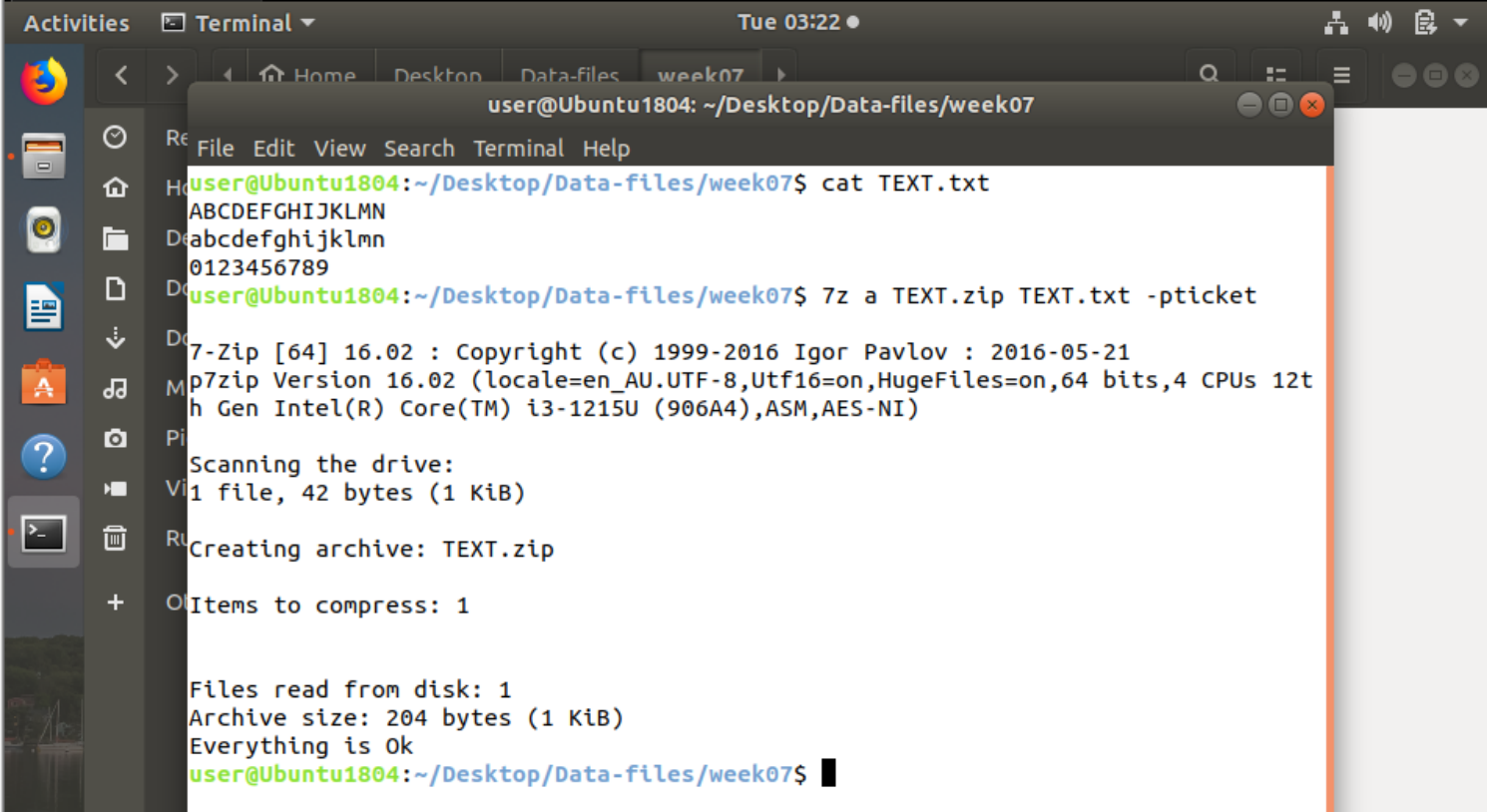


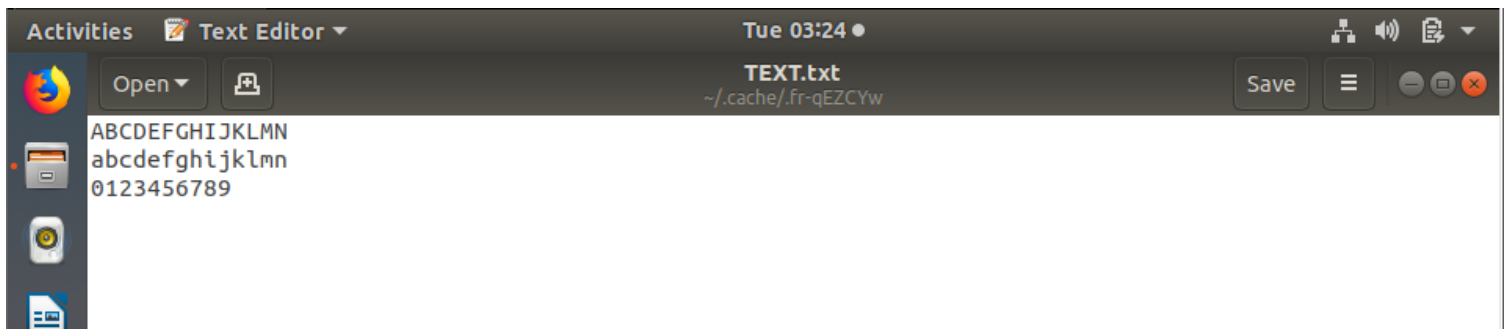
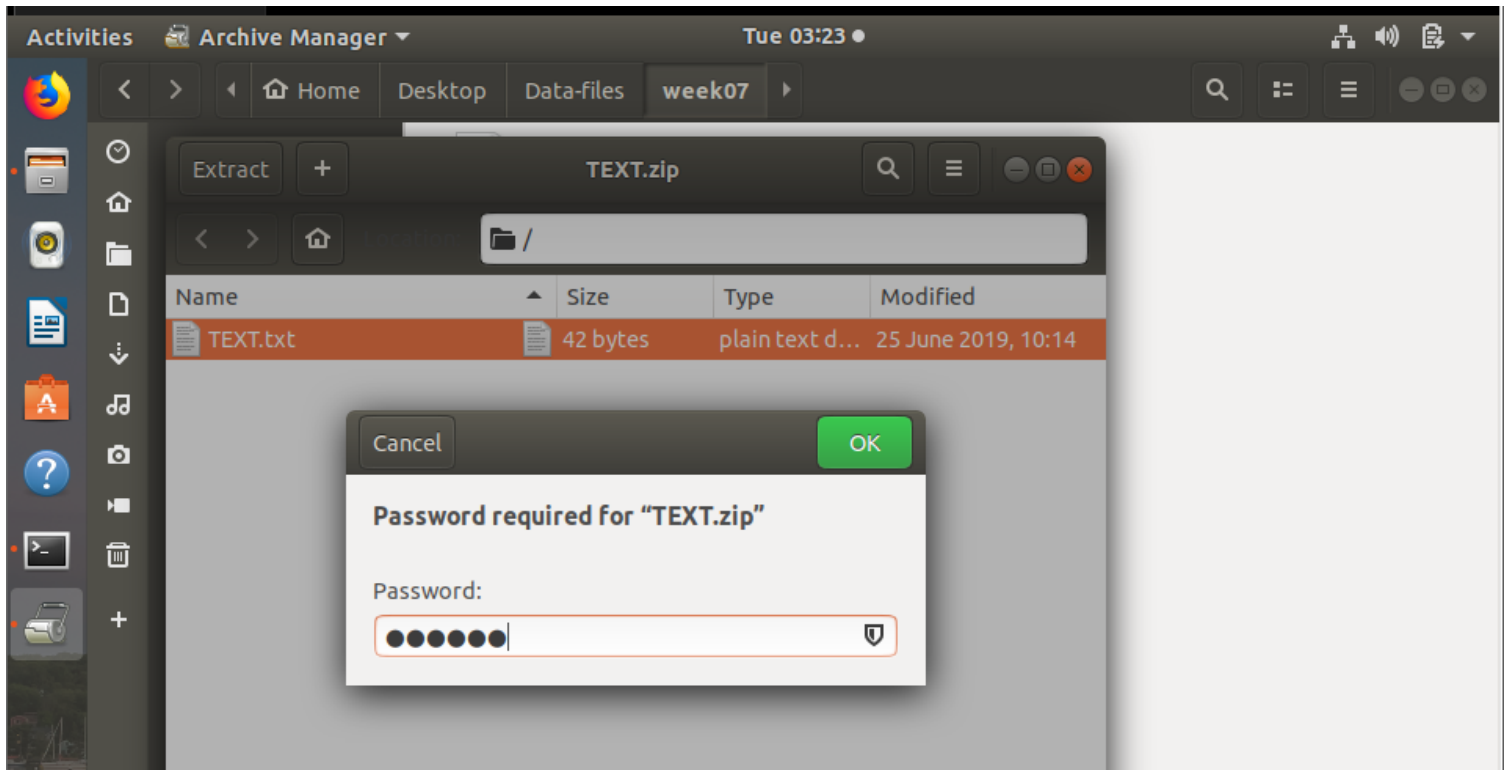
Introducing fcrackzip

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.

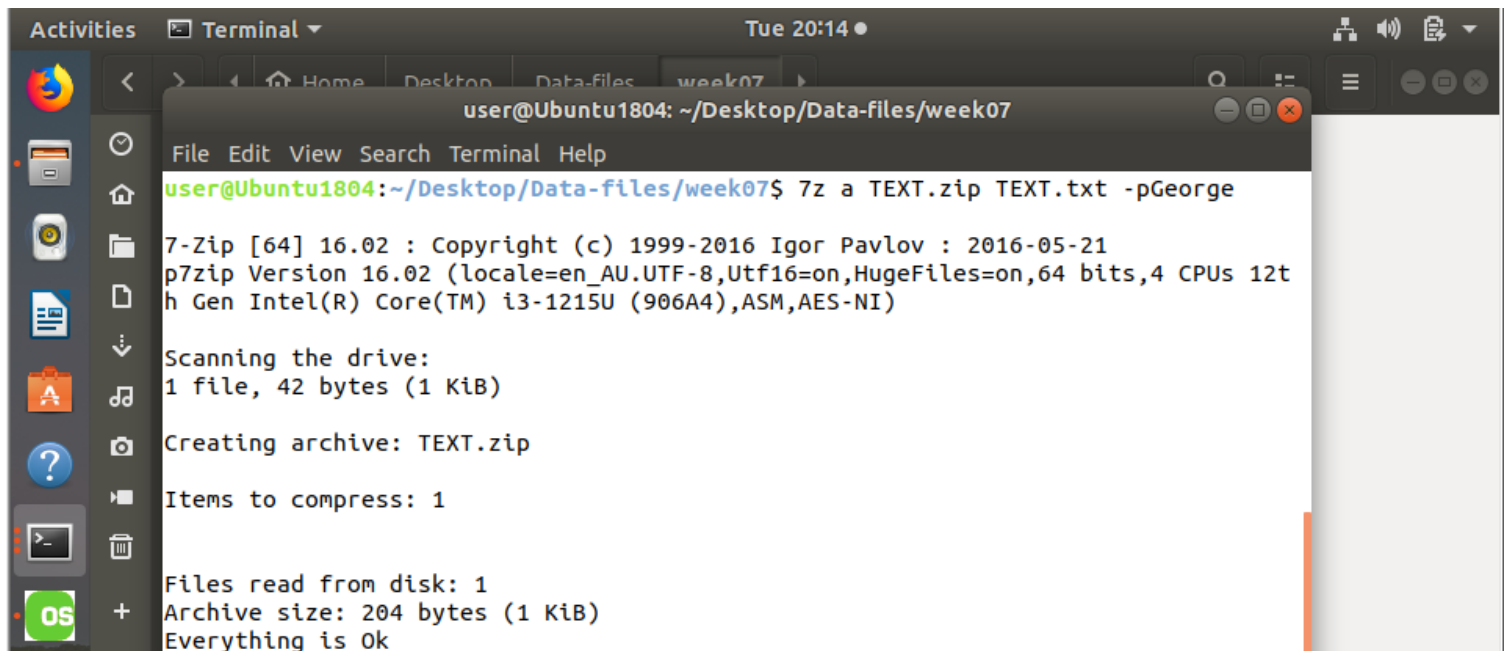
ZIP files and Windows computers using the Ubuntu virtual machine and an outside website. The first goal was to extract encryption passwords from ZIP files using fcrackzip. I began by using the 7zip application to create an encrypted ZIP file, and then I used fcrackzip to crack the password.



```
user@Ubuntu1804: ~/Desktop/Data-files/week07
File Edit View Search Terminal Help
user@Ubuntu1804:~/Desktop/Data-files/week07$ cat TEXT.txt
ABCDEFGHIJKLMN
D:abcdefghijklmn
0123456789
user@Ubuntu1804:~/Desktop/Data-files/week07$ 7z a TEXT.zip TEXT.txt -pticket
7-Zip [64] 16.02 : Copyright (c) 1999-2016 Igor Pavlov : 2016-05-21
p7zip Version 16.02 (locale=en_AU.UTF-8,Utf16=on,HugeFiles=on,64 bits,4 CPUs 12t
h Gen Intel(R) Core(TM) i3-1215U (906A4),ASM,AES-NI)
Scanning the drive:
1 file, 42 bytes (1 KiB)
Creating archive: TEXT.zip
Items to compress: 1
Files read from disk: 1
Archive size: 204 bytes (1 KiB)
Everything is Ok
user@Ubuntu1804:~/Desktop/Data-files/week07$
```



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.



A terminal window titled "user@Ubuntu1804: ~/Desktop/Data-files/week07" is shown. The window has a menu bar with "File", "Edit", "View", "Search", "Terminal", and "Help". The terminal output shows the command `7z a TEXT2.zip TEXT.txt -pEindhoven` being executed. The output includes version information for 7-Zip, a drive scan showing 1 file (42 bytes), and the creation of the archive TEXT2.zip. The final status is "Everything is Ok".

```
user@Ubuntu1804: ~/Desktop/Data-files/week07
File Edit View Search Terminal Help
user@Ubuntu1804:~/Desktop/Data-files/week07$ 7z a TEXT2.zip TEXT.txt -pEindhoven

7-Zip [64] 16.02 : Copyright (c) 1999-2016 Igor Pavlov : 2016-05-21
p7zip Version 16.02 (locale=en_AU.UTF-8,Utf16=on,HugeFiles=on,64 bits,4 CPUs 12t
h Gen Intel(R) Core(TM) i3-1215U (906A4),ASM,AES-NI)

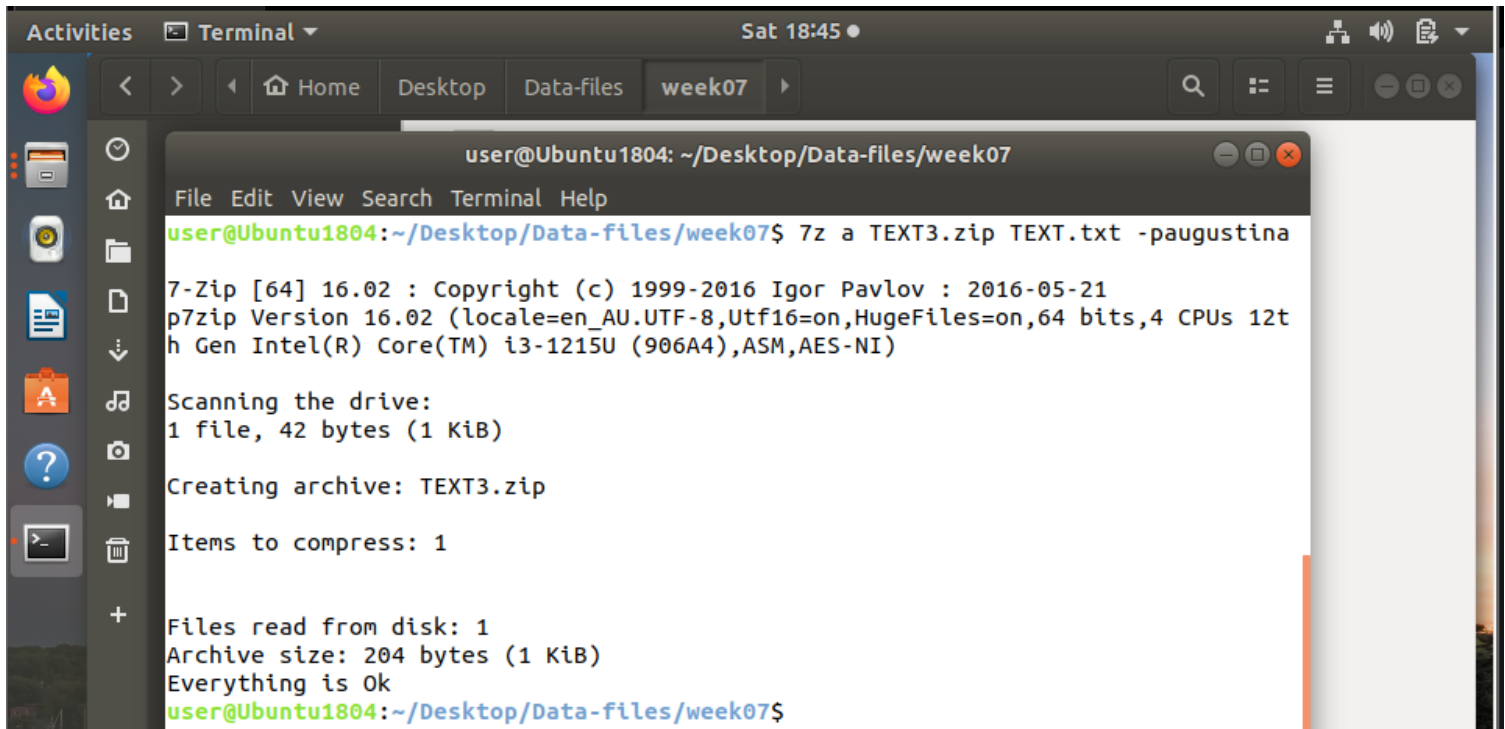
Scanning the drive:
1 file, 42 bytes (1 KiB)

Creating archive: TEXT2.zip

Items to compress: 1

Files read from disk: 1
Archive size: 204 bytes (1 KiB)
Everything is Ok
user@Ubuntu1804:~/Desktop/Data-files/week07$
```

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



A terminal window titled "user@Ubuntu1804: ~/Desktop/Data-files/week07" is shown. The window has a menu bar with "File", "Edit", "View", "Search", "Terminal", and "Help". The terminal output shows the command `7z a TEXT3.zip TEXT.txt -paugustina` being executed. The output includes version information for 7-Zip, a drive scan showing 1 file (42 bytes), and the creation of the archive TEXT3.zip. The final status is "Everything is Ok".

```
user@Ubuntu1804: ~/Desktop/Data-files/week07
File Edit View Search Terminal Help
user@Ubuntu1804:~/Desktop/Data-files/week07$ 7z a TEXT3.zip TEXT.txt -paugustina

7-Zip [64] 16.02 : Copyright (c) 1999-2016 Igor Pavlov : 2016-05-21
p7zip Version 16.02 (locale=en_AU.UTF-8,Utf16=on,HugeFiles=on,64 bits,4 CPUs 12t
h Gen Intel(R) Core(TM) i3-1215U (906A4),ASM,AES-NI)

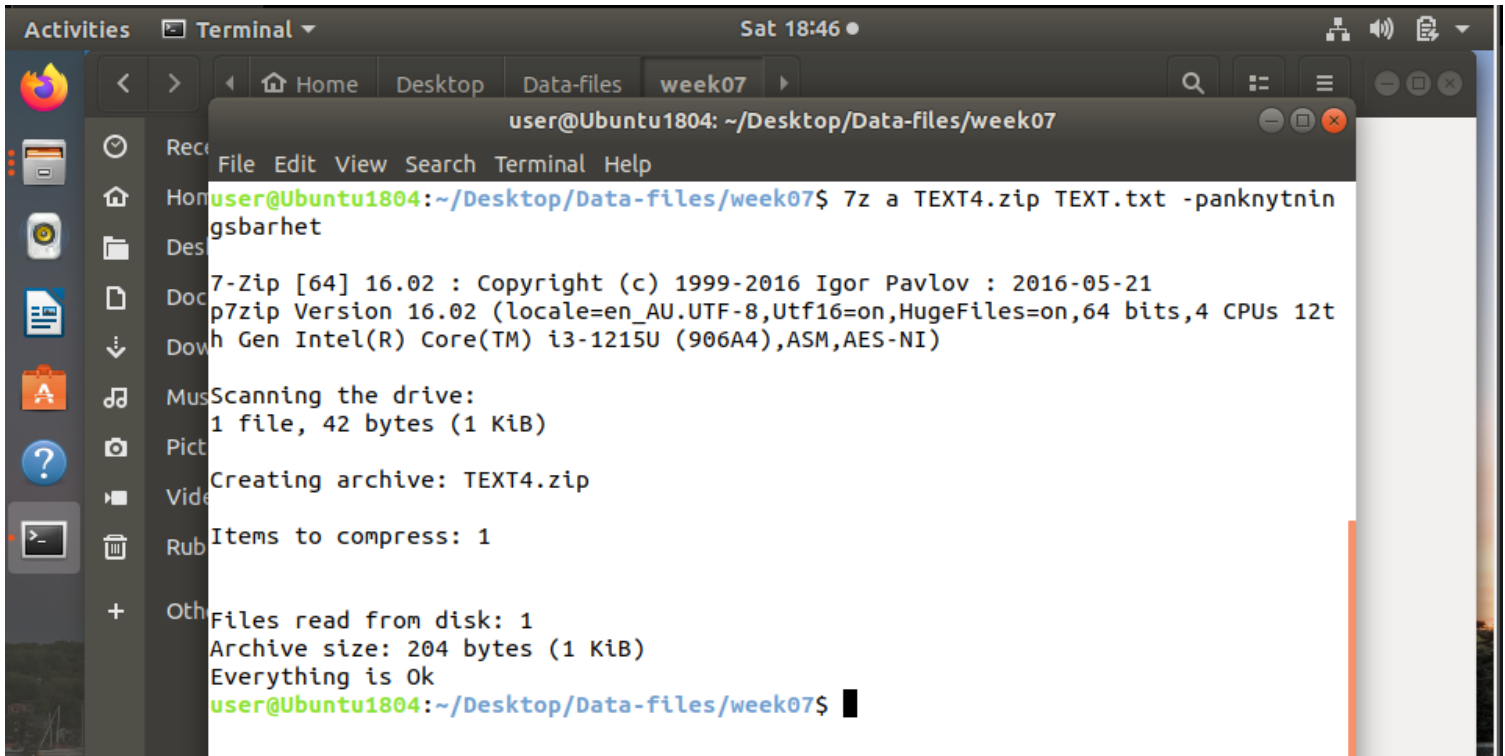
Scanning the drive:
1 file, 42 bytes (1 KiB)

Creating archive: TEXT3.zip

Items to compress: 1

Files read from disk: 1
Archive size: 204 bytes (1 KiB)
Everything is Ok
user@Ubuntu1804:~/Desktop/Data-files/week07$
```

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

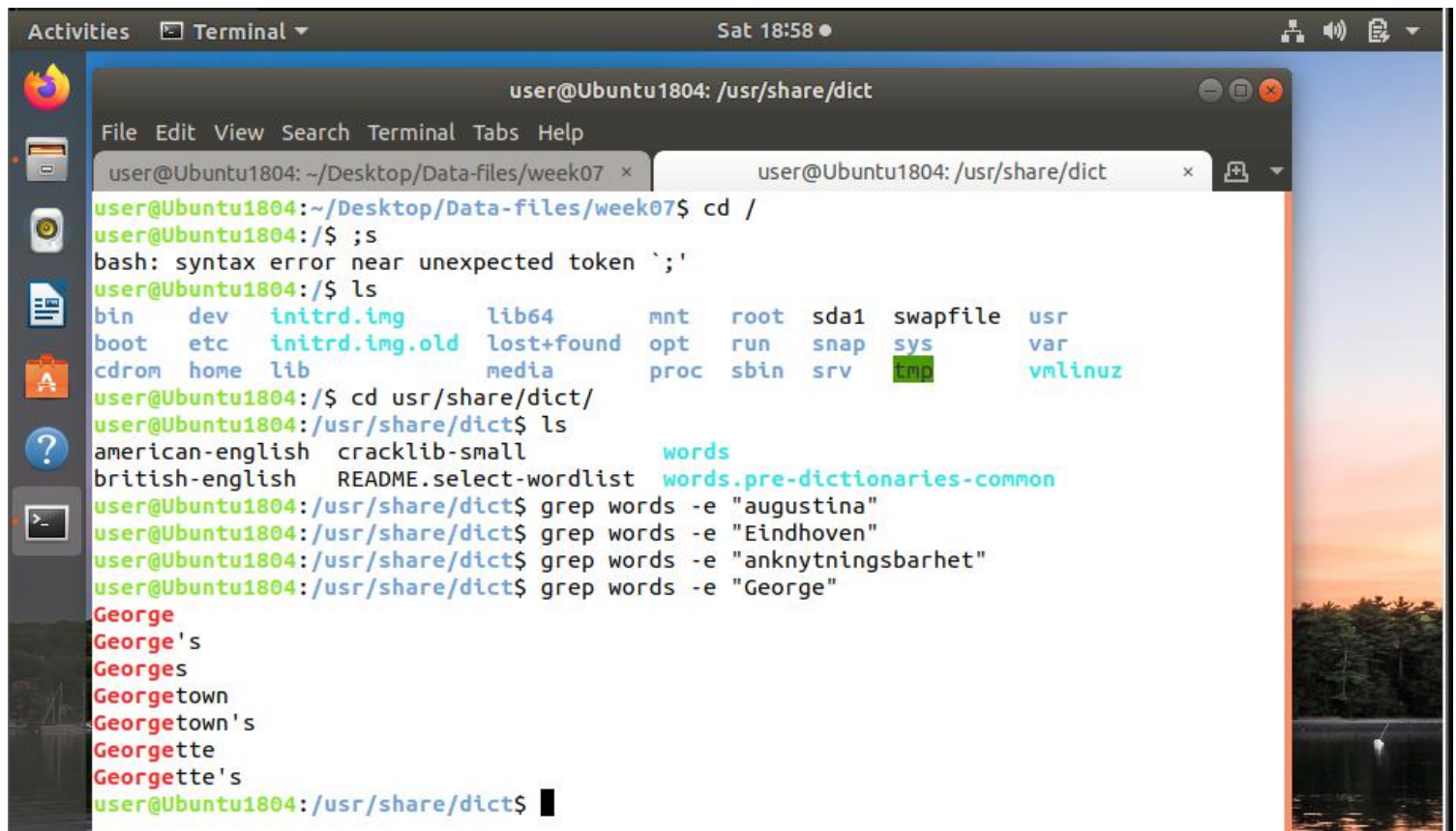


The screenshot shows a terminal window titled "user@Ubuntu1804: ~/Desktop/Data-files/week07". The user has executed the command `7z a TEXT4.zip TEXT.txt -panknytningsbarhet`. The terminal output shows the 7-Zip version (16.02), system information (Ubuntu 18.04, Intel Core i3-1215U), and the process of creating the archive. It indicates that 1 file (42 bytes) was scanned and compressed into TEXT4.zip, with an archive size of 204 bytes.

```
user@Ubuntu1804: ~/Desktop/Data-files/week07
File Edit View Search Terminal Help
user@Ubuntu1804:~/Desktop/Data-files/week07$ 7z a TEXT4.zip TEXT.txt -panknytnin
gsbarhet
7-Zip [64] 16.02 : Copyright (c) 1999-2016 Igor Pavlov : 2016-05-21
p7zip Version 16.02 (locale=en_AU.UTF-8,Utf16=on,HugeFiles=on,64 bits,4 CPUs 12t
h Gen Intel(R) Core(TM) i3-1215U (906A4),ASM,AES-NI)
Scanning the drive:
1 file, 42 bytes (1 KiB)
Creating archive: TEXT4.zip
Items to compress: 1
Files read from disk: 1
Archive size: 204 bytes (1 KiB)
Everything is Ok
user@Ubuntu1804:~/Desktop/Data-files/week07$
```

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.



The screenshot shows a terminal window titled "user@Ubuntu1804: /usr/share/dict". The user has navigated to the directory `/usr/share/dict` and listed the files. They then used the `grep` command to search for the password "George" in the dictionary files. The output shows that "George" is found in the file `words`.

```
user@Ubuntu1804: /usr/share/dict
File Edit View Search Terminal Tabs Help
user@Ubuntu1804:~/Desktop/Data-files/week07$ cd /
user@Ubuntu1804:/$ ;s
bash: syntax error near unexpected token `;'
user@Ubuntu1804:/$ ls
bin    dev    initrd.img    lib64    mnt    root    sda1    swapfile    usr
boot  etc    initrd.img.old  lost+found  opt    run    snap    sys    var
cdrom  home  lib          media    proc   sbin   srv     tmp     vmlinuz
user@Ubuntu1804:/$ cd /usr/share/dict/
user@Ubuntu1804:/usr/share/dict$ ls
american-english  cracklib-small  words
british-english  README.select-wordlist  words.pre-dictionaries-common
user@Ubuntu1804:/usr/share/dict$ grep words -e "augustina"
user@Ubuntu1804:/usr/share/dict$ grep words -e "Eindhoven"
user@Ubuntu1804:/usr/share/dict$ grep words -e "anknytningsbarhet"
user@Ubuntu1804:/usr/share/dict$ grep words -e "George"
George
George's
Georges
Georgetown
Georgetown's
Georgette
Georgette's
user@Ubuntu1804:/usr/share/dict$
```

```
Activities Terminal Sat 19:07
root@Ubuntu1804: /usr/share/dict

File Edit View Search Terminal Tabs Help
user@Ubuntu1804: ~/Desktop/Data-files/week07 x root@Ubuntu1804: /usr/share/dict x

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

```
Activities Terminal Sat 19:50
user@Ubuntu1804: ~/Desktop/Data-files/week07

File Edit View Search Terminal Tabs Help
user@Ubuntu1804: ~/Desktop/Data-files/week07 x root@Ubuntu1804: /usr/share/dict x

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$
```

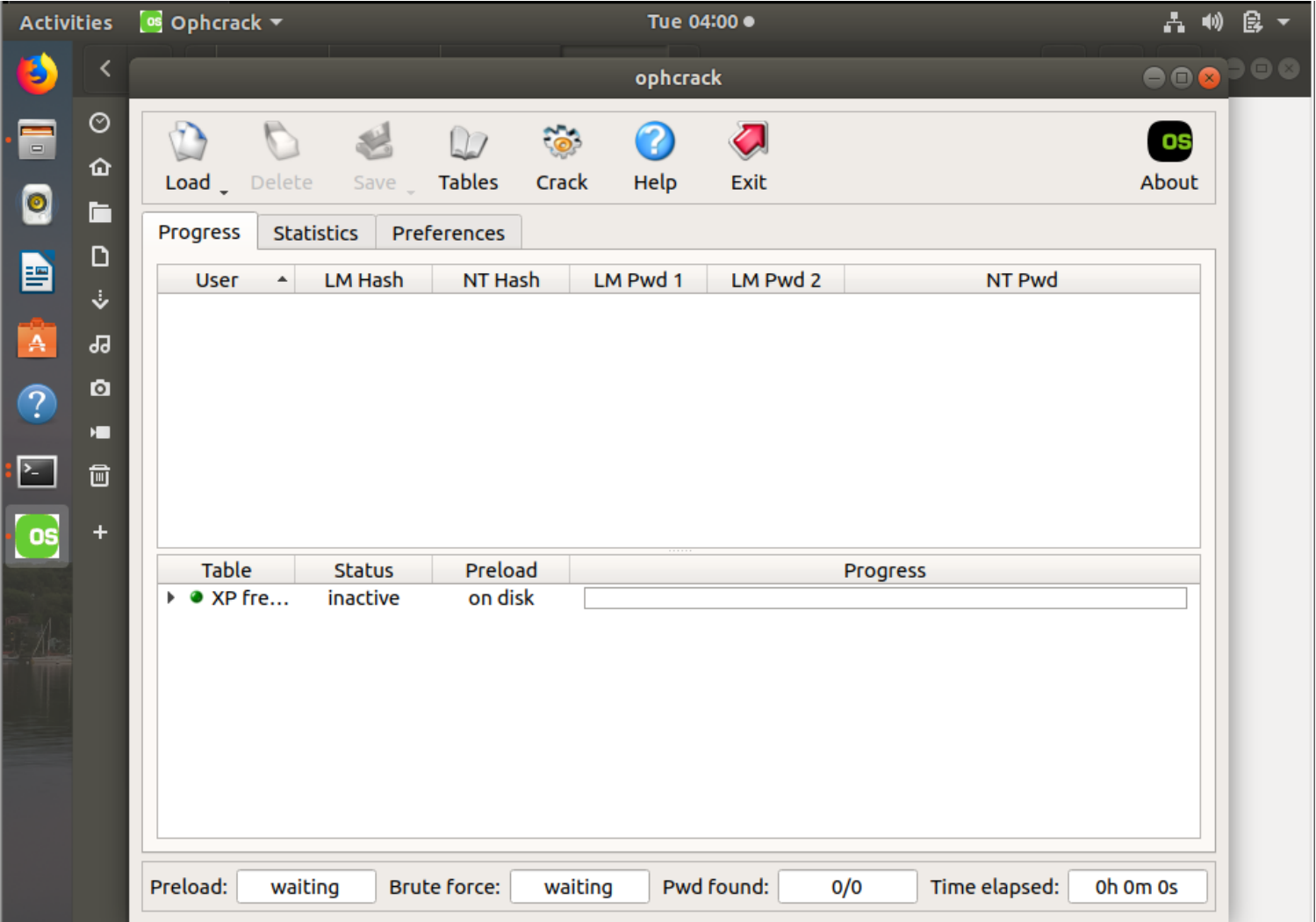
The time it took to crack the zip files with different passwords

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 called 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.

Activities

OS Ophcrack

Tue 04:13

OS

Load

Delete

Save

Tables

Crack

Help

Exit

About

Progress

Statistics

Preferences

User	LM Hash	NT Hash	LM Pwd 1	LM Pwd 2	NT Pwd
	c6100ace8...	d5e9e0db5...	SECURIT	Y	security

Table	Status	Preload	Progress
XP fre...	inactive	100% in RAM	

Preload: done

Brute force: done

Pwd found: 1/1

Time elapsed: 0h 0m 11s

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.

[TobTu](#) [Blog](#) [News](#) [Cracker](#) [Leaderboard](#) [Tools](#) [Beta](#) [Donate](#) [About](#)

☒ a-z

☒ A-Z

☒ 0-9

☐ Symbol 14 !@#\$%^&*()_-=

☐ Symbol 18 `~{}|\\:;'"<>,.?/

☐ Space

Character Set:

HacKer88

Length:

8

Passwords:

3

Generate Passwords

Calculate Hashes

Passwords:

8HacKH88
Heaa8are
rrcKH88r

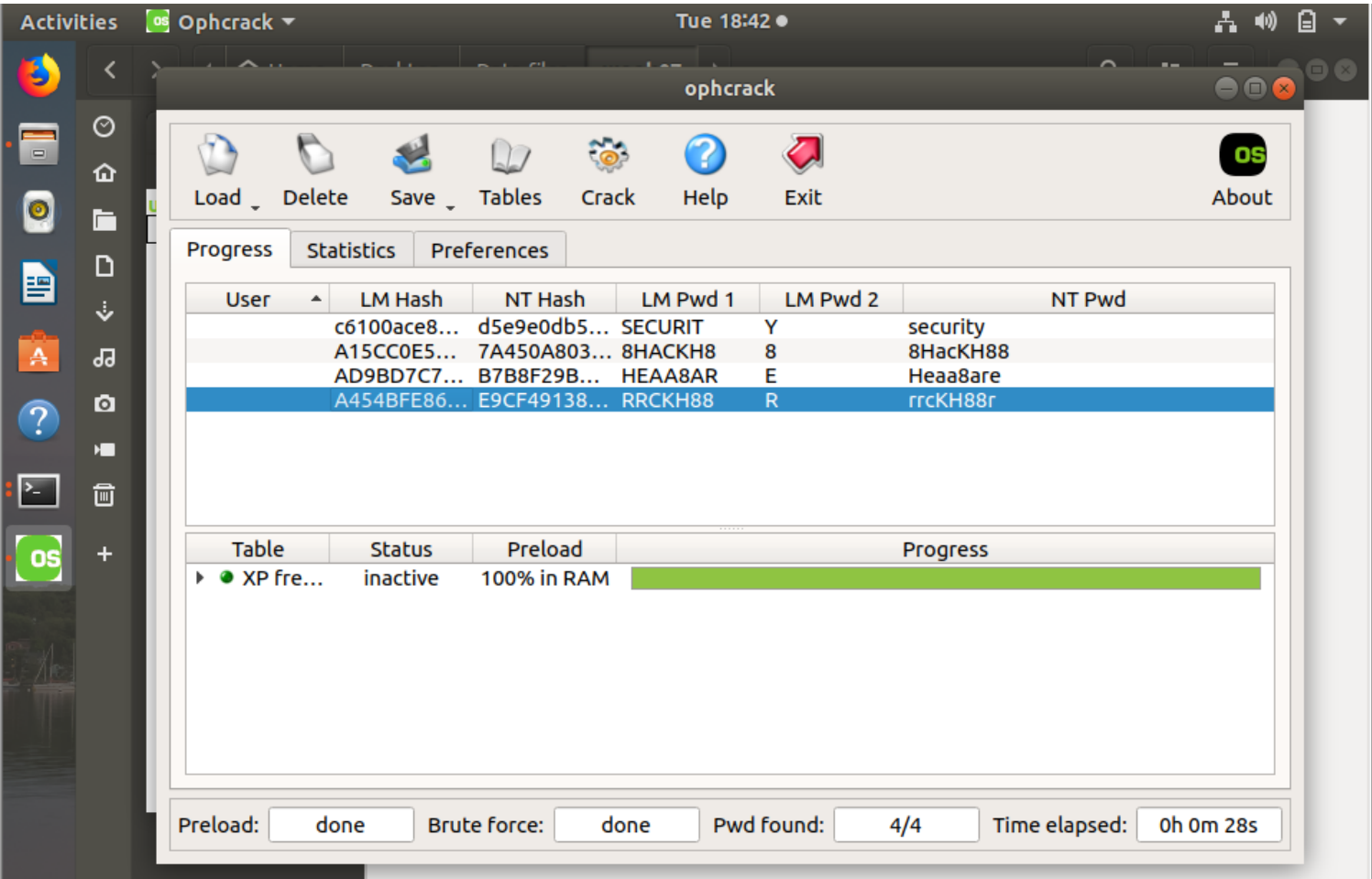
NTLM Hashes:

7A450A803621C22DC002935F67DD1EE0
B7B8F29B0D7D9EF4B281BDFED3894362
E9CF4913873BC60987177C4E327D93C6

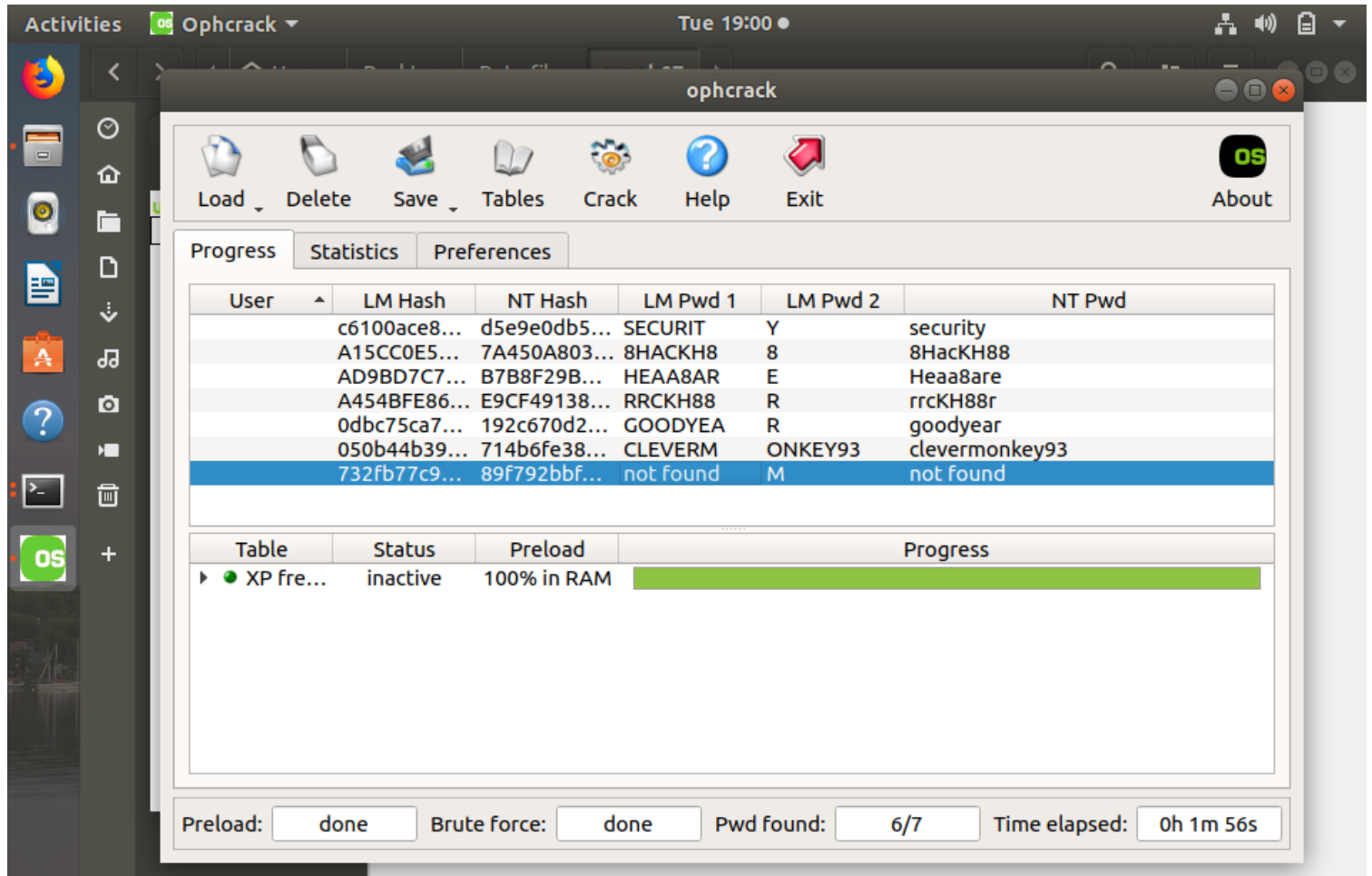
LM Hashes:

A15CC0E571CD810336077A718CCDF409
AD9BD7C704E845ED17306D272A9441BB
A454BFE86F52AE3D944E2DF489A880E4

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.