SIT282/SIT703 Computer Forensics and Investigations

Workshop Session 7

In general, you have to acquire the system administrative privilege of computer in order to launch powerful programs. Hacking passwords is one of the most popular and effective methods to gain access. We will continue to use our Ubuntu VM alongside an external website in this session.

Through this session, we will practice two forensic software tools – fcrackzip and OphCrack. The knowledge acquired in this session will help you recover passwords for ZIP files and Windows systems.

Learning Objectives

1. Describe the challenges faced by digital forensic investigators when dealing with password protected files.
2. Demonstrate that you can recover encryption passwords for ZIP files.
3. Practice encrypting and decrypting files using forensic tools and techniques to recover digital evidence.
4. Identify the elements of a Windows logon password, as well as generating and recovering Windows log on hashes.

1. Introducing fcrackzip

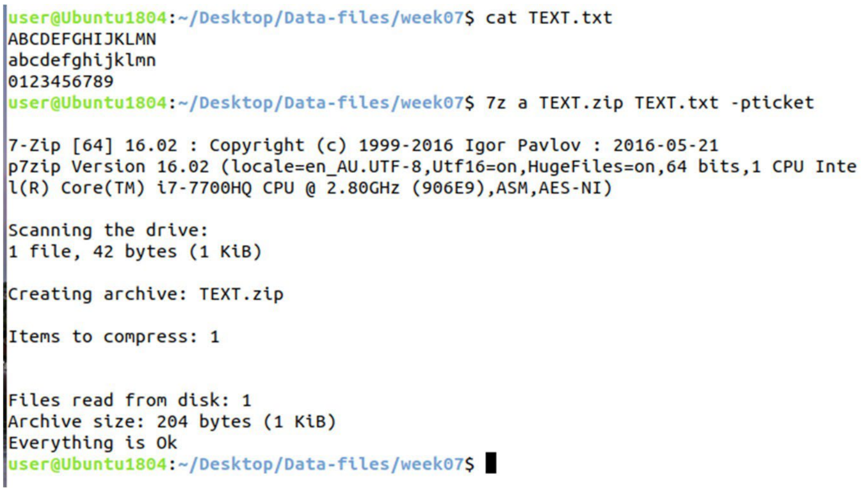
The tool fcrackzip is designed to recover the encryption passwords for ZIP files. The demo version of this program at least enables you to work on encrypted ZIP files. That is, you should be able to recover the encryption password of any ZIP file by using fcrackzip.

Note: Before we go to the next step, in case "**TEXT.zip**" already exists, delete the file by navigating to the folder using the file manager on the Ubuntu desktop or from the command line using "rm TEXT.zip" to "remove" the file.

Now, let's prepare an encrypted ZIP file. Launch the "Terminal" inside the virtual machine, change directory to "~/Desktop/Data-files/week07". In the folder, you will find a file named **TEXT.txt**. This text file contains some random text. We use the 7zip program to encrypt this file to TEXT.zip with the password "ticket".

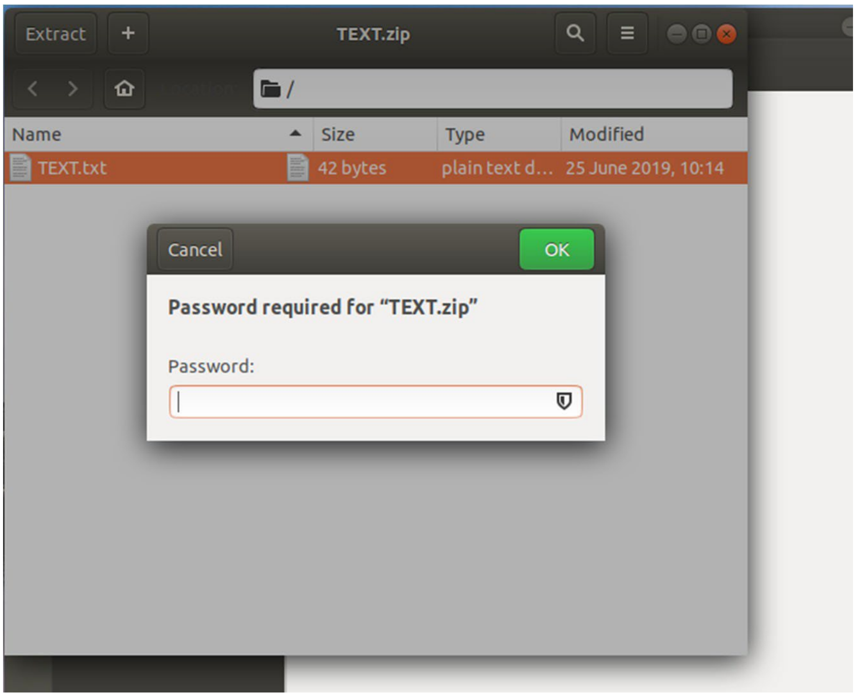
The command is "7z a TEXT.zip TEXT.txt -pticket", where:
7z – File archive program
a – Add files to archive TEXT.zip – Archive name
-p – Set password ticket – password

You will see an output similar to this.



```
user@Ubuntu1804:~/Desktop/Data-files/week07$ cat TEXT.txt
ABCDEFGHIJKLMN
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,1 CPU Inte
l(R) Core(TM) i7-7700HQ CPU @ 2.80GHz (906E9),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$ 
```

You may verify if the newly created zip file has the correct password protection. That is, navigate to the folder and double click the zip file. When a prompt appears asking for the password, input “ticket”. You should see something similar to the following screenshot. Once it is verified, you may proceed to the next step.



Name	Size	Type	Modified
TEXT.txt	42 bytes	plain text d...	25 June 2019, 10:14

Password required for “TEXT.zip”

Password:

Switch back to the Terminal, now we can use the tool fcrackzip to crack the zip password. Let’s use a simple dictionary covering potential passwords. Type the command: “**fcrackzip -u -D -p '/usr/share/dict/american-english' TEXT.zip”,** where:

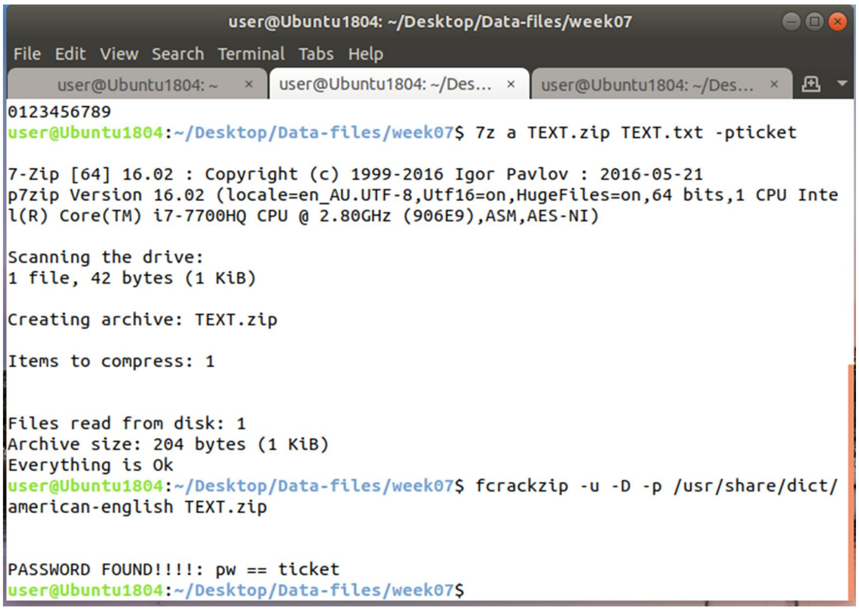
fcrackzip – Zip Password Cracker

-u – use unzip to decompress the file with guessed password

-D – dictionary mode to read passwords from a file

-p – password file

You will see the tool cracks the password correctly. (Remember to use the option “-u” to show the password, otherwise you will not see the cracked password.)


user@Ubuntu1804: ~/Desktop/Data-files/week07
File Edit View Search Terminal Tabs Help
user@Ubuntu1804: ~
user@Ubuntu1804: ~/Des...
user@Ubuntu1804: ~/Des...

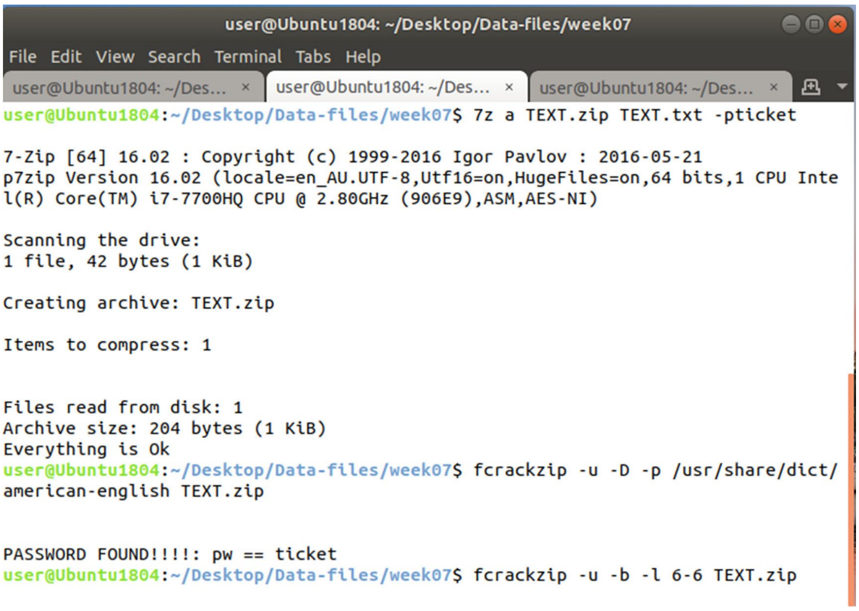
```
0123456789
user@Ubuntu1804:~/Desktop/Data-files/week07$ 7z a TEXT.zip TEXT.txt -pticket

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,1 CPU Inte
l(R) Core(TM) i7-7700HQ CPU @ 2.80GHz (906E9),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$ fcrackzip -u -D -p /usr/share/dict/
american-english TEXT.zip


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

The following is an example of dictionary attack with the option brute-force “-b” and the option cracking length “-l 6-6”.

Note: “-l” specifies the password length. It has 2 parameters: min and max; max is optional – so “6-6” means use an initial password of 6 characters in length and check all passwords up to 6 characters in length.

If the password is in the dictionary, fcrackzip can crack the password. Let us also try the brute-force attack where it applies in more general situations when you don’t have a good list of passwords. The brute-force attack will complete but will take much longer to crack the password.

Warning: This process may take quite some time (longer than 1 hour on one of our test machines).


user@Ubuntu1804: ~/Desktop/Data-files/week07
File Edit View Search Terminal Tabs Help
user@Ubuntu1804: ~/Des...
user@Ubuntu1804: ~/Des...
user@Ubuntu1804: ~/Des...

```
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,1 CPU Inte
l(R) Core(TM) i7-7700HQ CPU @ 2.80GHz (906E9),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$ fcrackzip -u -D -p /usr/share/dict/
american-english TEXT.zip


PASSWORD FOUND!!!!: pw == ticket
user@Ubuntu1804:~/Desktop/Data-files/week07$ fcrackzip -u -b -l 6-6 TEXT.zip
```

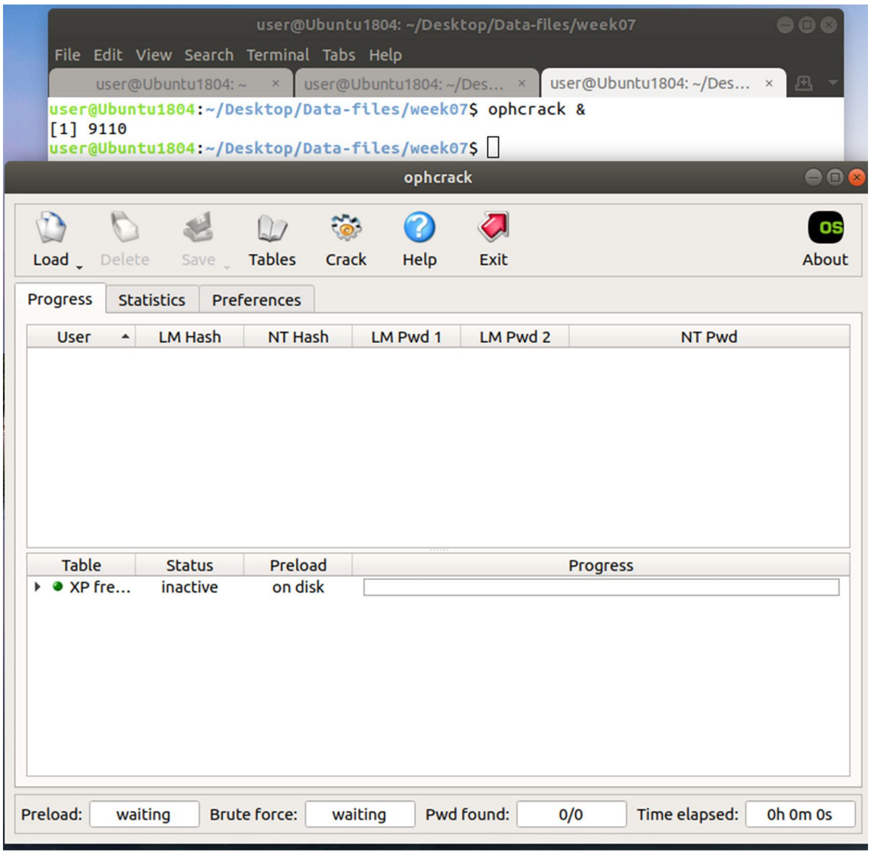
Now, use 7-zip to encrypt the same TEXT.txt file to ZIP files with the following passwords – “George”, “Eindhoven”, “augustina”, “anknytningsbarhet”. Compare the cracking time used by the tool fcrackzip. (Hint: for fast cracking, think about where to find a good list of passwords before applying the brute-force attack.)

You can use the following table to record your results.

Password	**George**	**Eindhoven**	**augustina**	**anknytningsbarhet**
Decryption Time				

2. Using OphCrack to Recover Windows Logon Password

Switch to the “Terminal” and type “ophcrack” to launch the program.



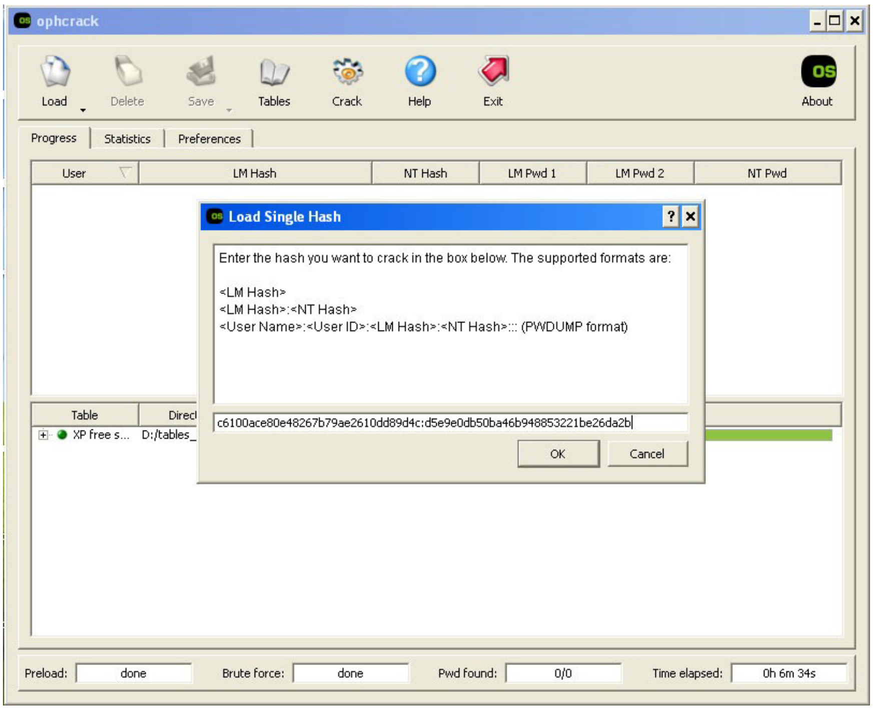
```
user@Ubuntu1804:~/Desktop/Data-files/week07$ ophcrack &
[1] 9110
user@Ubuntu1804:~/Desktop/Data-files/week07$ 
```

User	LM Hash	NT Hash	LM Pwd 1	LM Pwd 2	NT Pwd

Table	Status	Preload	Progress
XP fre…	inactive	on disk	

Preload: waiting Brute force: waiting Pwd found: 0/0 Time elapsed: 0h 0m 0s

We can verify whether ophcrack works properly by cracking an NTLM hash. Click the “Load” button and select “Single Hash” from the drop down list, then paste a testing hash value to the text box: “**c6100ace80e48267b79ae2610dd89d4c:d5e9e0db50ba46b948853221be26da2b**”



Enter the hash you want to crack in the box below. The supported formats are:

```
<LM Hash>
<LM Hash>:<NT Hash>
<User Name>:<User ID>:<LM Hash>:<NT Hash>::: (PWDUMP format)
```

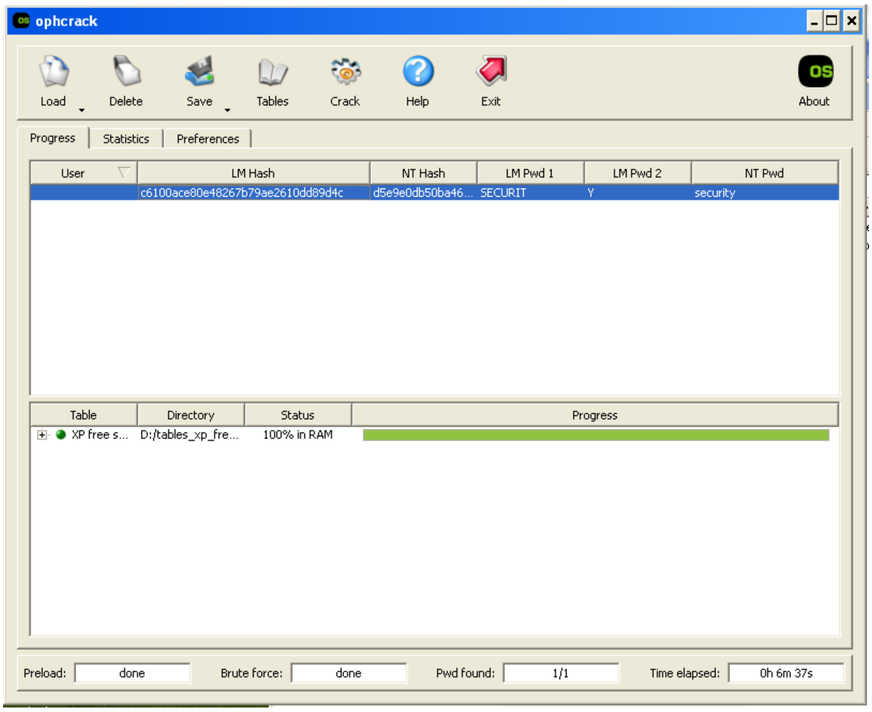
```
c6100ace80e48267b79ae2610dd89d4c:d5e9e0db50ba46b948853221be26da2b
```

User	LM Hash	NT Hash	LM Pwd 1	LM Pwd 2	NT Pwd

Table	Direct
XP free s...	D:/tables_

Preload: done   Brute force: done   Pwd found: 0/0   Time elapsed: 0h 6m 34s

Click “Ok” and then click “Crack” button from the main menu. You need to wait a few minutes before seeing any results because it normally takes a few minutes to fully load the rainbow tables in the memory. The actual cracking phase is relatively short. You can see the recovered password is actually the word “security”.



User	LM Hash	NT Hash	LM Pwd 1	LM Pwd 2	NT Pwd
	c6100ace80e48267b79ae2610dd89d4c	d5e9e0db50ba46...	SECURIT	Y	security

Table	Directory	Status	Progress
XP free s...	D:/tables_xp_fre...	100% in RAM	

Preload: done   Brute force: done   Pwd found: 1/1   Time elapsed: 0h 6m 37s

3. Forensic Tasks

Create 3 alpha-numerical passwords which are 8-characters long. Convert them to the Windows logon hashes on the website http://www.tobtu.com/lmntlm.php. (Use the "Generate Hashes" button and take the LM hash and the NT hash.) Use OphCrack to crack the passwords you just created, see how accurately the program works.

Crack the following 3 hashes by using the OphCrack program with default settings
0dbc75ca710e732c944e2df489a880e4:192c670d242fe23e0e7f3ac4061b94aa
050b44b3930b270253bac0fa79a61dc4:714b6fe38e859afb64674beb90dc69e6
732fb77c95422bc51486235a2333e4d2:89f792bbf84ea3898cf30f49d8c814e2

Record which hash cannot be cracked and why. We will discuss this in our session.
(hints: goodyear, clevermonkey93, N/A)