



UNIVERSITÉ  
DE LORRAINE

UFR MATHÉMATIQUES INFORMATIQUE  
MÉCANIQUE ET AUTOMATIQUE

MASTRANTONIO  
CALOGERO

## Projet Sécurité des réseaux (Etude du logiciel TrueCrypt)

Ce rapport a pour but d'expliquer l'utilisation de TrueCrypt et d'étudier sa sécurité



TRUECRYPT

## Table des matières

Introduction.....	2
Arrêt du développement.....	2
Note importante.....	3
Choix de l'environnement .....	3
➤ D'être sous Linux et plus précisément Kali Linux .....	3
➤ D'utiliser la version 7.1 de TrueCrypt .....	4
➤ D'utiliser TrueCrack 3.0 .....	5
Créer un bloc chiffré et choisir les options.....	6
➤ Tout d'abord choisir un emplacement « slot » .....	6
➤ Cliquer ensuite sur « Create Volume ».....	6
➤ Pour une utilisation standard et rapide, laisser les choix par défaut.....	7
➤ Choisir le nom du bloc chiffré.....	7
➤ Choisir l'algorithme d'encryptions ainsi que le hash de l'algorithme. ....	8
➤ Définir la taille du bloc à chiffrer .....	9
➤ Création du mot de passe .....	10
➤ Format Options.....	10
➤ Volume Format.....	11
Comment utiliser TrueCrack pour tenter de trouver le mot de passe.....	12
Résultat.....	13
Conclusion .....	15

## Introduction

TrueCrypt est à la fois un format de système de fichier chiffré, notamment géré par Linux dans son module dm-crypt depuis la version 3, est un logiciel de chiffrement à la volée fonctionnant sur Microsoft Windows XP/2000/2003/Vista /7/8, Mac OS X et GNU/Linux, ce dernier étant à l'origine de ce système de fichier.

TrueCrypt est gratuit et son code source est disponible bien qu'il n'ait pas le statut de logiciel libre. Le logiciel tc-play, pour Linux, est par contre un logiciel libre sous Licence BSD, dont la version 1.0 est sortie en mai 2013 et est compatible avec TrueCrypt.

TrueCrypt permet de créer un disque virtuel chiffré (volume TrueCrypt) contenu dans un fichier et de le monter comme un disque physique réel. TrueCrypt peut aussi chiffrer une partition entière ou un périphérique, par exemple une disquette ou une clé USB. Le chiffrement est automatique, en temps réel et transparent.

Tout ce qui sera stocké dans un volume TrueCrypt sera entièrement chiffré, y compris noms de fichiers et répertoires. Les volumes TrueCrypt se comportent, une fois montés, comme des disques durs physiques.

## Arrêt du développement

Le 28 mai 2014, le site officiel de TrueCrypt annonce la fin du développement en prétextant la fin du support de Windows XP par Microsoft. Il affirme par ailleurs que le logiciel est compromis et demande d'utiliser à la place le logiciel commercial BitLocker de Microsoft, pourtant connu pour fournir des portes dérobées aux services de renseignement et ne permettant pas une interopérabilité (ne fonctionnant que sous Windows) comme le permet TrueCrypt. Le site web renvoie vers la version 7.2 qui révèle, après un audit rapide par la communauté informatique, qu'il est impossible de chiffrer de nouvelles données, tout en signalant par une fenêtre surgissant que TrueCrypt est compromis. La communauté informatique soupçonne que les développeurs ont été piratés ou ont été contactés par les services de renseignement.

Selon Gibson Research Corporation (en), les développeurs anonymes de TrueCrypt n'ont pas souhaité poursuivre le développement après une dizaine d'années consacrées au sujet, car "il n'y avait plus d'intérêt" à sa poursuite<sup>11</sup>. Le projet initial visait à l'époque à combler le manque d'outil de chiffrement en standard sur Windows XP.

## Note importante

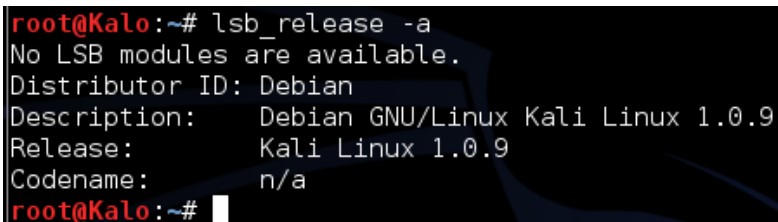
Malgré le bruit que tout cela a provoqué, et jusqu'à preuve du contraire, TrueCrypt est toujours fiable.

Ici on ne se pose pas la question si TrueCrypt est corrompu ou pas, le but est d'évaluer le logiciel pour ce pour quoi il existe, c'est-à-dire chiffrer (une partie de disque, clé USB, etc...) pour protéger l'information.

## Choix de l'environnement

Pour travailler sur mon sujet j'ai décidé :

- D'être sous Linux et plus précisément Kali Linux

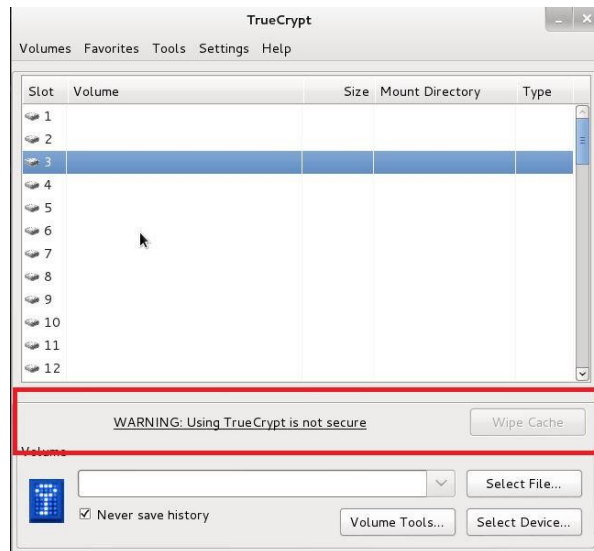
A terminal window with a dark background and a Kali Linux logo. The text shows the command 'lsb\_release -a' being executed, resulting in the following output:

```
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:~#
```

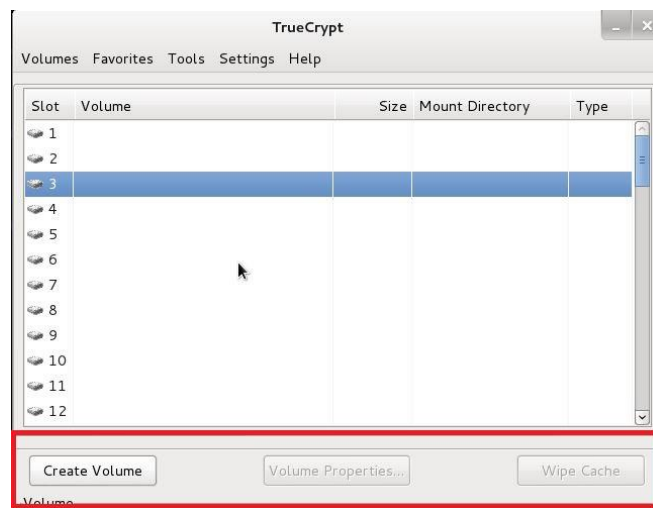
Pour faire mes tests sur TrueCrypt j'avais besoin d'être sous Linux et le fait d'utiliser Kali Linux était pratique car le logiciel complémentaire que j'utilisais « TrueCrack » était déjà installé de base.

➤ D'utiliser la version 7.1 de TrueCrypt

Il existe une version 7.2 (la dernière) mais cette dernière (sous linux) ne me permet pas de créer des partitions



Alors que la 7.1 oui.



### ➤ D'utiliser 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. Optimized with Nvidia Cuda technology.
Based on TrueCrypt, freely available at http://www.truecrypt.org/
Copyright (c) 2011 by Luca Vaccaro.
```

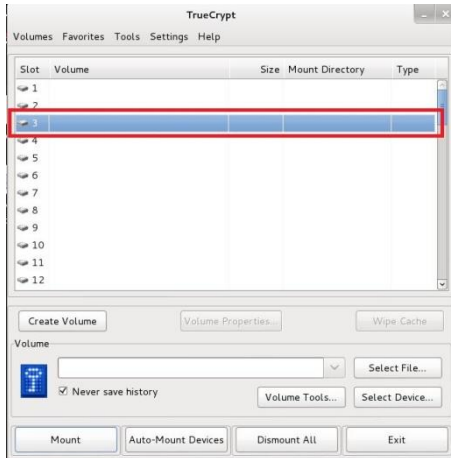
TrueCrack permet de cracker les mots de passe de TrueCrypt. L'application utilise une méthode de brute-force pour tenter de retrouver le mot de passe sur une base de dictionnaire. TrueCrack est optimisé CUDA et supporte donc les GPU nVidia. Cela offre ainsi une puissance de calcul décuplée réduisant la phase de recherche d'un facteur de 20 selon la complexité du mot de passe.

Il n'y a pas de raison particulière d'utiliser cette version, mais comme elle est déjà installée de base sur mon Kali Linux et qu'elle convient parfaitement il n'y avait aucune raison de la changer.

## Créer un bloc chiffré et choisir les options

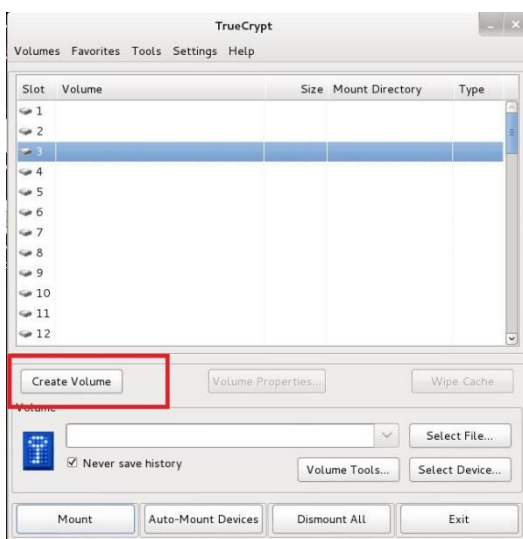
Pour une meilleure compréhension et une facilité d'écriture je vais expliquer comment monter un bloc chiffré avec les choix d'options que je vais présenter pour éviter une redondance dans ce rapport.

### ➤ **Tout d'abord choisir un emplacement « slot »**



(Le choix du numéro n'a aucune importance)

### ➤ **Cliquer ensuite sur « Create Volume »**

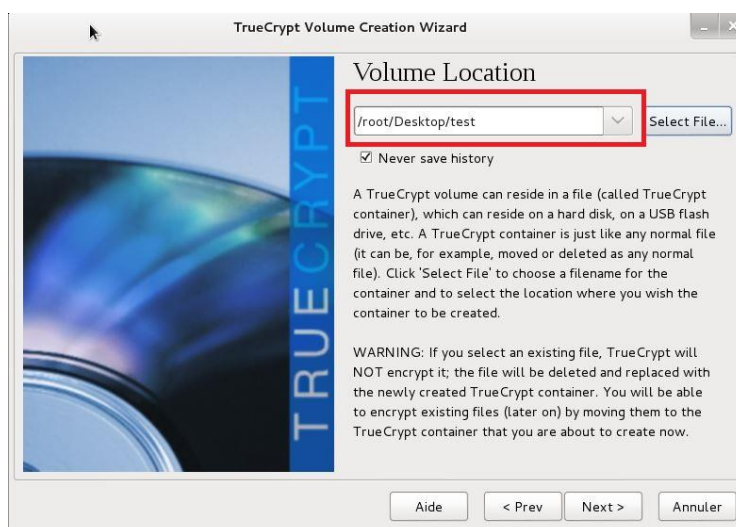


- Pour une utilisation standard et rapide, laisser les choix par défaut



- Choisir le nom du bloc chiffré

Il faut donner le chemin du bloc, avec le dernier mot comme nom du bloc chiffré.



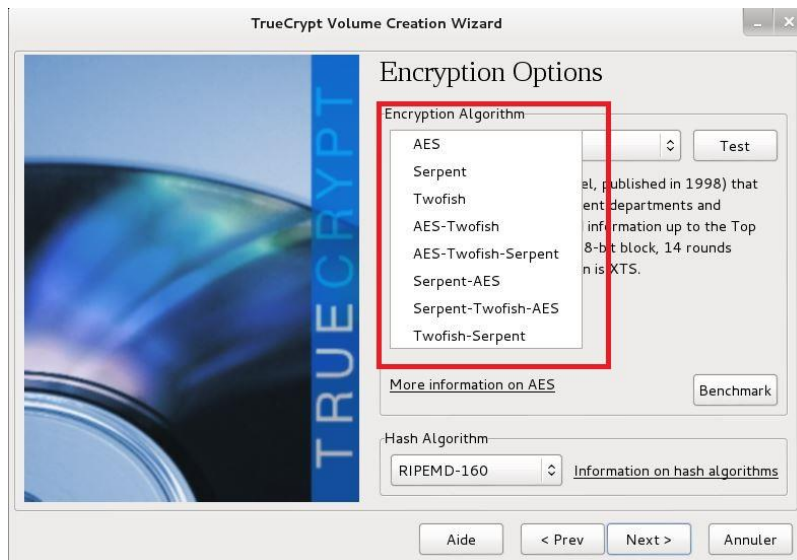


➤ Choisir l'algorithme d'encryptions ainsi que le hash de l'algorithme.

Pour notre projet c'est ici que les choix seront effectués et étudiés. En effet nous allons comparer les types d'algorithme et les types de hash pour voir si pour un mot de passe donné, il vaut mieux privilégier un choix plutôt qu'un autre.

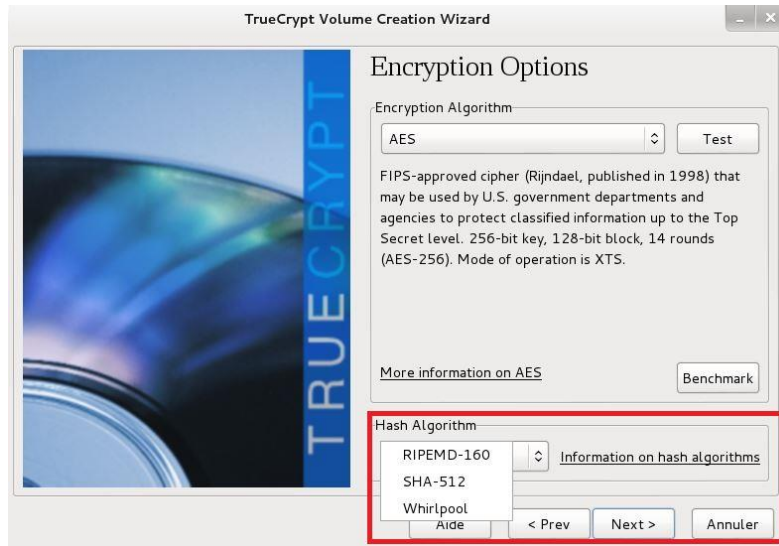
TrueCrypt nous donne le choix entre 8 choix d'algorithme pour encrypter

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



Et 3 algorithmes pour hacher.

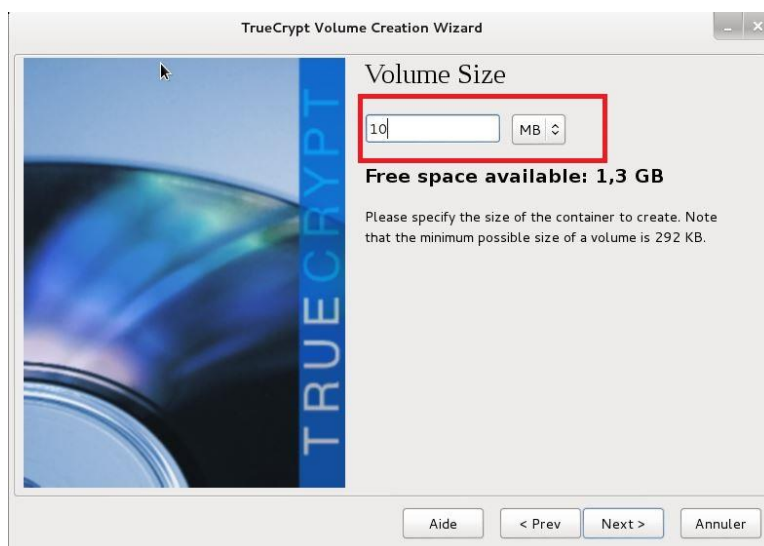
- RIPEMD-160
- SHA-512
- Whirlpool



Pour finir le tutoriel je choisis AES et RIPEMD-160 (cliquer sur next pour passer à l'étape suivante)

### ➤ Définir la taille du bloc à chiffrer

Insérer le chiffre désiré puis choisir la taille entre KB, MB, GB



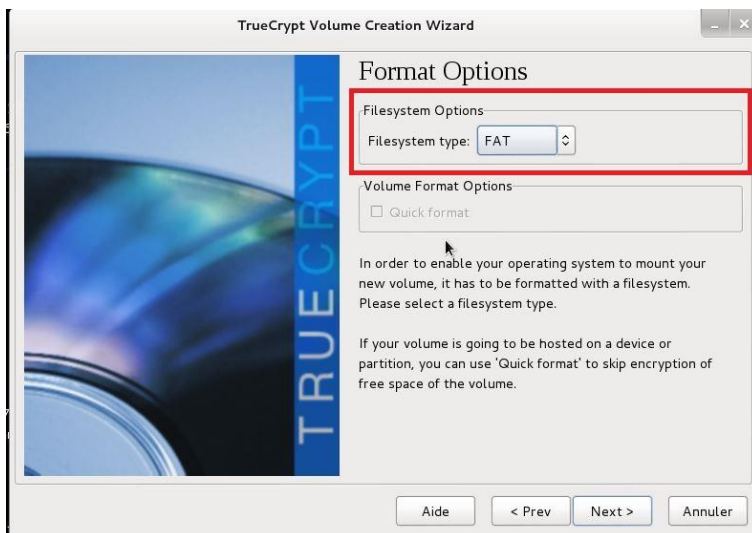
## ➤ Création du mot de passe

Le choix d'un bon mot de passe est très important.



## ➤ Format Options

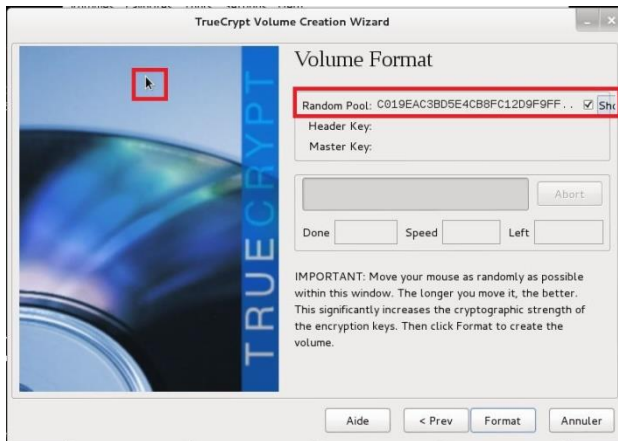
Choisir celle par défaut (FAT) c'est la plus utilisé.



## ➤ Volume Format

Bouger la souris aléatoirement permet de rendre la cryptographie plus difficilement vulnérable.

Donc plus on bouge la souris meilleur sera le résultat.



Voilà la création d'un bloc chiffré est terminée.

## Comment utiliser TrueCrack pour tenter de trouver le mot de passe

Pour utiliser TrueCrack il faut 2 choses. Connaitre le chemin du bloc chiffré et avoir un dictionnaire d'attaque.

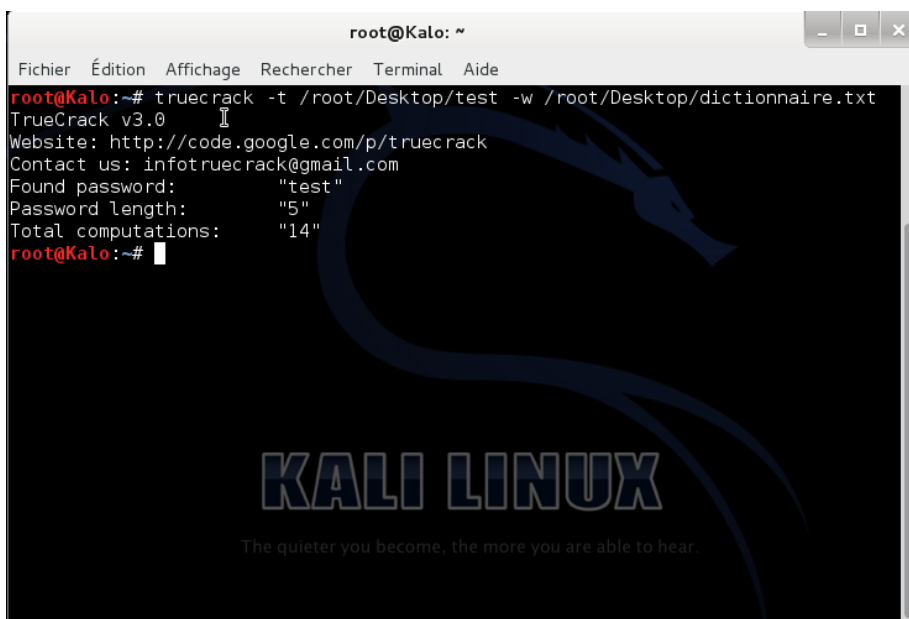
Le `-t` permet de dire qu'il s'agit d'un bloc chiffré par TrueCrypt

Le `-w` permet de dire qu'on utilise l'attaque par dictionnaire

Le chemin qui se termine par `/test` est le chemin du bloc chiffré.

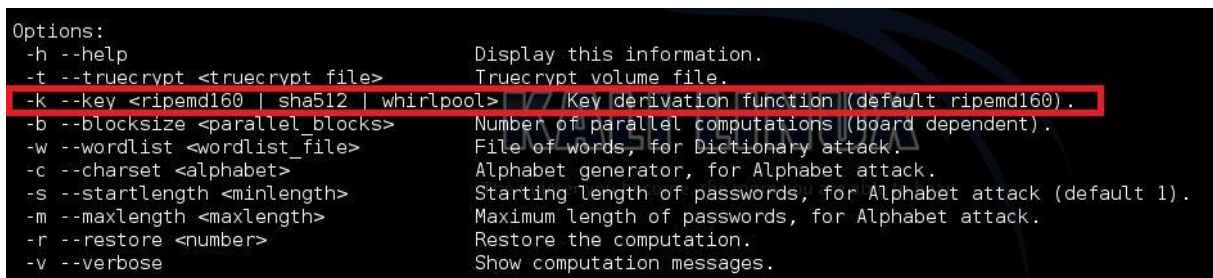
Le chemin qui se termine par `/dictionnaire` est le chemin du dictionnaire.

Dans cet exemple TrueCrack trouve le mot de passe.



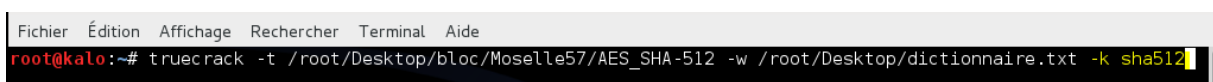
```
root@Kalo: ~
Fichier  Édition  Affichage  Recherche  Terminal  Aide
root@Kalo:~# truecrack -t /root/Desktop/test -w /root/Desktop/dictionnaire.txt
TrueCrack v3.0
Website: http://code.google.com/p/truecrack
Contact us: infotruetrack@gmail.com
Found password: "test"
Password length: "5"
Total computations: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

Le `-k` nous permet de tester en fonction du hash que nous voulons.



```
Options:
-h --help                Display this information.
-t --truecrypt <truecrypt file> Truecrypt volume file.
-k --key <riplemd160 | 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.
```

Exemple : on test en précisant l'option SHA512 comme algorithme de hash



```
Fichier  Édition  Affichage  Recherche  Terminal  Aide
root@kalo:~# truecrack -t /root/Desktop/bloc/Moselle57/AES_SHA-512 -w /root/Desktop/dictionnaire.txt -k sha512
```

## Résultat

Comme dit plus haut dans le rapport, TrueCrypt nous donne le choix entre 8 algorithmes d'encryptions et 3 pour hacher.

Est-ce-que tous les algorithmes pour un mot de passe et dictionnaire donnés sont équivalents ?

Voici les mots de mon dictionnaire (dictionnaire.txt) qui sera utilisé :





























































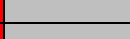
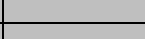
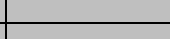
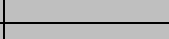
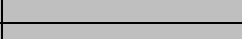



















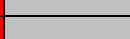
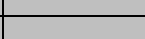
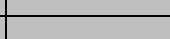
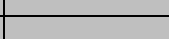
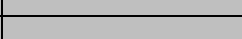



















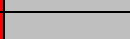
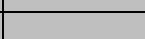
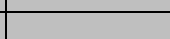
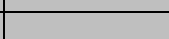
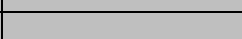

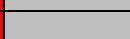
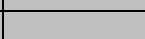
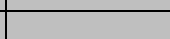
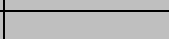
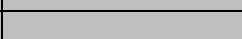







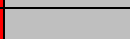
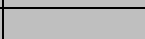
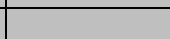
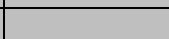
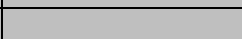








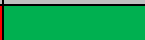

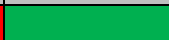

dictionnaire.txt				
Fichier	Édition	Rechercher	Options	Aide
Aurai				
-				
je				
une				
bonne				
note				
(				
20				
)				
pour				
mon				
projet				
test				
?				
Luxembourg				
MIM				
Moselle				
ParisNew-York20!				
France				
Italie				
Manger				
Cigarette				
facile				
maladroit				

Note : Le mot de passe se trouve dans le dictionnaire ceci est volontaire

 Mot de passe trouvé

 Mot de passe non trouvé

 Non testé (explication dans la conclusion)

Algorithme utilisé	Mot de passe utilisé					
	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

Comme on peut le voir les mêmes facteurs reviennent lorsque le mot de passe est trouvé :

- ❖ Le mot de passe se trouve dans le dictionnaire
- ❖ L'algorithme de chiffrement est AES

Donc pour mes tests tous les algorithmes sont équivalents sauf celui d'AES qui est à éviter.

Pour les algorithmes de hash ils sont tous équivalents

La version de TrueCrack utilisée nous permet de choisir le hash mais pas l'algorithme de chiffrement pour tenter de trouver le mot de passe.

**Seul l'algorithme AES est pris en compte donc après un premier test avec les autres algorithmes il était inutile de les tester avec des mots de passe plus fort, ceci est inutile TrueCrack ne l'aurait pas trouvé.**

Il existe une autre version de TrueCrack (ou une extension) qui permet de rajouter l'option du choix de l'algorithme de chiffrement.

Après plusieurs tests sur mon ordinateur je n'ai pas réussi à installer une autre version ou l'extension, mais **le principe et le résultat de ma conclusion serait la même.**

**Avec une version de TrueCrack avec l'option du choix d'algorithme de chiffrement (-e) tous les algorithmes deviendraient équivalents (contrairement à mes tests où AES était à éviter).**

**Si l'option ne permet que de choisir un algorithme alors privilégier un choix d'algorithme qui combine plusieurs algorithmes de chiffrement (Serpent-Twofish-AES par exemple) pour se protéger d'une attaque.**

Donc si TrueCrack connaît l'algorithme de chiffrement ainsi que l'algorithme de hash et que le mot de passe soit dans le dictionnaire utilisé le mot de passe est trouvé.

Tester quelle est la combinaison de l'algorithme de chiffrement et de l'algorithme de hachage ne coûte rien à l'attaquant ( $8 \times 3 = 24$  combinaisons)

(Dans mes tests  $1 \times 3$  car AES + un choix de hash)

Pour se protéger de l'attaque il faut donc un mot de passe qui ne soit pas dans un dictionnaire d'attaque.

Le but ici n'est pas de donner un cours de comment choisir un bon mot de passe mais voici quelques conseils :

- ❖ Choisir une bonne longueur (10 caractères minimum)
- ❖ Une suite de caractère avec minuscule, majuscule, chiffre et caractère spécial (-, !, \$,...)
- ❖ Pas de mot d'un dictionnaire
- ❖ Ne pas choisir quelque chose d'aisément devinable



Mon astuce pour mémoriser un bon mot de passe: Choisir une phrase et prendre la 1<sup>ère</sup> lettre de chaque mot en alternant majuscule et minuscule.

Exemple : Sérieusement que pensez-vous de mon rapport il vaut 20/20 ?

Mot de passe : SqP-vDmRiV20?

**Avant mon rapport TrueCrack était considéré comme un des meilleurs logiciels pour chiffrer ses données (toujours sans parler du débat s'il est compromis ou pas dès le départ)**

**Avec un bon mot de passe le niveau de sécurité de ce logiciel est très bon et répond à sa réputation.**

**[Source des définitions wikipedia.fr](https://fr.wikipedia.org/)**