UNIVERSITÉ DE LORRAINE
UFR MATHÉMATIQUES INFORMATIQUE MÉCANIQUE ET AUTOMATIQUE

MASTRANTONIO CALOGERO

Network Security Project (TrueCrypt Software Study)

This report explains the use of TrueCrypt and studies its safety

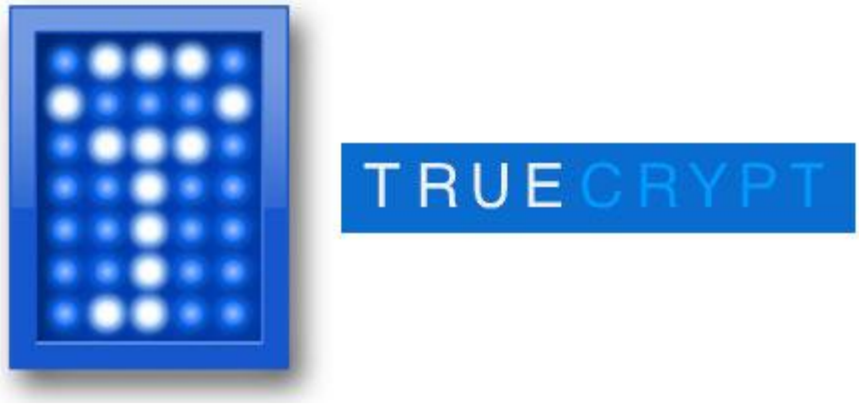


Table of Contents

Introduction 2

Developmental arrest 2

Important note 2

Choice of environment 2

- ➢ To be Linux and specifically Kali Linux 2
- ➢ To use version 7.1 TrueCrypt 3
- ➢ To use TrueCrack 3.0 4

Create an encrypted block and select options 5

- ➢ First of all choose a "slot" location 5
- ➢ Then click on "Create Volume" 5
- ➢ Leave the default choice 6
- ➢ Select the name of the encrypted block 6
- ➢ Select the encryption algorithm and the hash algorithm. 7
- ➢ Set the block size to be encrypted 8
- ➢ Creating password 9
- ➢ Format Options 9
- ➢ Volume Format 10

How to use TrueCrack attempt to find the password 11

Result 12

Conclusion 14

Introduction

TrueCrypt is a discontinued source-available freeware utility used for on-the-fly encryption (OTFE). It can create a virtual encrypted disk within a file or encrypt a partition or (under Microsoft Windows except Windows 8 with GPT) the entire storage device (pre-boot authentication).

TrueCrypt creates a virtual encrypted disk (TrueCrypt volume) contained in a file and mount it as a real physical disk. TrueCrypt can also encrypt an entire partition or device, such as a floppy disk or flash drive. Encryption is automatic, real-time and transparent.

All that will be stored in a TrueCrypt volume will be fully encrypted, including file names and directories. The TrueCrypt volumes behave, once installed, as physical hard drives.

Developmental arrest

On 28 May 2014, the TrueCrypt website announced that the project was no longer maintained and recommended users to find alternative solutions.

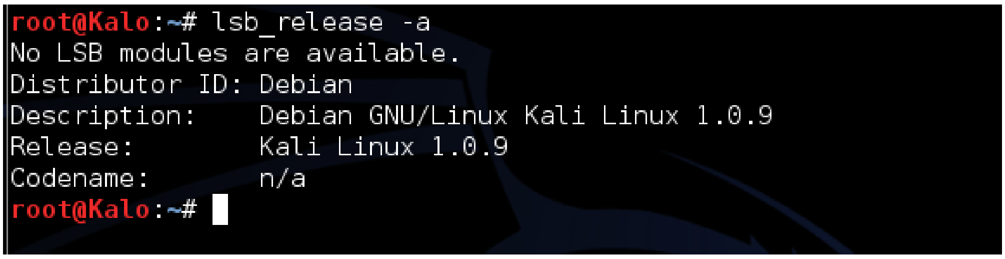
Important note

Despite the controversy that this has caused and until proven otherwise, TrueCrypt is always reliable. Here we do not ask if TrueCrypt is corrupted or not, the goal is to evaluate the software for what it is, that is to say encrypt (a disk portion, flash drive, etc...) to protect information.

Choice of environment

To work on my subject I decided:

- To be Linux and specifically Kali Linux

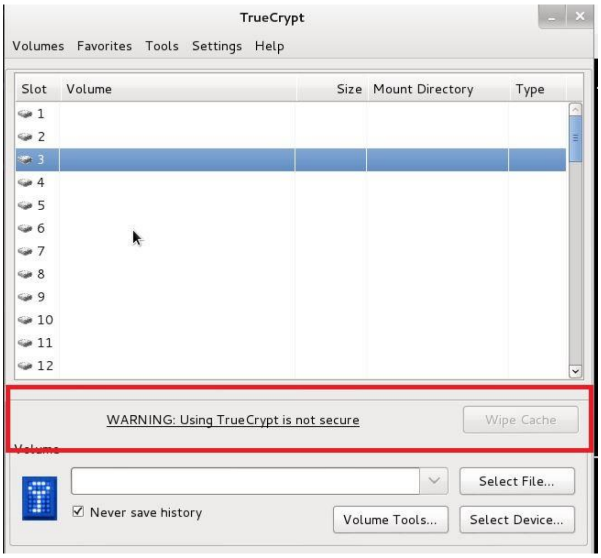


```
root@Kalo:~# lsb_release -a
No LSB modules are available.
Distributor ID: Debian
Description:    Debian GNU/Linux Kali Linux 1.0.9
Release:        Kali Linux 1.0.9
Codename:       n/a
root@Kalo:~# 
```

To my TrueCrypt tests I needed to be on Linux and the fact of using Linux Kali was great because the additional software I was using "TrueCrack" was already installed base.

➢ To use version 7.1 TrueCrypt

There is a version 7.2 (the latest), but it (Linux) does not allow me to create partitions

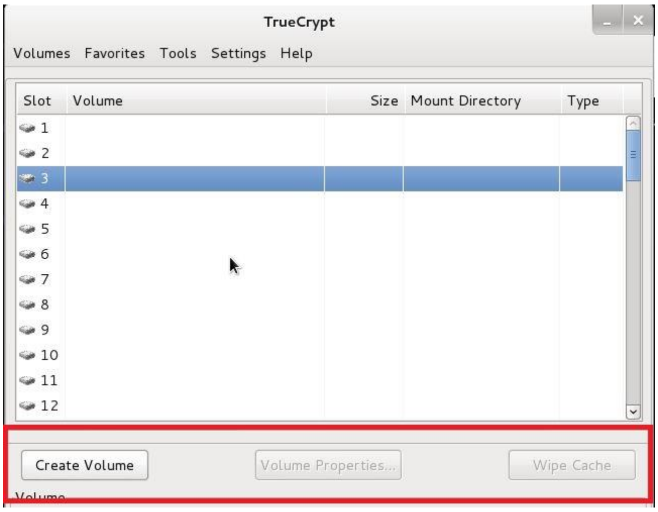


Slot	Volume	Size	Mount Directory	Type
1				
2				
3				
4				
5				
6				
7				
8				
9				
10				
11				
12				

WARNING: Using TrueCrypt is not secure

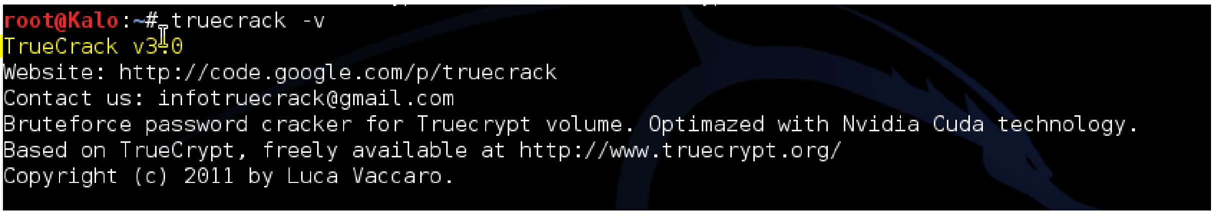
☑ Never save history

7.1 can be.



Slot	Volume	Size	Mount Directory	Type
1				
2				
3				
4				
5				
6				
7				
8				
9				
10				
11				
12				

- To use TrueCrack 3.0



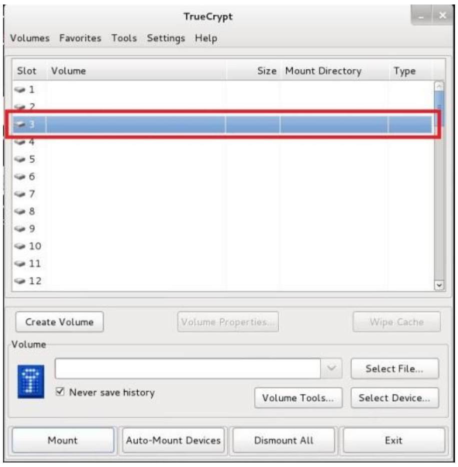
```
root@Kalo:~# truecrack -v
TrueCrack v3.0
Website: http://code.google.com/p/truecrack
Contact us: infotruecrack@gmail.com
Bruteforce password cracker for Truecrypt volume. Optimazed with Nvidia Cuda technology.
Based on TrueCrypt, freely available at http://www.truecrypt.org/
Copyright (c) 2011 by Luca Vaccaro.
```

TrueCrack allows cracking passwords. The application uses a brute-force method to try to find the password on a dictionary. There is no particular reason to use this version, but as it is already installed on my Linux and it is perfect there was no reason to change.

Create an encrypted block and select options

For a better understanding and ease of writing I will explain how to mount an encrypted block with the range of options that I will present to avoid redundancy in this report.

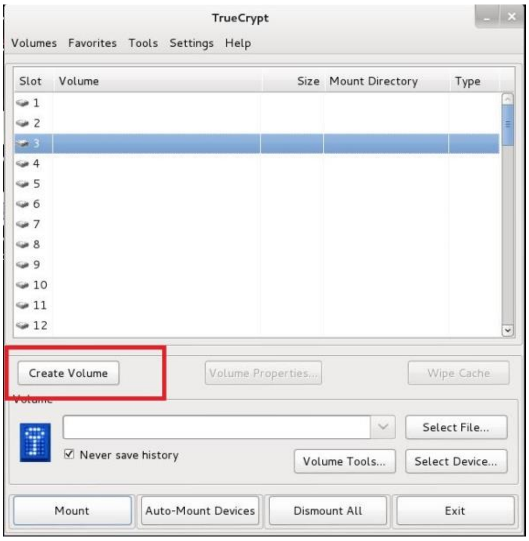
- **First of all choose a "slot" location**



☑ Never save history

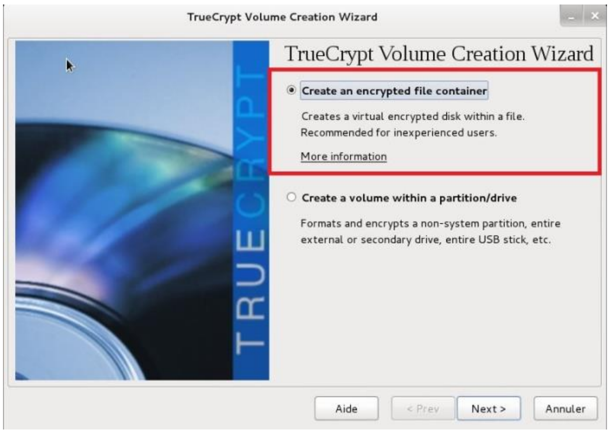
(The choice of the number does not matter)

- **Then click on "Create Volume"**



☑ Never save history

- **Leave the default choice**



TrueCrypt Volume Creation Wizard

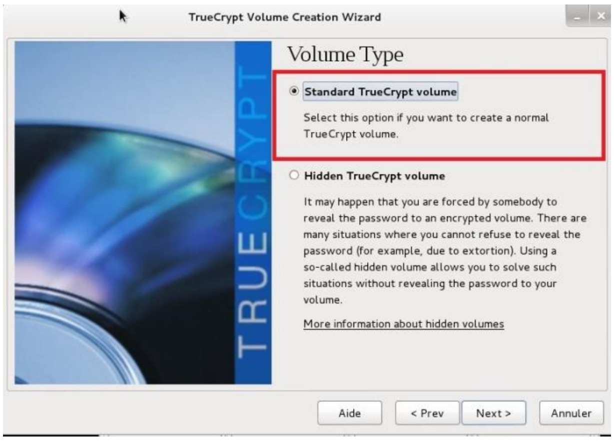
● Create an encrypted file container

Creates a virtual encrypted disk within a file. Recommended for inexperienced users.

More information

○ Create a volume within a partition/drive

Formats and encrypts a non-system partition, entire external or secondary drive, entire USB stick, etc.



Volume Type

● Standard TrueCrypt volume

Select this option if you want to create a normal TrueCrypt volume.

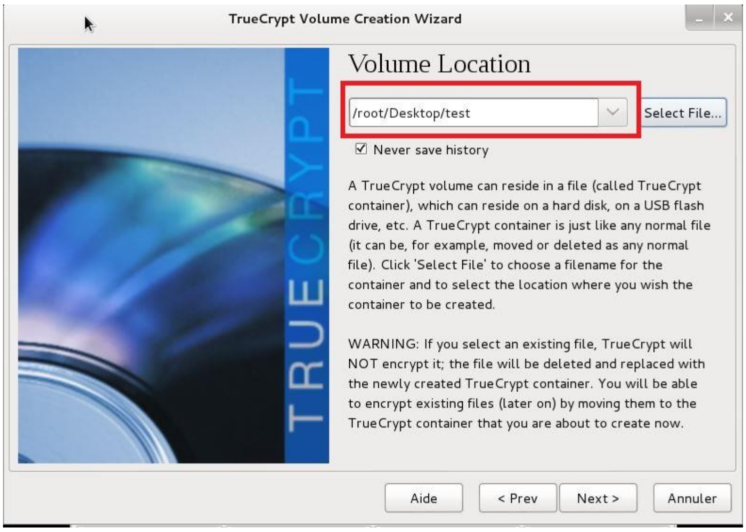
○ Hidden TrueCrypt volume

It may happen that you are forced by somebody to reveal the password to an encrypted volume. There are many situations where you cannot refuse to reveal the password (for example, due to extortion). Using a so-called hidden volume allows you to solve such situations without revealing the password to your volume.

More information about hidden volumes

- **Select the name of the encrypted block**

You have to give the way, with the last word as the name of the encrypted block.



Volume Location

/root/Desktop/test

☑ Never save history

A TrueCrypt volume can reside in a file (called TrueCrypt container), which can reside on a hard disk, on a USB flash drive, etc. A TrueCrypt container is just like any normal file (it can be, for example, moved or deleted as any normal file). Click 'Select File' to choose a filename for the container and to select the location where you wish the container to be created.

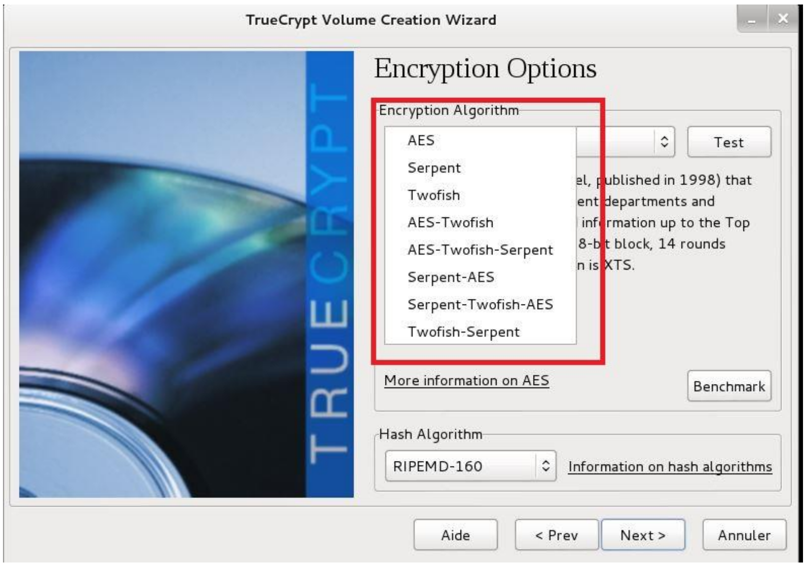
WARNING: If you select an existing file, TrueCrypt will NOT encrypt it; the file will be deleted and replaced with the newly created TrueCrypt container. You will be able to encrypt existing files (later on) by moving them to the TrueCrypt container that you are about to create now.

➢ Select the encryption algorithm and the hash algorithm.

For my project it is here that the choices will be made and studied. Indeed we will compare the algorithm types and types of hash to see if a given password, it is better to focus a choice over another.

TrueCrypt gives us a choice of 8 algorithms to encrypt:

- AES
- Serpent
- Twofish
- AES-Twofish
- AES-Twofish-Serpent
- Serpent-AES
- Serpent-Twofish-AES
- Twofish-Serpent



TrueCrypt Volume Creation Wizard

Encryption Options

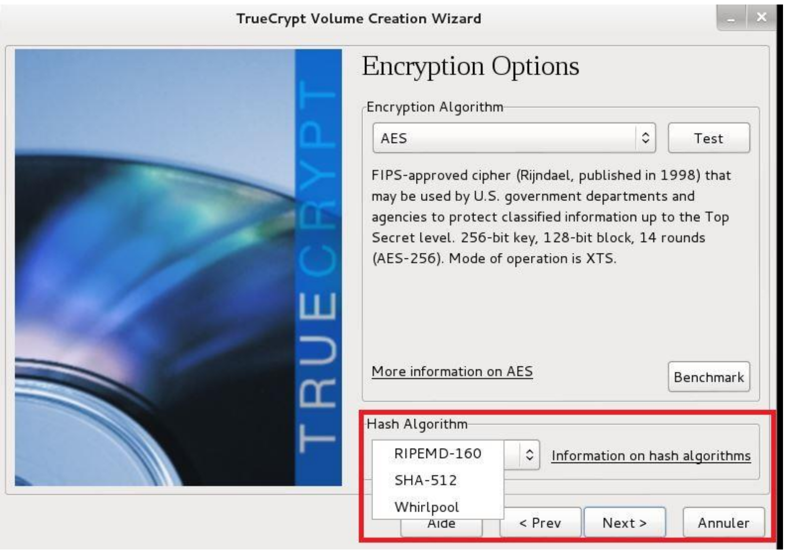
Encryption Algorithm: AES, Serpent, Twofish, AES-Twofish, AES-Twofish-Serpent, Serpent-AES, Serpent-Twofish-AES, Twofish-Serpent

el, published in 1998) that ent departments and information up to the Top 8-bit block, 14 rounds n is XTS.

Hash Algorithm: RIPEMD-160

And 3 algorithms for hashing:

- RIPEMD-160
- SHA-512
- Whirlpool



TrueCrypt Volume Creation Wizard

Encryption Options

Encryption Algorithm: AES

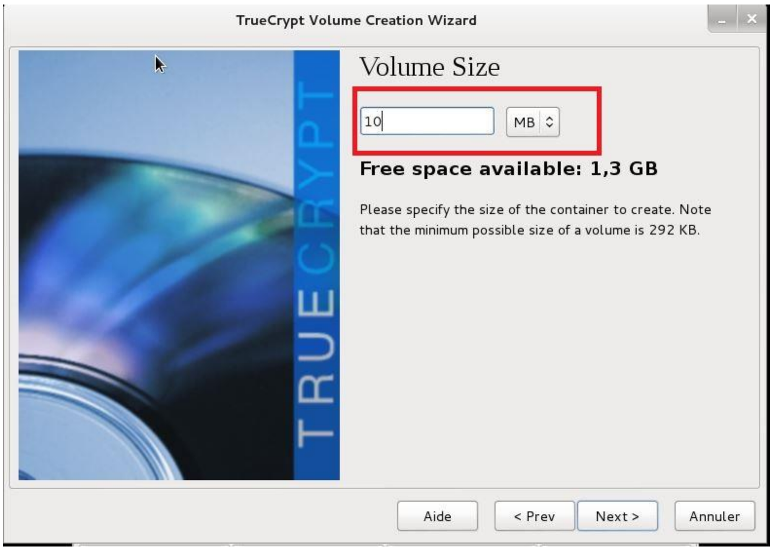
FIPS-approved cipher (Rijndael, published in 1998) that may be used by U.S. government departments and agencies to protect classified information up to the Top Secret level. 256-bit key, 128-bit block, 14 rounds (AES-256). Mode of operation is XTS.

Hash Algorithm: RIPEMD-160

To finish the tutorial I chose AES and RIPEMD-160 (click next to proceed to the next step)

➢ Set the block size to be encrypted

Insert the desired number and choose size between KB, MB, and GB



TrueCrypt Volume Creation Wizard

Volume Size

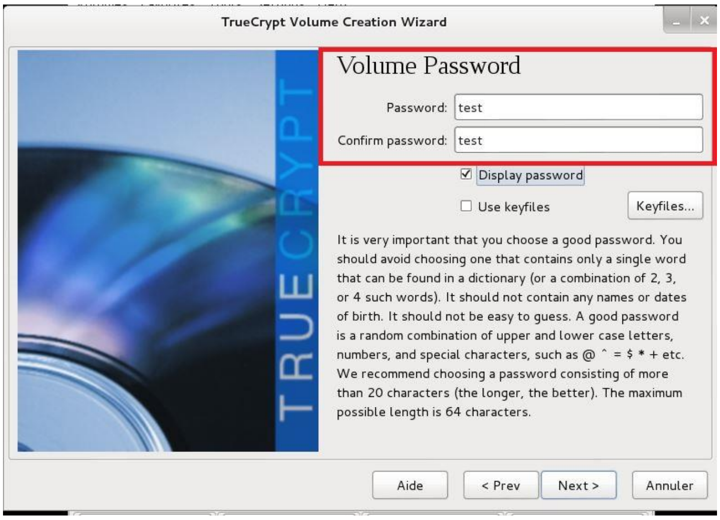
10 MB

Free space available: 1,3 GB

Please specify the size of the container to create. Note that the minimum possible size of a volume is 292 KB.

➢ Creating password

Choosing a good password is very important.



TrueCrypt Volume Creation Wizard

Volume Password

Password: test

Confirm password: test

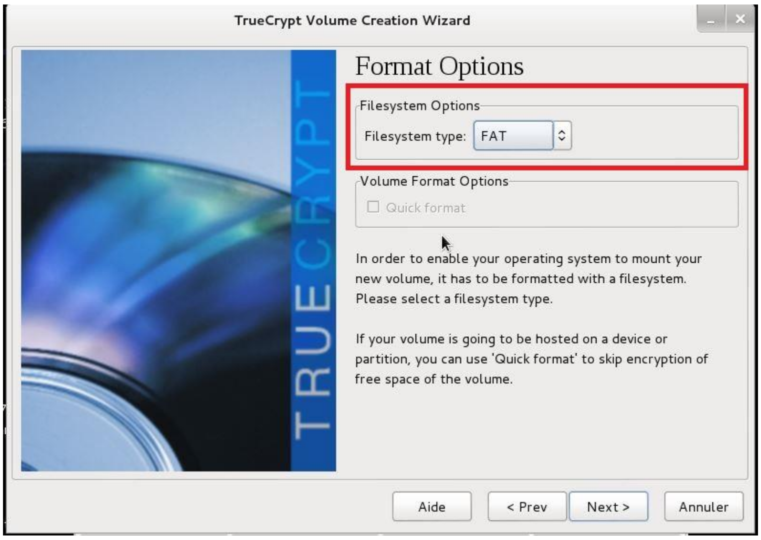
☑ Display password

□ Use keyfiles

It is very important that you choose a good password. You should avoid choosing one that contains only a single word that can be found in a dictionary (or a combination of 2, 3, or 4 such words). It should not contain any names or dates of birth. It should not be easy to guess. A good password is a random combination of upper and lower case letters, numbers, and special characters, such as @ ^ = $ * + etc. We recommend choosing a password consisting of more than 20 characters (the longer, the better). The maximum possible length is 64 characters.

➢ Format Options

Choose the default (FAT) is the most used.



TrueCrypt Volume Creation Wizard

Format Options

Filesystem Options

Filesystem type: FAT

Volume Format Options

□ Quick format

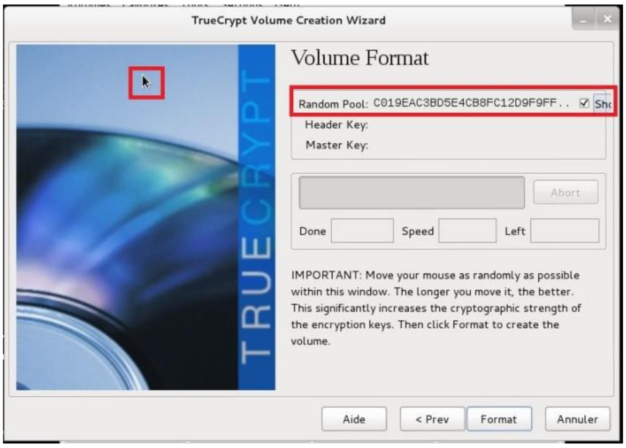
In order to enable your operating system to mount your new volume, it has to be formatted with a filesystem. Please select a filesystem type.

If your volume is going to be hosted on a device or partition, you can use 'Quick format' to skip encryption of free space of the volume.

Volume Format

Move the mouse randomly allows making harder vulnerable cryptography.

So the more you move the better mouse will be the result.



TrueCrypt Volume Creation Wizard

Volume Format

Random Pool: C019EAC3BD5E4CB8FC12D9F9FF.. ☑ Sho

Header Key:

Master Key:

Done Speed Left

IMPORTANT: Move your mouse as randomly as possible within this window. The longer you move it, the better. This significantly increases the cryptographic strength of the encryption keys. Then click Format to create the volume.

This is creating an encrypted block is completed.

How to use TrueCrack attempt to find the password

To use TrueCrack must be 2 things. Knowing the way encrypted block and have a dictionary attack.

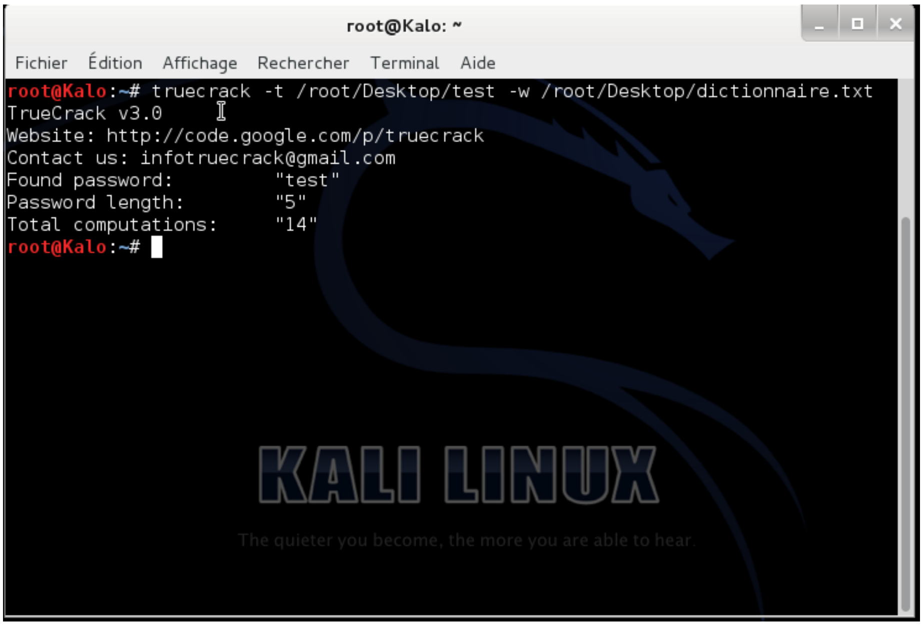
The -t let's say that this is an encrypted TrueCrypt block

The -w let's say we use the dictionary attack

The path that ends with /test is the path of the encrypted block.

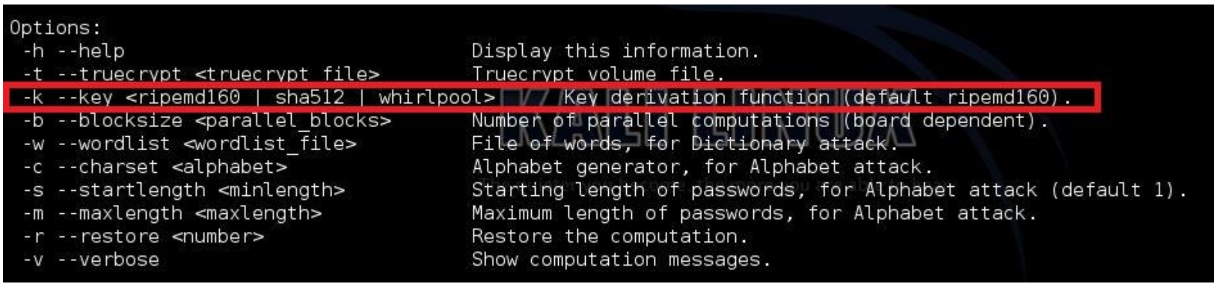
The path ends with /Dictionnaire is the way the dictionary.

In this example TrueCrack find the password.



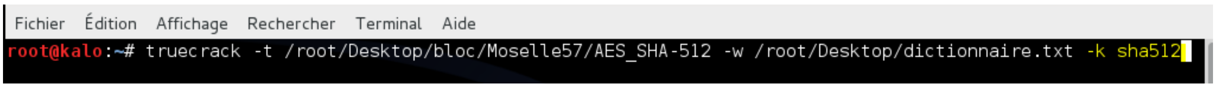
```
root@Kalo:~# truecrack -t /root/Desktop/test -w /root/Desktop/dictionnaire.txt
TrueCrack v3.0
Website: http://code.google.com/p/truecrack
Contact us: infotruecrack@gmail.com
Found password:         "test"
Password length:        "5"
Total computations:     "14"
root@Kalo:~#
```

The -k allows us to test based on the hash we want.



```
Options:
 -h --help                             Display this information.
 -t --truecrypt <truecrypt_file>       Truecrypt volume file.
 -k --key <ripemd160 | sha512 | whirlpool>   Key derivation function (default ripemd160).
 -b --blocksize <parallel_blocks>      Number of parallel computations (board dependent).
 -w --wordlist <wordlist_file>         File of words, for Dictionary attack.
 -c --charset <alphabet>               Alphabet generator, for Alphabet attack.
 -s --startlength <minlength>          Starting length of passwords, for Alphabet attack (default 1).
 -m --maxlength <maxlength>            Maximum length of passwords, for Alphabet attack.
 -r --restore <number>                 Restore the computation.
 -v --verbose                          Show computation messages.
```

Example: We test indicating the SHA512 hash algorithm as option



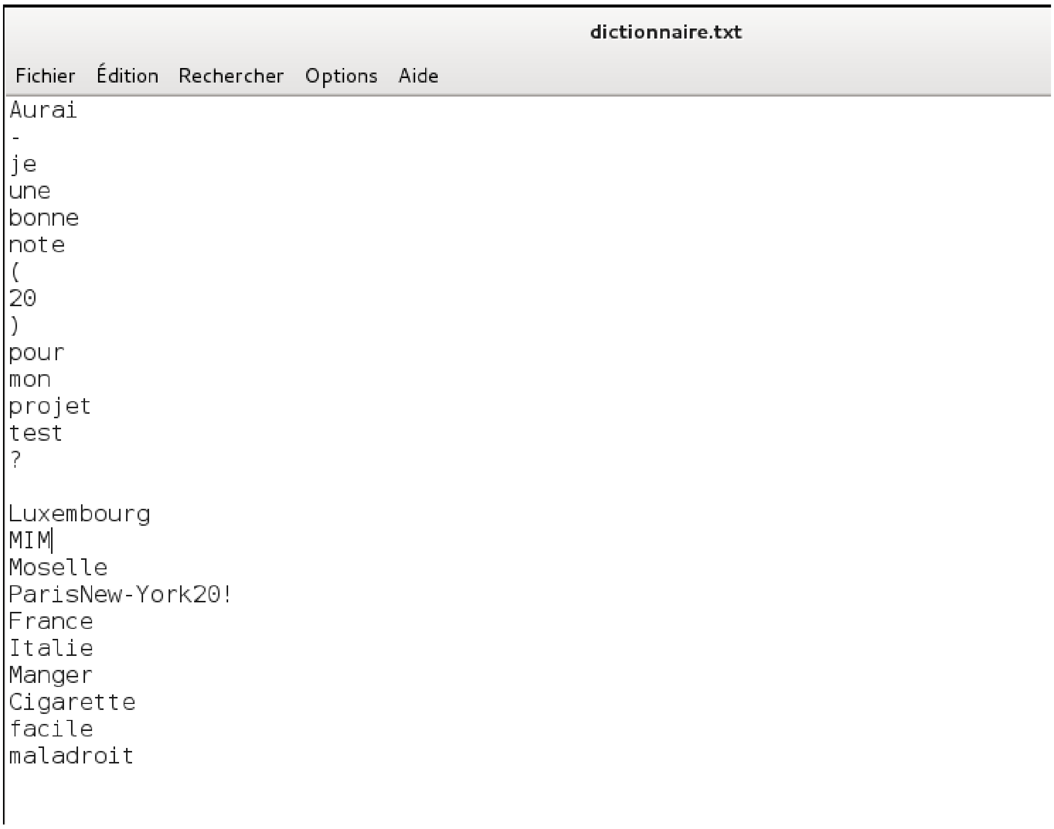
```
root@kalo:~# truecrack -t /root/Desktop/bloc/Moselle57/AES_SHA-512 -w /root/Desktop/dictionnaire.txt -k sha512
```

Result

As mentioned earlier in the report, TrueCrypt gives us a choice of 8 encryption algorithms and 3 for hashing.

Is all algorithms for password dictionaries are given equivalent?

Here are the words to my dictionary (dictionnaire.txt) that will be used:



```
Aurai
-
je
une
bonne
note
(
20
)
pour
mon
projet
test
?

Luxembourg
MIM
Moselle
ParisNew-York20!
France
Italie
Manger
Cigarette
facile
maladroit
```

Note: The password is in the dictionary this is voluntary

🟩 **Password found**

🟥 **Password Not Found**

▨ **Not tested (explanation in the conclusion)**

The algorithm used	Password used					
Encryption_Hash	test	test123	Moselle	Moselle57	ParisNew-York20!	Los-AngelesTokyo10?
AES_RIPEMD-160	🟩	🟥	🟩	🟥	🟩	🟥
Serpent_RIPEMD-160	🟥	▨	▨	▨	▨	▨
Twofish_RIPEMD-160	🟥	▨	▨	▨	▨	▨
AES-Twofish_RIPEMD-160	🟥	▨	▨	▨	▨	▨
AES-Twofish-Serpent_RIPEMD-160	🟥	▨	▨	▨	▨	▨
Serpent-AES_RIPEMD-160	🟥	▨	▨	▨	▨	▨
Serpent-Twofish-AES_RIPEMD-160	🟥	▨	▨	▨	▨	▨
Twofish-Serpent_RIPEMD-160	🟥	▨	▨	▨	▨	▨
AES_SHA-512	🟩	🟥	🟩	🟥	🟩	🟥
Serpent_SHA-512	🟥	▨	▨	▨	▨	▨
Twofish_SHA-512	🟥	▨	▨	▨	▨	▨
AES-Twofish_SHA-512	🟥	▨	▨	▨	▨	▨
AES-Twofish-Serpent_SHA-512	🟥	▨	▨	▨	▨	▨
Serpent-AES_SHA-512	🟥	▨	▨	▨	▨	▨
Serpent-Twofish-AES_SHA-512	🟥	▨	▨	▨	▨	▨
Twofish-Serpent_SHA-512	🟥	▨	▨	▨	▨	▨
AES_Whirlpool	🟩	🟥	🟩	🟥	🟩	🟥
Serpent_Whirlpool	🟥	▨	▨	▨	▨	▨
Twofish_Whirlpool	🟥	▨	▨	▨	▨	▨
AES-Twofish_Whirlpool	🟥	▨	▨	▨	▨	▨
AES-Twofish-Serpent_Whirlpool	🟥	▨	▨	▨	▨	▨
Serpent-AES_Whirlpool	🟥	▨	▨	▨	▨	▨
Serpent-Twofish-AES_Whirlpool	🟥	▨	▨	▨	▨	▨
Twofish-Serpent_Whirlpool	🟥	▨	▨	▨	▨	▨

Conclusion

As we can see the same factors come back when the password is found:

- The password is in the dictionary
- The encryption algorithm is AES

So for my tests all algorithms are equivalent except AES.

For hash algorithms are all equivalent

The version of TrueCrack used allows us to choose the hash but not the encryption algorithm to try to find the password.

Only the AES algorithm is considered so after a first test with other algorithms it was unnecessary to test with stronger passwords, this is unnecessary TrueCrack would not have found it.

There is another version of TrueCrack (or extension) that is used to add the option of selecting the encryption algorithm.

After several tests on my computer I did not manage to install another version or extension, but the principle and the result of my conclusion would be the same.

With a version of TrueCrack with the option of choosing encryption algorithm (-e) all algorithms become equivalent (unlike my tests when AES was avoided).

If the option allows to select a preferred algorithm, then an algorithm of choice that combines several encryption algorithms (AES-Twofish-Serpent, for example), to protect themselves from attack.

So if TrueCrack knows the encryption algorithm and the hash algorithm and the password is in the dictionary used the password is found.

Test what combination of the encryption algorithm and hash algorithm does not hurt the attacker (8 * 3 = 24 combinations)

(In my tests 1 * 3 + AES as a hash of choice)

To protect themselves from the attack you have a password that is not in the dictionary.

The goal here is not to give a course on how to choose a good password, but here are some tips:

- Choose a good length (10 characters minimum)
- A suite of character with lowercase, uppercase, number and special character (-, $…)
- No word from a dictionary
- Do not choose something easily guessable

My tip to remember a good password: Choose a phrase and take the first letter of each word, alternating upper and lower case.

Example: Seriously what do you think of my report it is 20/20?

Password: SwDyToMrIi20?

TrueCrack was considered one of the best software to encrypt its data (still without speaking of the debate if it is compromised or not from the start)

With the correct password for this software security is very good.

Source definitions: wikipedia.en