2A452D9E0C1A4A5F282C


c:\Users\user\Downloads\pwdump8-8.2\pwdump8>pwdump8.exe > ..\..\..\Documents\hash.txt

c:\Users\user\Downloads\pwdump8-8.2\pwdump8>
```

Figure 2: List of all users on the machine and their associated password hashes.

Now we generate a rainbow table to match the possible passwords.



Rainbow Table properties

Hash: ntlm

Min Len: 4

Max Len: 7

Index: 0

Chain Len: 2400

Chain Count: 4000000

N° of tables: 1

Charset: loweralpha

abcdefghijklmnopqrstuvwxyz

Table properties

Key space: 8353064304 keys

Disk space: 61.03 MB

Success probability: 0.596599 (59.66%)

Benchmark

Hash speed: 7621950 hash/sec

Step speed: 3810975 step/sec

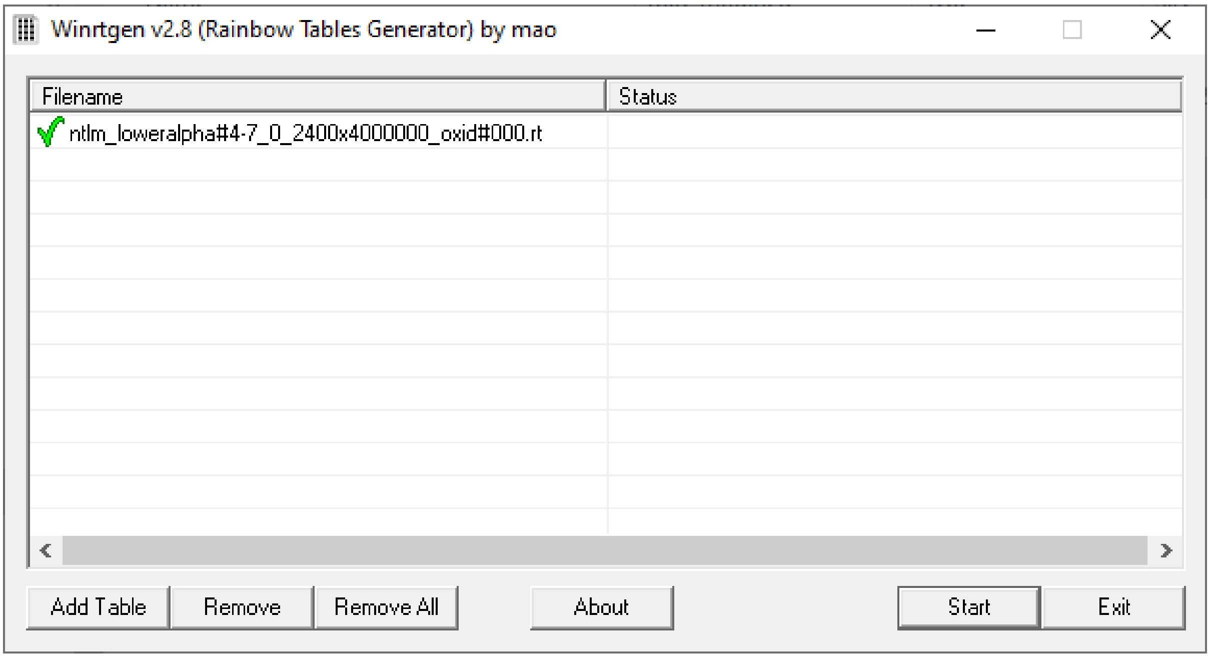
Table precomputation time: 41.984 minutes

Total precomputation time: 41.984 minutes

Max cryptanalysis time: 0.755712 seconds

Optional parameter: Administrator

Figure 3: Parameters for creating the rainbow table.

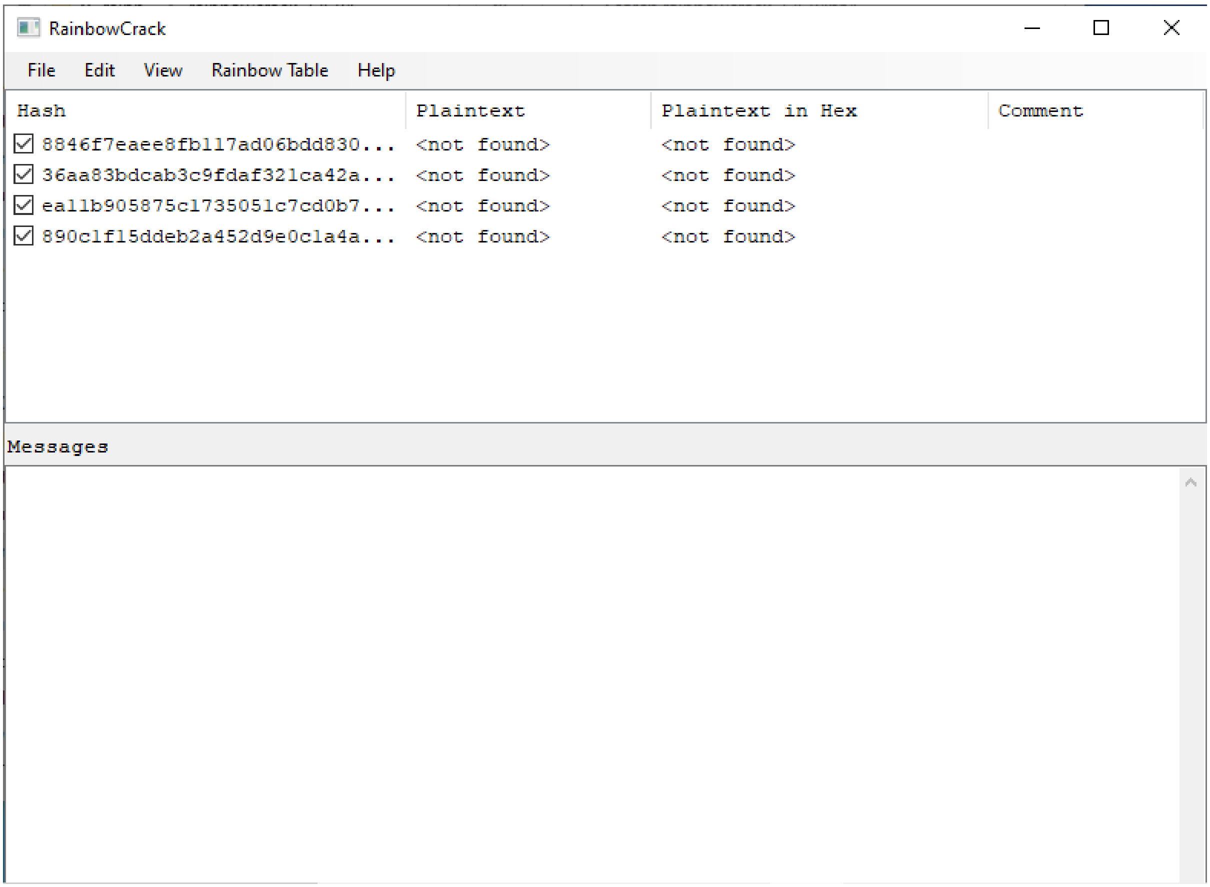


Winrtgen v2.8 (Rainbow Tables Generator) by mao

Filename	Status
✓ ntlm_loweralpha#4-7_0_2400x4000000_oxid#000.rt	

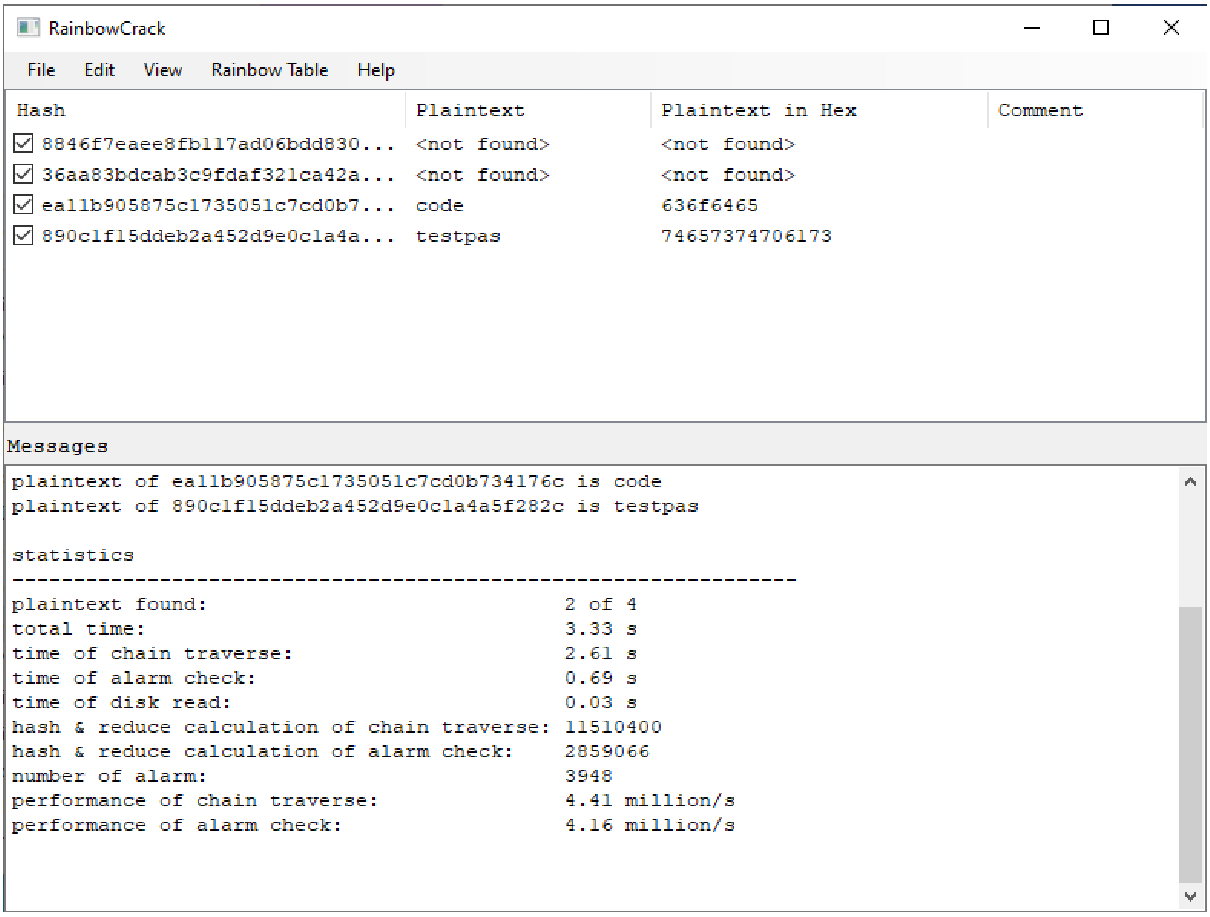
Figure 4: Completed rainbow table.

RainbowCrack had an issue with finding the proper DLL's so I had to import them from my host machine. Once RainbowCrack was working I added the hashes. After locating the rainbow table, RainbowCrack will find the hashes.



Hash	Plaintext	Plaintext in Hex	Comment
☑ 8846f7eaee8fb117ad06bdd830...	<not found>	<not found>	
☑ 36aa83bdcab3c9fdaf321ca42a...	<not found>	<not found>	
☑ ea11b905875c1735051c7cd0b7...	<not found>	<not found>	
☑ 890c1f15ddeb2a452d9e0c1a4a...	<not found>	<not found>	

Figure 5: Added hashes to RainbowCrack.



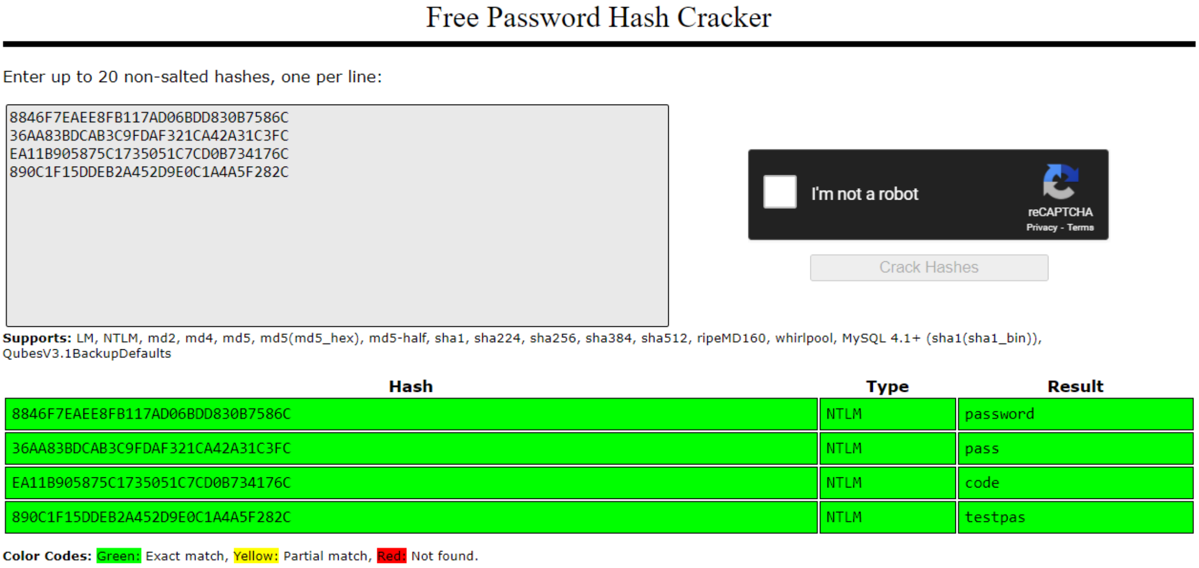
Hash	Plaintext	Plaintext in Hex	Comment
☑ 8846f7eaee8fb117ad06bdd830...	<not found>	<not found>	
☑ 36aa83bdcab3c9fdaf321ca42a...	<not found>	<not found>	
☑ ea11b905875c1735051c7cd0b7...	code	636f6465	
☑ 890c1f15ddeb2a452d9e0c1a4a...	testpas	74657374706173	

Messages

```
plaintext of ea11b905875c1735051c7cd0b734176c is code
plaintext of 890c1f15ddeb2a452d9e0c1a4a5f282c is testpas

statistics
----------------------------------------------------------------
plaintext found:                          2 of 4
total time:                               3.33 s
time of chain traverse:                   2.61 s
time of alarm check:                      0.69 s
time of disk read:                        0.03 s
hash & reduce calculation of chain traverse: 11510400
hash & reduce calculation of alarm check:    2859066
number of alarm:                          3948
performance of chain traverse:            4.41 million/s
performance of alarm check:               4.16 million/s
```

Figure 6: Output of RainbowCrack attempting to find the passwords.

I assume that the reason some passwords were not found was the the rainbow table we generated was not large enough. As a separate test I took them to `crackstation.net` and their rainbow table was able to find the passwords.



Free Password Hash Cracker

Enter up to 20 non-salted hashes, one per line:

```
8846F7EAEE8FB117AD06BDD830B7586C
36AA83BDCAB3C9FDAF321CA42A31C3FC
EA11B905875C1735051C7CD0B734176C
890C1F15DDEB2A452D9E0C1A4A5F282C
```

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
8846F7EAEE8FB117AD06BDD830B7586C	NTLM	password
36AA83BDCAB3C9FDAF321CA42A31C3FC	NTLM	pass
EA11B905875C1735051C7CD0B734176C	NTLM	code
890C1F15DDEB2A452D9E0C1A4A5F282C	NTLM	testpas

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

Figure 7: CrackStation.net output.

This lab taught me how to crack passwords using a rainbow table. First there need to be accounts with passwords susceptible to attacks. These passwords are retrieved from the Security Account Manager (SAM) database file. Next we create a rainbow table that fit the minimum needs of the passwords we are cracking. As stated earlier, the number of values is probably to small to exhaust the password list. RainbowCrack is used to compare the password hashes to the rainbow table, and print the initial text to create the hash.