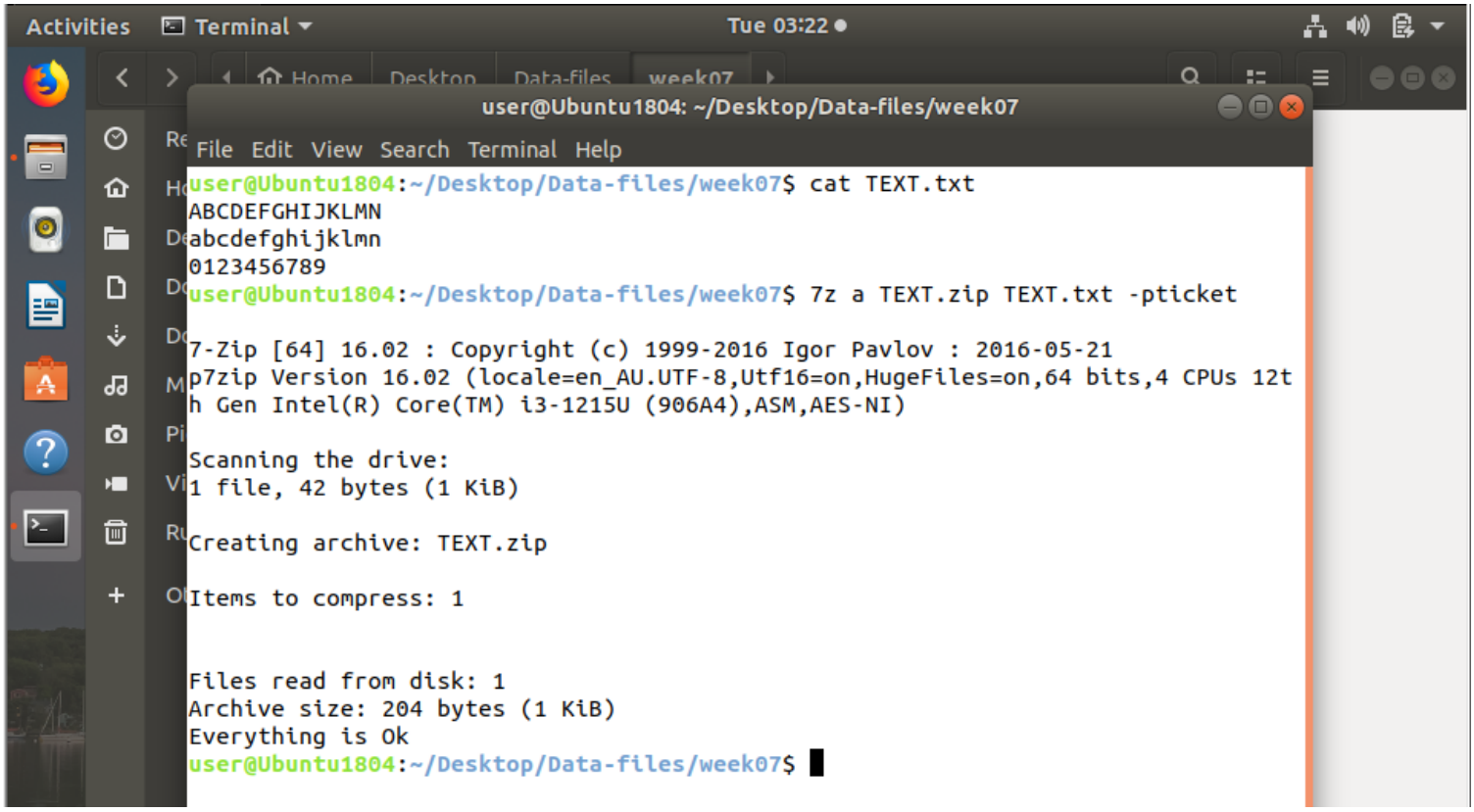
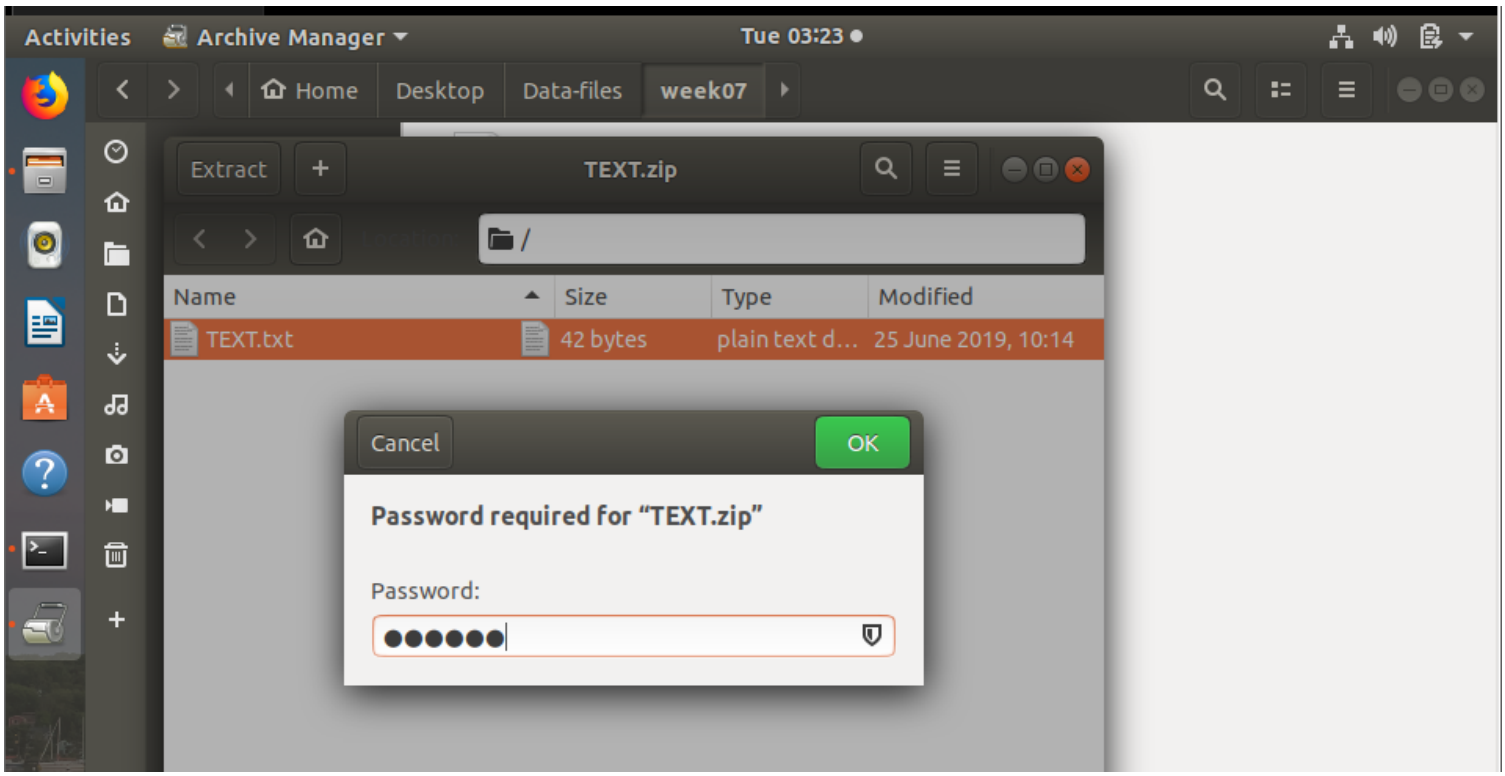
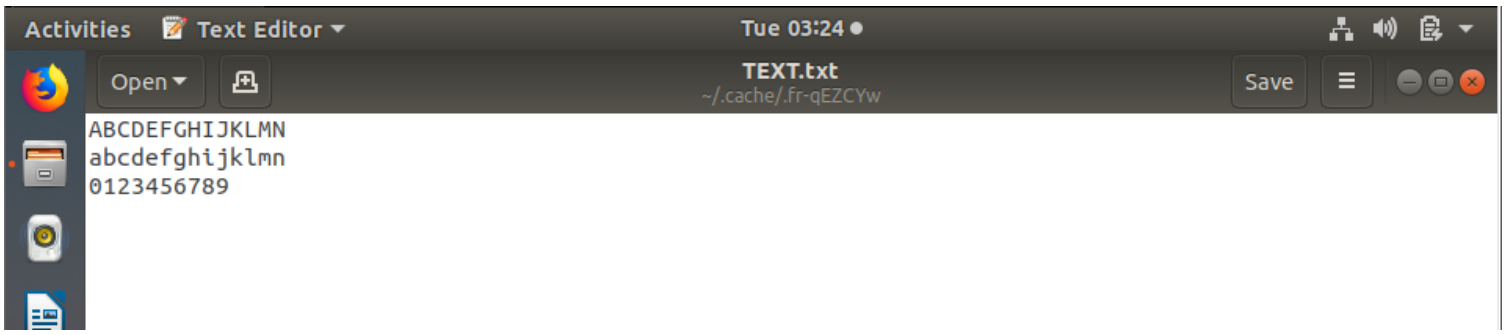
Introducing fcrackzip

The task's main goal was to obtain system administrator rights by breaking passwords with the use of forensic programs like OphCrack and fcrackzip. Initially, I practiced retrieving passwords for ZIP files and Windows computers using the Ubuntu virtual machine and an outside website.

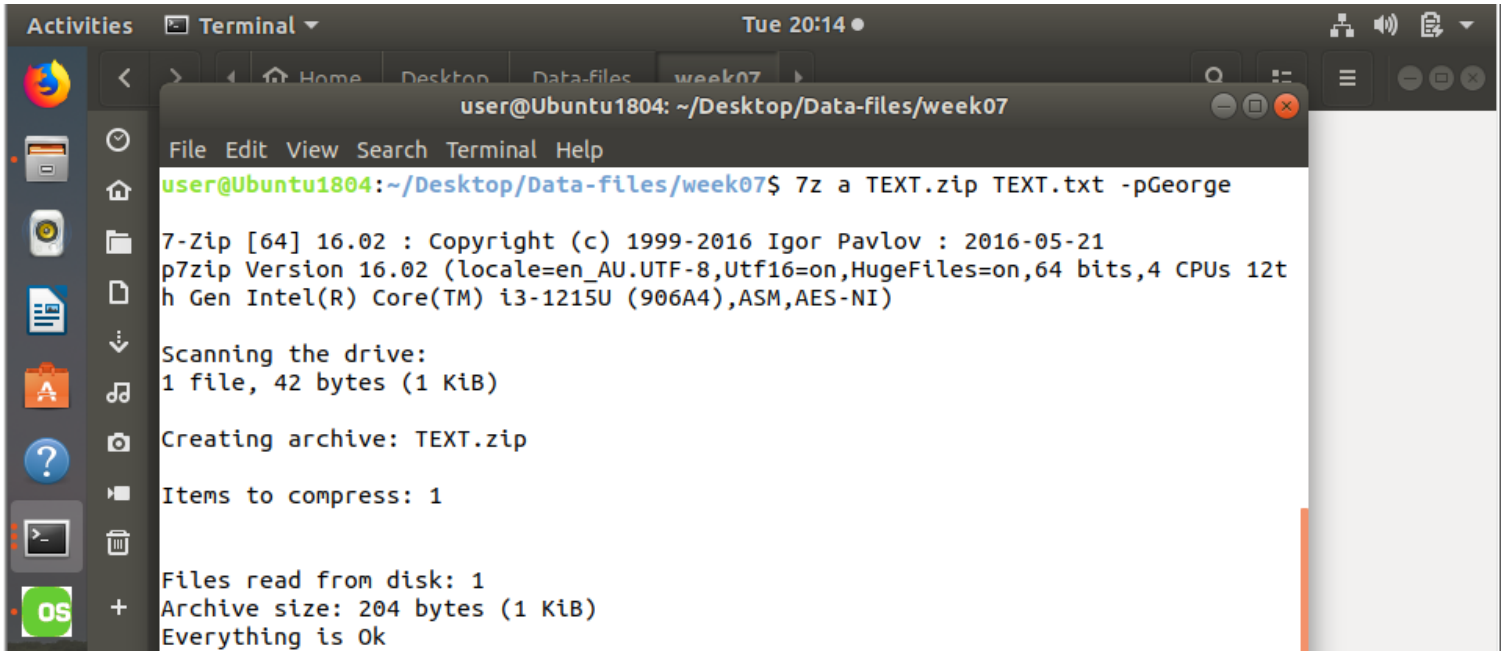
ZIP files and Windows computers using the Ubuntu virtual machine and an outside website. The first goal was to extract encryption passwords from ZIP files using fcrackzip. I began by using the 7zip application to create an encrypted ZIP file, and then I used fcrackzip to crack the password.



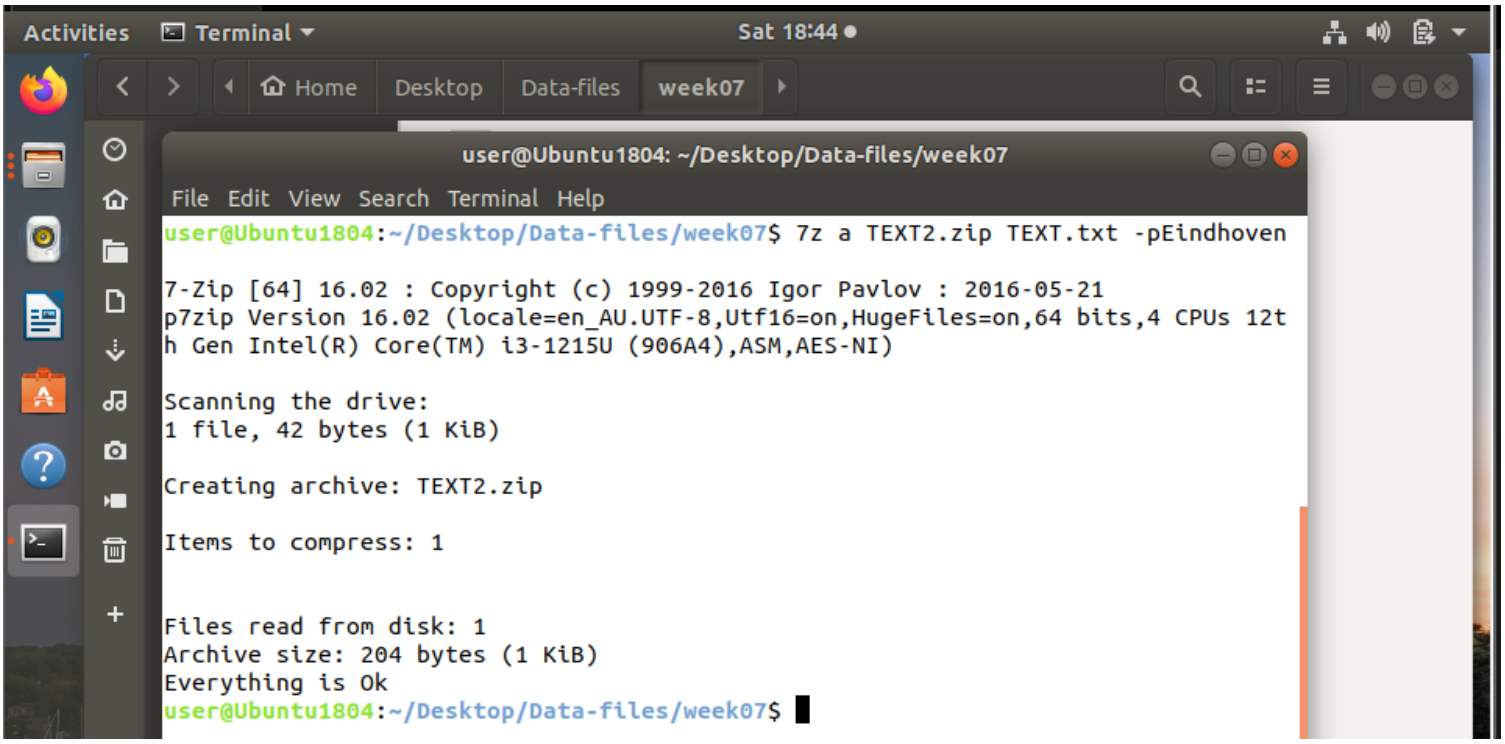




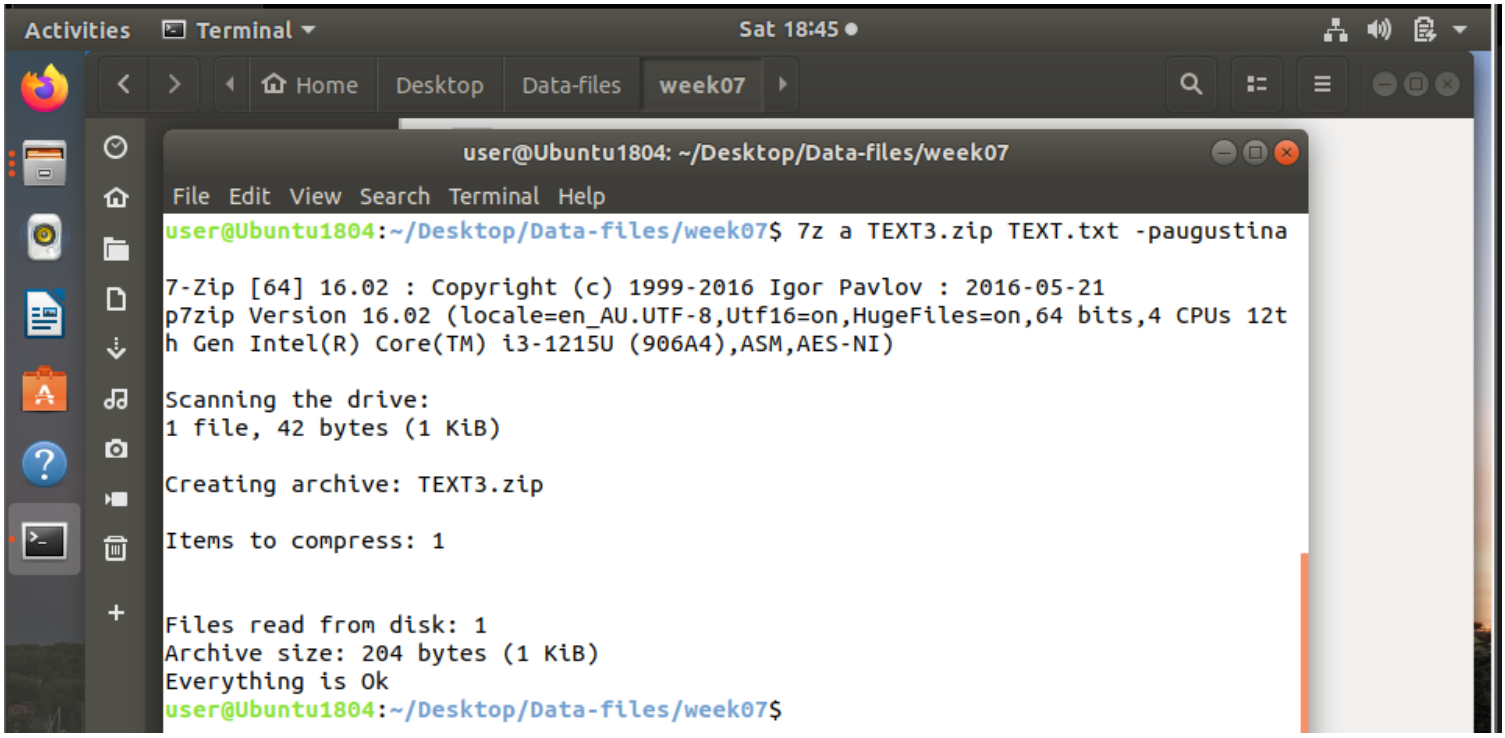
Now, I will create three more text.zip files with different passwords for each using the 7z tool and used the fcrackzip tool to crack it. For this the first TEXT.zip is created with the password George.



For this the first TEXT2.zip is created with the password Eindhoven.



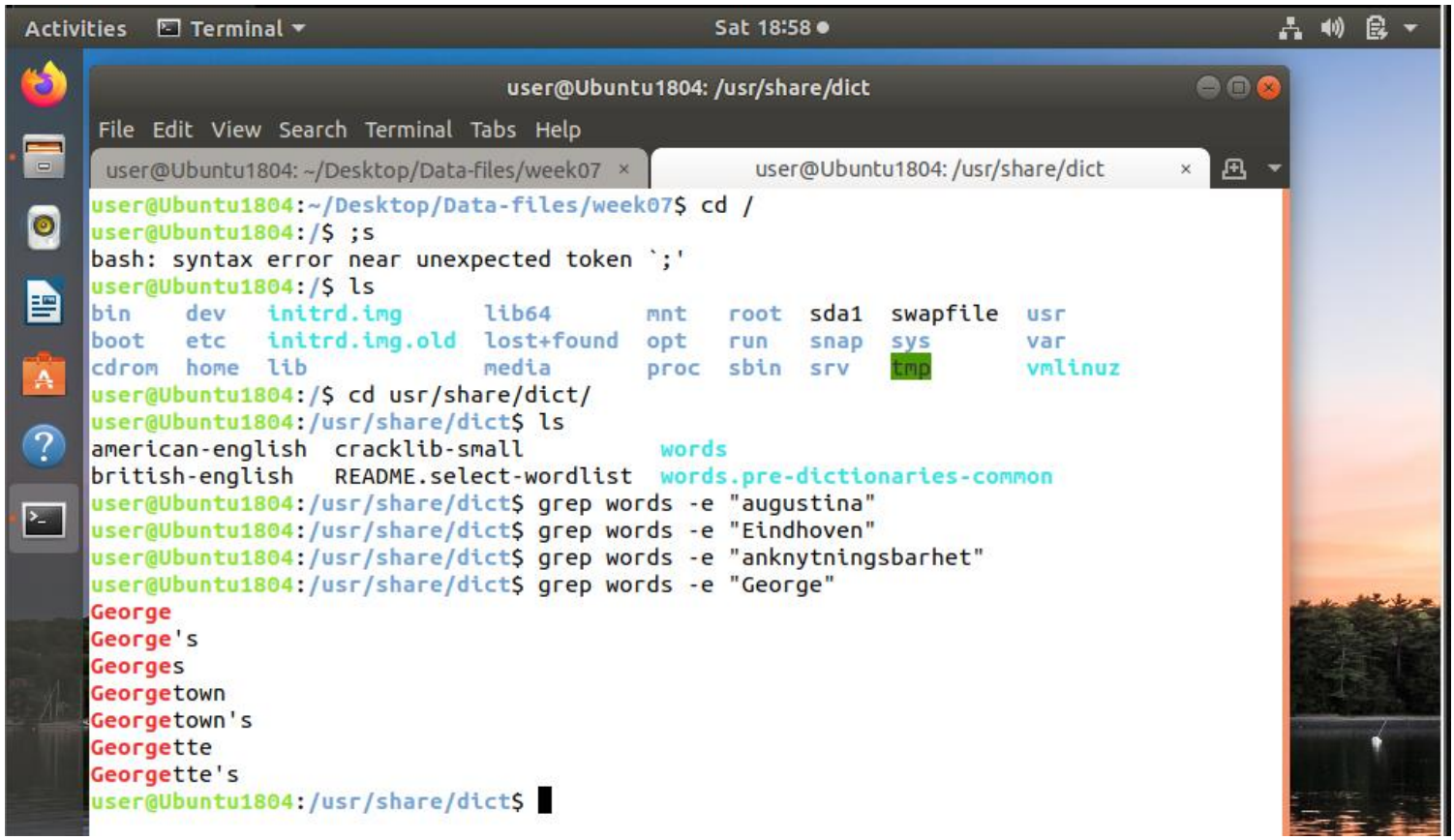
For this the first TEXT3.zip is created with the password augustina.



For this the first TEXT4.zip is created with the password anknytningsbarhet.

I then timed the decryption times for a variety of passwords and ran dictionary and brute-force attacks to compare their efficacy.

But I found that some passwords except George were not in the available password list to bruteforce it, so, if I tried to crack it without the list, it takes a lot of time. So, to solve the problem, I inserted the passwords inside the available list using the echo command.



```
user@Ubuntu1804:/usr/share/dict$ echo "augustina" >> words
bash: words: Permission denied
user@Ubuntu1804:/usr/share/dict$ sudo echo "augustina" >> words
bash: words: Permission denied
user@Ubuntu1804:/usr/share/dict$ sudo su
[sudo] password for user:
root@Ubuntu1804:/usr/share/dict# echo "augustina" >> words
root@Ubuntu1804:/usr/share/dict# echo "Eindhoven" >> words
root@Ubuntu1804:/usr/share/dict# echo "anknytningsbarhet" >> words
root@Ubuntu1804:/usr/share/dict# grep words -e "augustina"
augustina
root@Ubuntu1804:/usr/share/dict# grep words -e "Eindhoven"
Eindhoven
root@Ubuntu1804:/usr/share/dict# grep words -e "anknytningsbarhet"
anknytningsbarhet
root@Ubuntu1804:/usr/share/dict#
```

Now, I used the fcrackzip to brute force the password

```
user@Ubuntu1804:~/Desktop/Data-files/week07$ fcrackzip -u -D -p /usr/share/dict/words T
EXT2.zip


PASSWORD FOUND!!!!: pw == Eindhoven
user@Ubuntu1804:~/Desktop/Data-files/week07$ fcrackzip -u -D -p /usr/share/dict/words T
EXT3.zip


PASSWORD FOUND!!!!: pw == augustina
user@Ubuntu1804:~/Desktop/Data-files/week07$ fcrackzip -u -D -p /usr/share/dict/words T
EXT4.zip


PASSWORD FOUND!!!!: pw == anknytningsbarhet
user@Ubuntu1804:~/Desktop/Data-files/week07$
```

```
user@Ubuntu1804:~/Desktop/Data-files/week07$ fcrackzip -u -D -p /usr/share/dict/
words TEXT.zip


PASSWORD FOUND!!!!: pw == George
user@Ubuntu1804:~/Desktop/Data-files/week07$
```

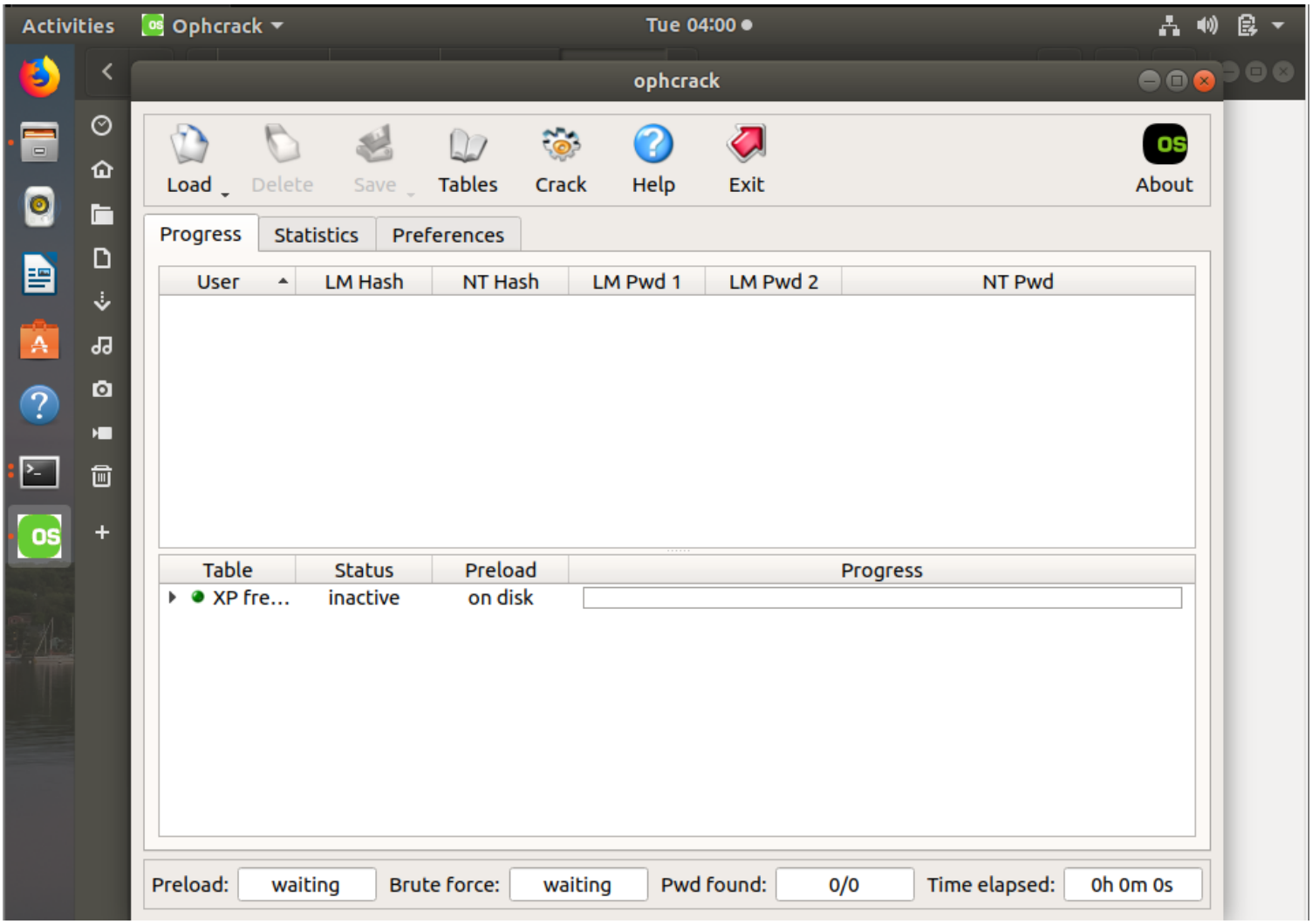
The time it took to crack the zip files with different passwords

Password	George	Eindhoven	augustina	anknytningsbarhet
Decryption Time	4 seconds	4 seconds	4 seconds	4 seconds

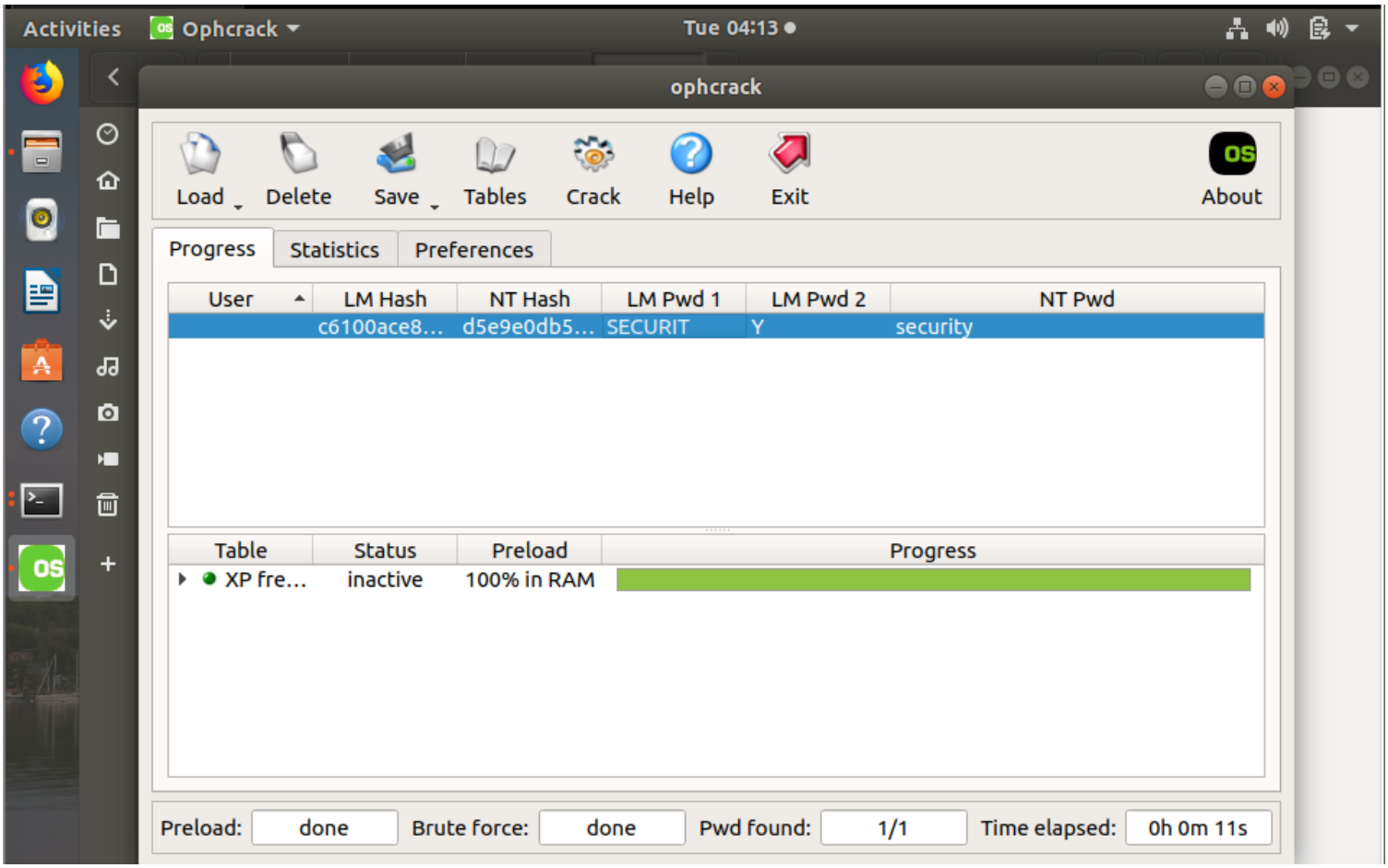
So, this proves that despite the length of the passwords, it takes the same time to crack the passwords that is in the password list.

Using OphCrack to Recover Windows Logon Password

In this task I used the tool calles OphCrack to recover windows logon passwords by providing the hashes for those passwords. To test it, I used the given hash value, and tried to recover the password.



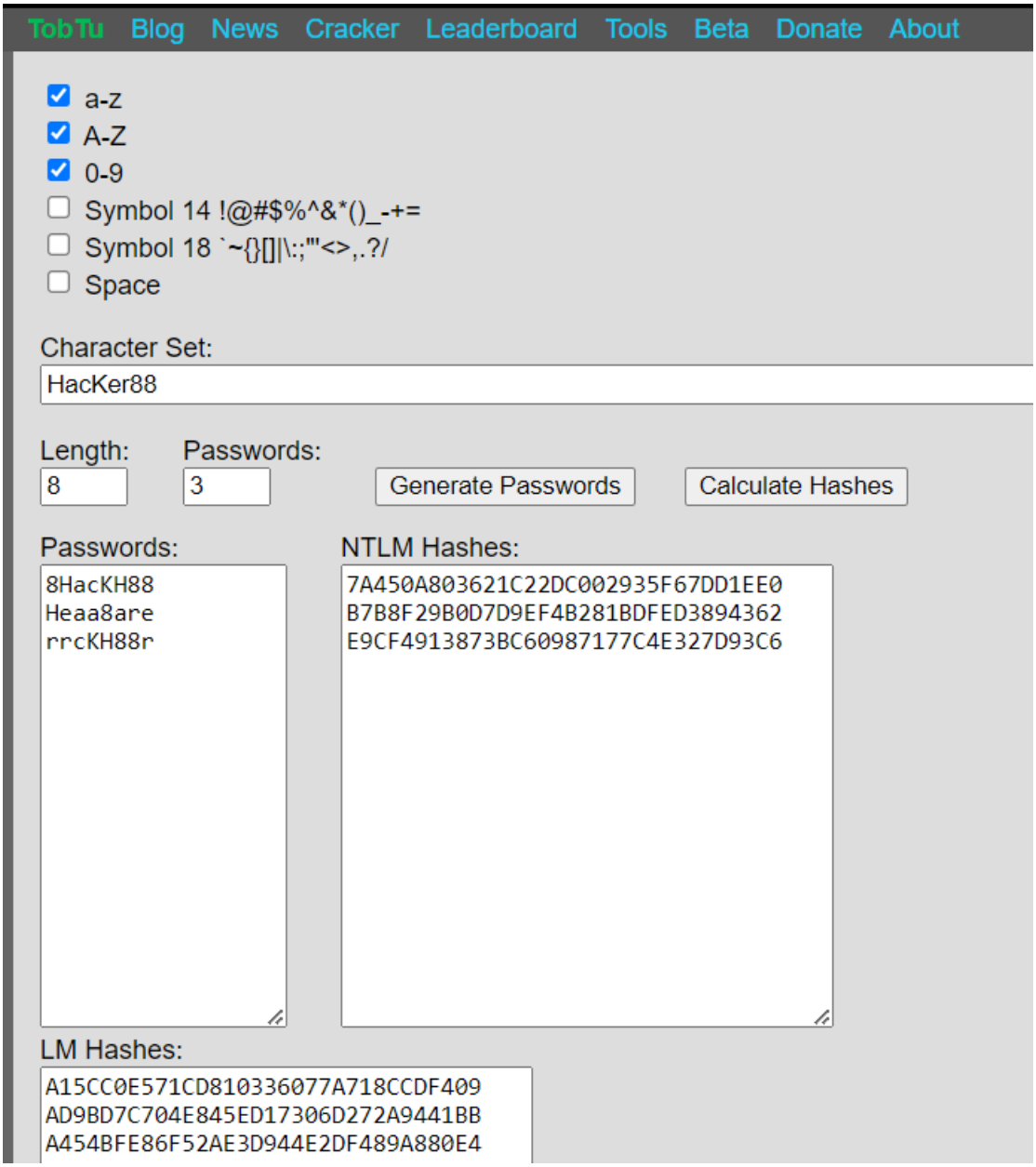
I uploaded the hash and recovered the security.



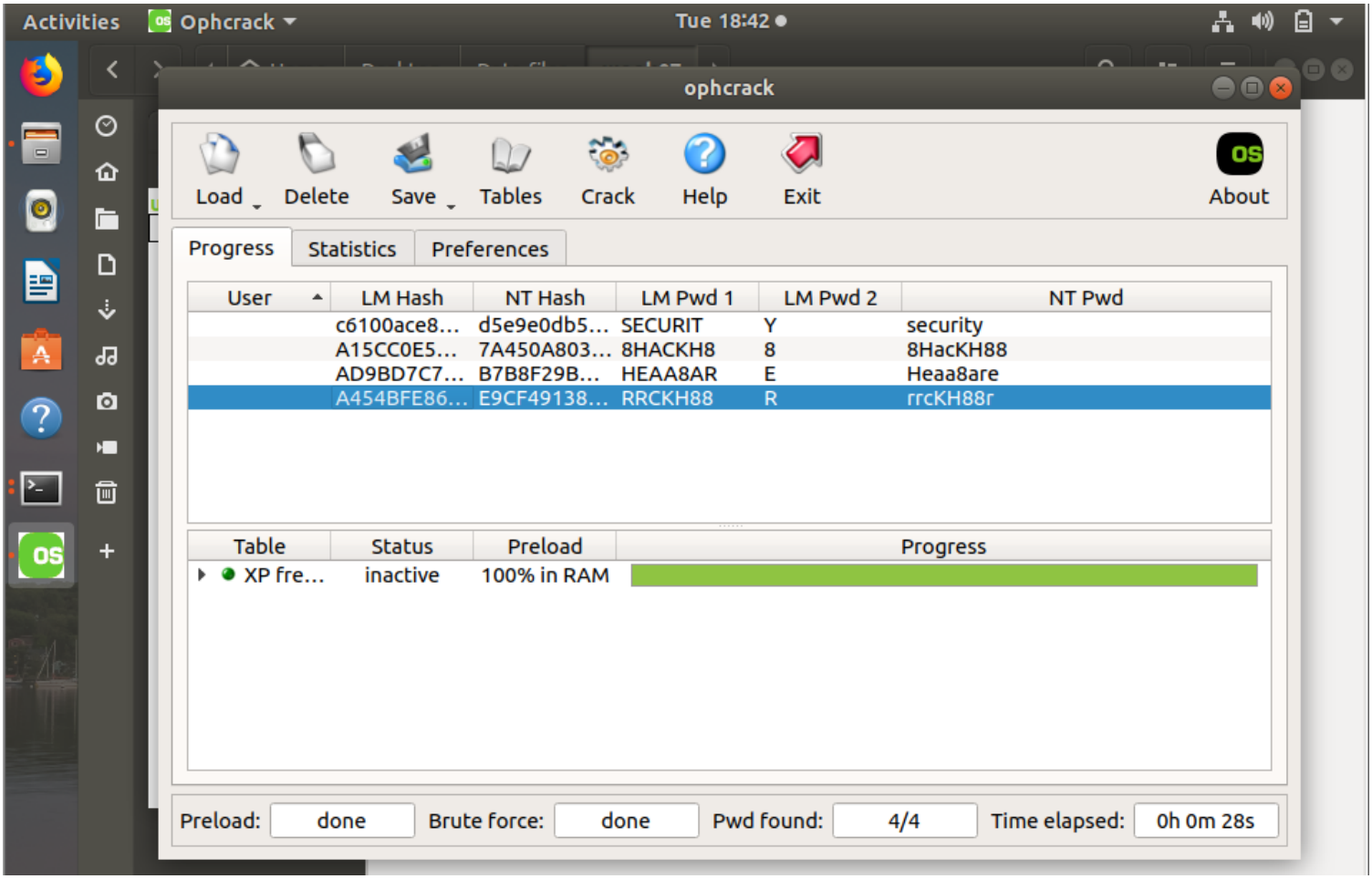
Forensic Tasks

In the end, I created and cracked my own alpha-numeric passwords and tried to crack the hashes that were provided, recording any difficulties and going over the outcomes during the session.

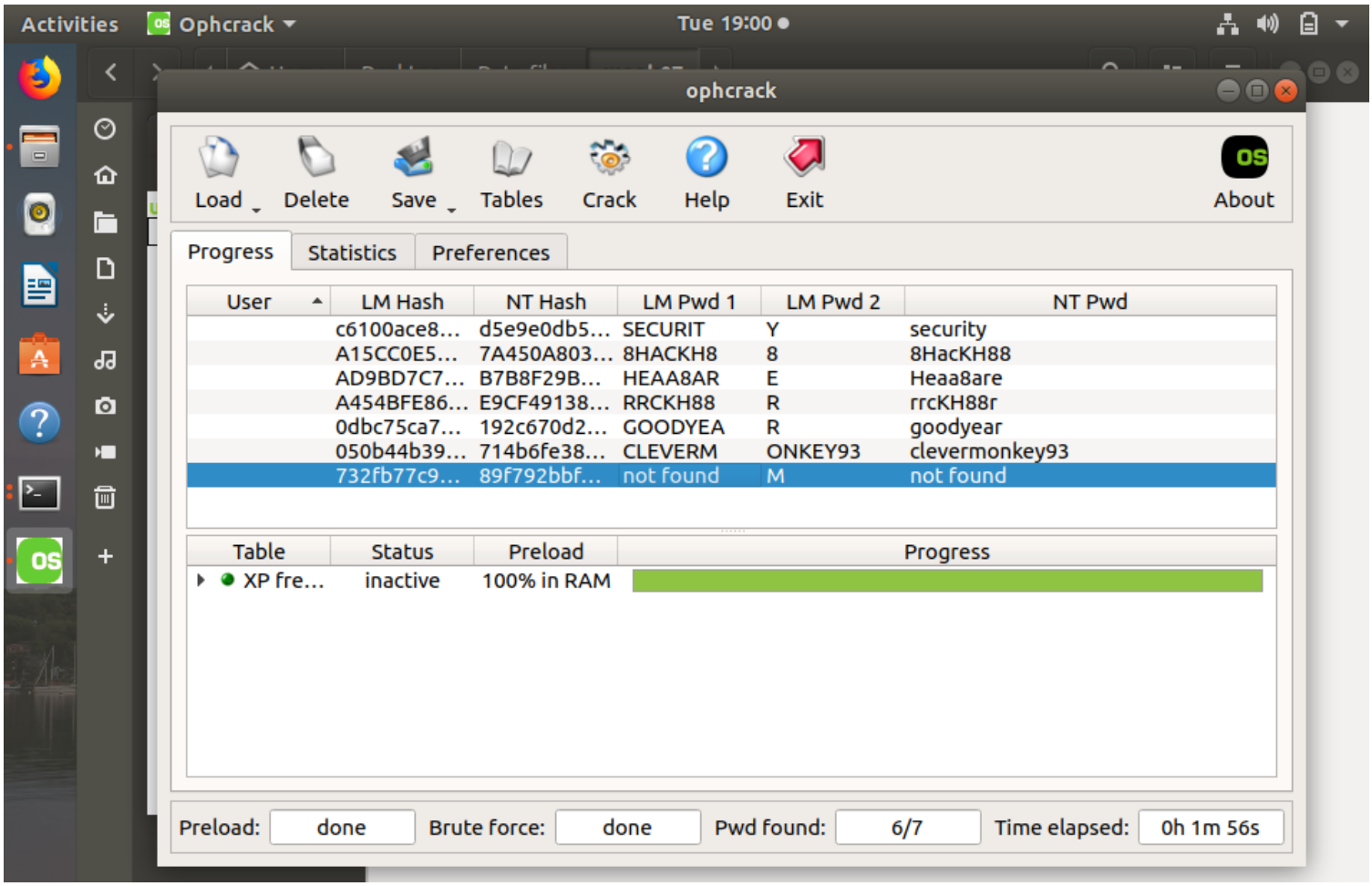
First, I used the **tobtu** to generate hash values for different passwords that I give.



Then I used the OphCrack tool to find how accurately it can recover the passwords. After running the hashes in the tool, it recovered the passwords correctly.



Finally, I tried to recover the password for the given hashes in the assignment. Out of three hashes, two hashes were recovered, which is goodyear and clevermonkey93 and the 3rd one was unable to be found.



Only the last hash was unable to be found. That can be because of various reasons:

- It can be a hash from an alternative software or operating system. Ophcrack is limited to cracking Windows system hashes, both LM and NT.
- That hash could be corrupted. Cracking the hash with ophcrack is not possible if it was tampered with during the password reset procedure.
- It might not even be a hash. The value in the "NT Hash" column might just be a character string that is chosen at random.