ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ
Τμήμα Πληροφορικής

Εργασία Μαθήματος ***Ασφάλεια Πληροφοριακών Συστημάτων***

Άσκηση *<<αριθμός άσκησης>>*	***4η Άσκηση - Ασφάλεια συνθηματικών***
Όνομα φοιτητή – Αρ. Μητρώου (όλων σε περίπτωση ομαδικής εργασίας)	Κουσουννής Κωνσταντίνος p14086
Ημερομηνία παράδοσης	03-12-2018

Χρησιμοποιώντας όποια εργαλεία ελέγχου συνθηματικών θέλετε (π.χ. Cain, John the Ripper, OphCrack κτλ) να αποκρυπτογραφήσετε τα συνθηματικά, με την καταλληλότερη μέθοδο, με βάση τα δεδομένα που δίνονται σε κάθε περίπτωση. Να αναφέρεται σε κάθε περίπτωση, το συνθηματικό, ποια μέθοδο χρησιμοποιήσατε, γιατί την επιλέξατε και πόσος χρόνος απαιτήθηκε.

1)9FC63641386C279AB1A62C51F0C8268AF67309218121C804905E3F3BD7D59E51 : Το συνθηματικό μπορεί να περιλαμβάνει οποιοδήποτε χαρακτήρα αλλά έχει μικρό μήκος (<6). Με βάση τα χαρακτηριστικά του hash value να βρείτε ποια συνάρτηση έχει χρησιμοποιηθεί.

2)95DCC3CEAC9865A72B66C84546A3549C : Είναι MD5 συνθηματικό. Το συνθηματικό περιλαμβάνει μόνο μικρά γράμματα και είναι μέχρι 7 χαρακτήρες.
3)B54B9E2BE205AB4D239258FEE9735952D19C9762 : Πρόκειται για SHA-1 συνθηματικό, το οποίο είναι πάνω από 10 χαρακτήρες. Είναι passphrase το οποίο περιλαμβάνει μόνο γράμματα, μικρά και κεφαλαία. (Υπόδειξη: διαλέξτε την κατάλληλη μέθοδο ανάκτησης του συνθηματικού και τις κατάλληλες παραμέτρους)

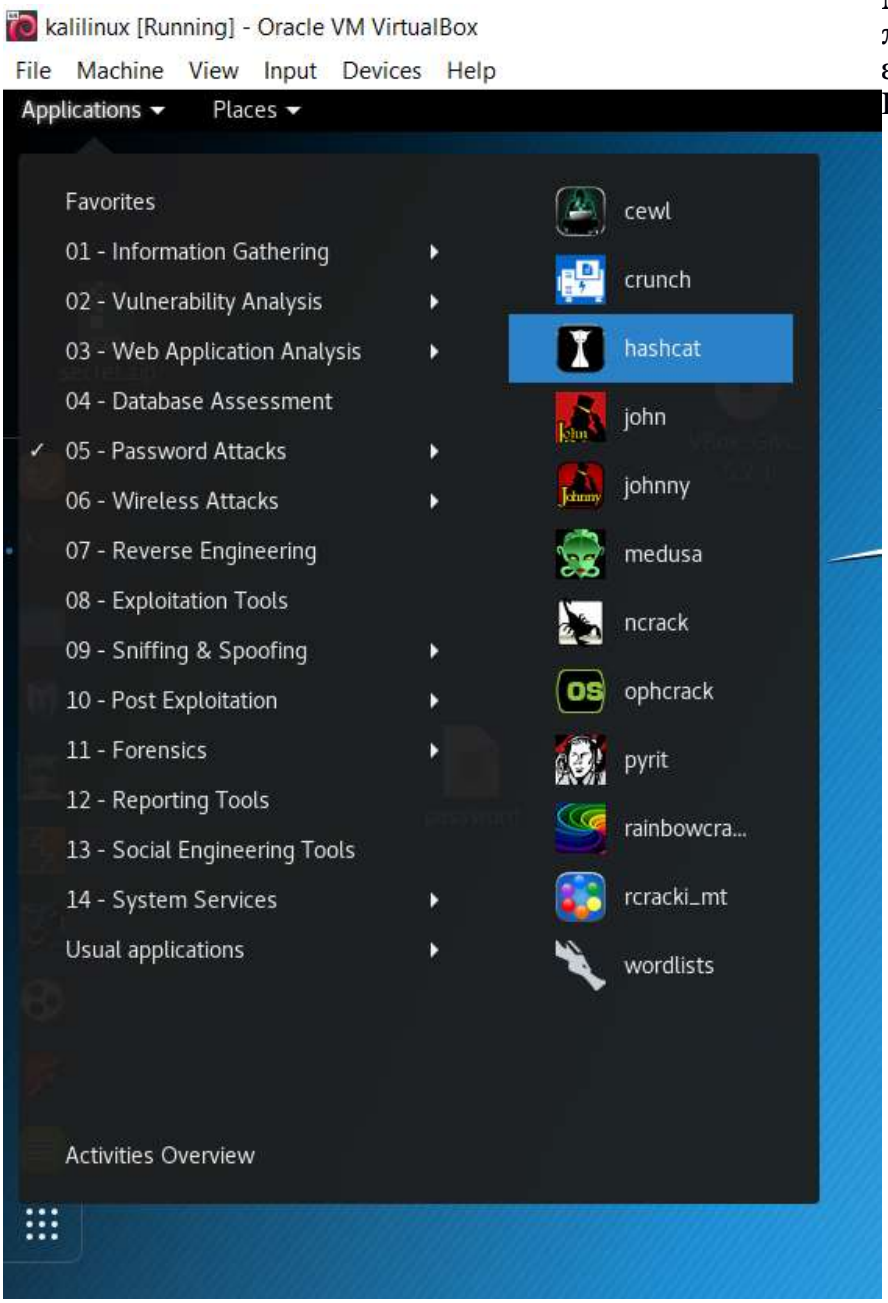
3)836DCD3F1A0E9A14B0D83E64125B32E0D4440F45 : Το συνθηματικό είναι ελληνική λέξη.

4)2D4027D6DF9C0256B8D4474CE88F8C88 : Πρόκειται για το MD5 hash του συνθηματικού. Όμως επειδή γνωρίζουμε ότι το σύστημα-στόχος χρησιμοποιεί μόνο 4-ψήφια PIN, καλείστε να δημιουργήσετε το rainbow table για όλα τα συνθηματικά-PIN 4 ψηφίων για τη συνάρτηση MD5. Περιλάβετε στην απάντηση αυτού του βήματος πόσος χρόνος απαιτήθηκε στο σύστημά σας για να υπολογιστεί το rainbow table το οποίο θα έχει δημιουργηθεί με τέτοιες παραμέτρους ώστε (α) να παρέχει 100% επιτυχία για την εύρεση οποιουδήποτε PIN 4 ψηφίων και (β) να έχει το ελάχιστο δυνατό μέγεθος. Επίσης περιλάβετε screenshot από την δημιουργία του rainbow table.

1)9FC63641386C279AB1A62C51F0C8268AF67309218121C804905E3F3BD7D59E51 : Το συνθηματικό μπορεί να περιλαμβάνει οποιοδήποτε χαρακτήρα αλλά έχει μικρό μήκος (<6). Με βάση τα χαρακτηριστικά του hash value να βρείτε ποια συνάρτηση έχει χρησιμοποιηθεί.

Ανοίγω στο kali linux το εργαλείο που λέγεται hash-identify
Πληκτρολογώ τον κωδικό στο εργαλείο και μου εμφανίζει τα πιθανά hashes

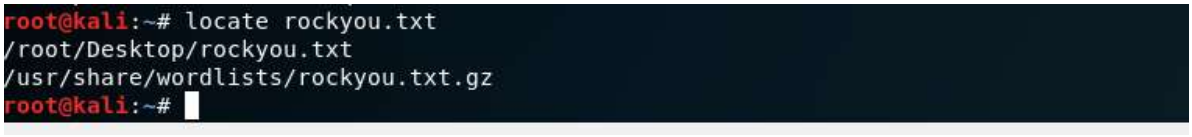
Θα χρησιμοποιήσουμε το εργαλείο hashcat στο Kali Linux.



Μας λέει οτι τα ποιο πιθανά αποτελέσματα είναι το SHA-256 ή Haval-256

Παιρνουμε το dictionary που έχει το hashcat

Πληκτρολογούμε την εντολή **locate rockyou.txt** και μας βρίσκει η εντολή το αντίστοιχο path δηλαδή:

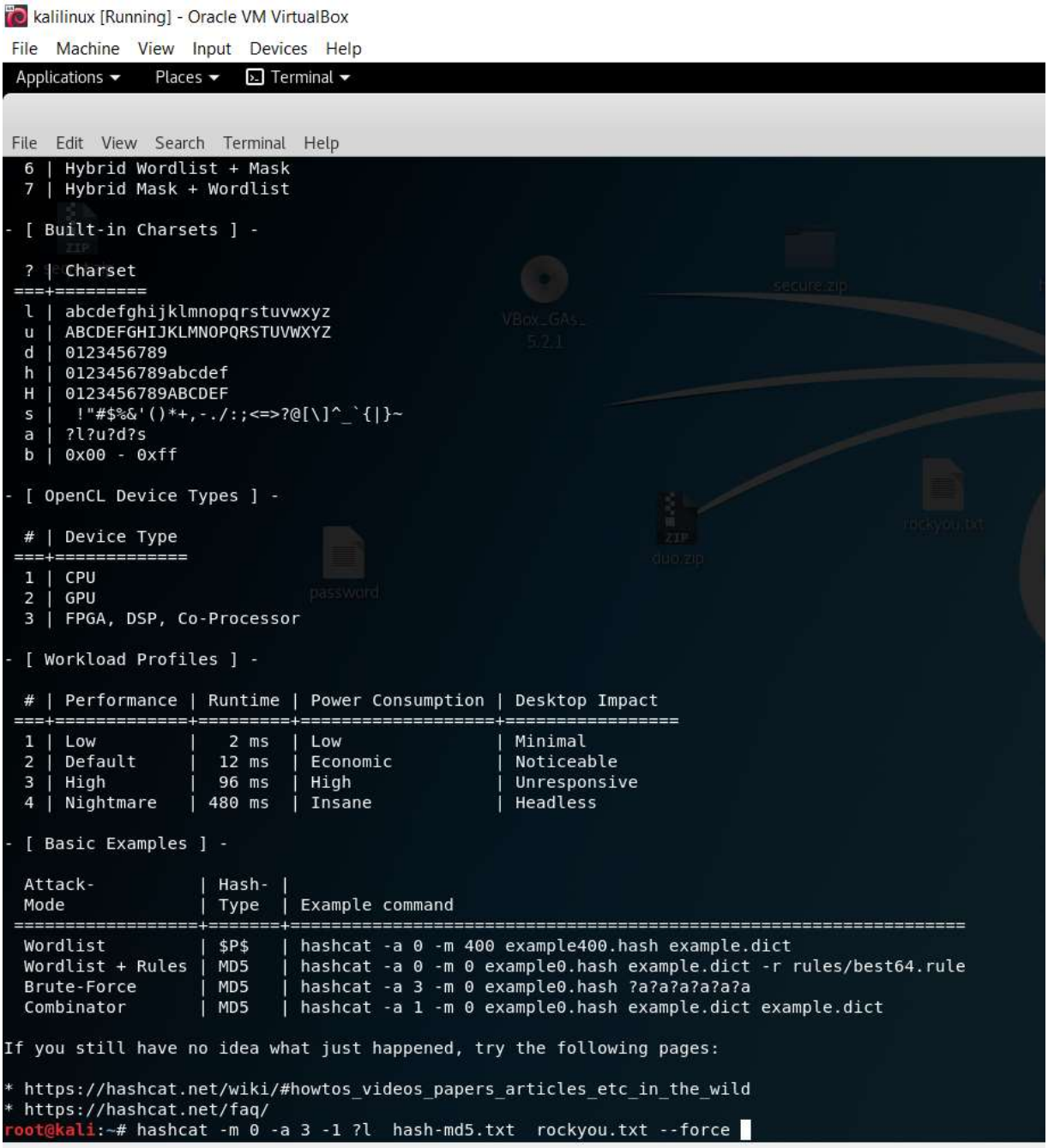


Βλέπουμε οτι το P**ath:/usr/share/wordlist/rockyou.txt.gz**

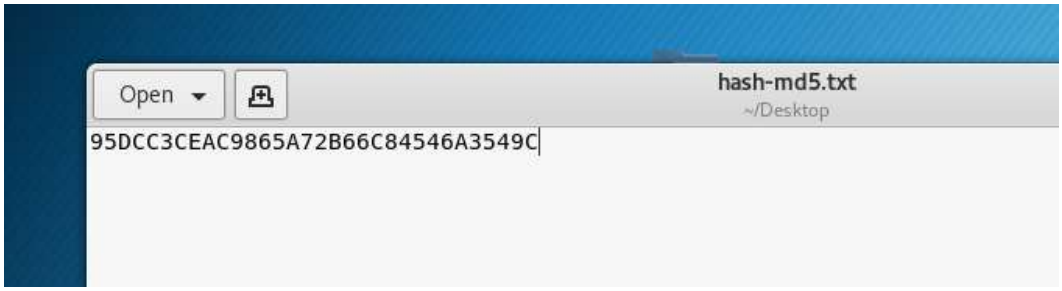
Στην συνέχεια κανουμε αντιγραφή στην επιφάνει εργασίας με την εντολή
cp /usr/share/wordlist/rockyou.txt.gz root/Desktop/rockyou.txt.gz

Στην συνέχεια έξαγουμε το ζιπαρισμένο αρχείο σε txt αρχείο
gunzip rockyou.txt.gz rockyou.txt

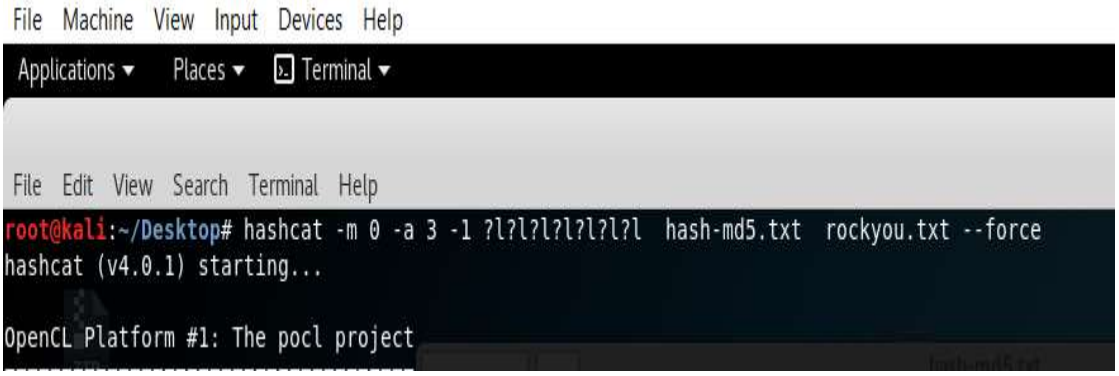
2)95DCC3CEAC9865A72B66C84546A3549C : Είναι MD5 συνθηματικό. Το συνθηματικό περιλαμβάνει μόνο μικρά γράμματα και είναι μέχρι 7 χαρακτήρες.



Παίρνουμε το password απο την εκφώνηση **95DCC3CEAC9865A72B66C84546A3549C**

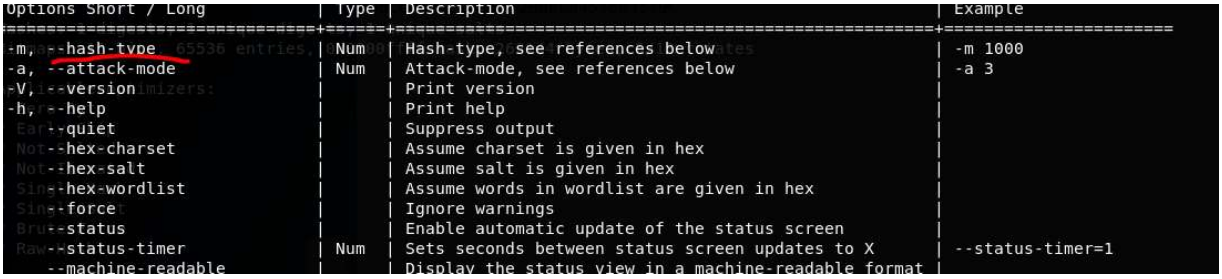


Αποθηκεύουμε το κωδικό σε ένα αρχείο που ονομάζεται hash-md5.txt



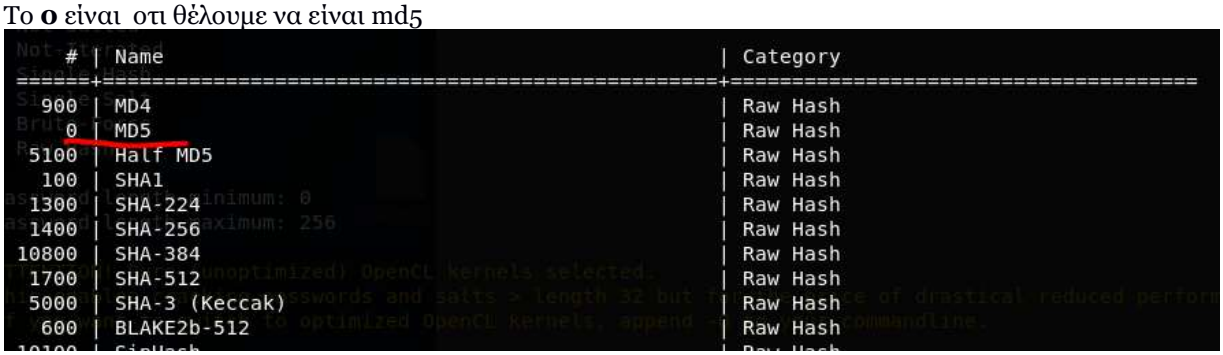
Πληκρολογώ την εντολή :
hashcat -m 0 -a 3 -1 ?l?l?l?l?l?l?l hash-md5.txt rockyou.txt –force

Το **-m** είναι το hashtype που χρησιμοποιείτε.



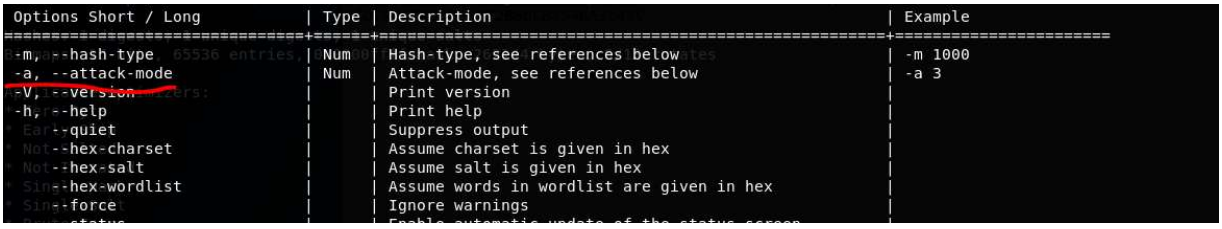
Options Short / Long	Type	Description	Example
-m, --hash-type	Num	Hash-type, see references below	-m 1000
-a, --attack-mode	Num	Attack-mode, see references below	-a 3
-V, --version		Print version	
-h, --help		Print help	
--quiet		Suppress output	
--hex-charset		Assume charset is given in hex	
--hex-salt		Assume salt is given in hex	
--hex-wordlist		Assume words in wordlist are given in hex	
--force		Ignore warnings	
--status		Enable automatic update of the status screen	
--status-timer	Num	Sets seconds between status screen updates to X	--status-timer=1
--machine-readable		Display the status view in a machine-readable format	

Το **o** είναι οτι θέλουμε να είναι md5



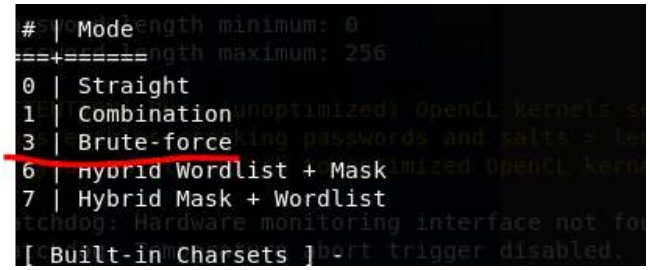
#	Name	Category
900	MD4	Raw Hash
0	MD5	Raw Hash
5100	Half MD5	Raw Hash
100	SHA1	Raw Hash
1300	SHA-224	Raw Hash
1400	SHA-256	Raw Hash
10800	SHA-384	Raw Hash
1700	SHA-512	Raw Hash
5000	SHA-3 (Keccak)	Raw Hash
600	BLAKE2b-512	Raw Hash

Το **-α** είναι το είδος της επίθεσης

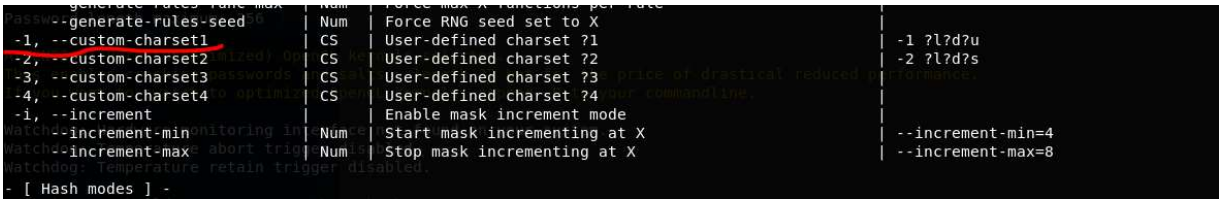


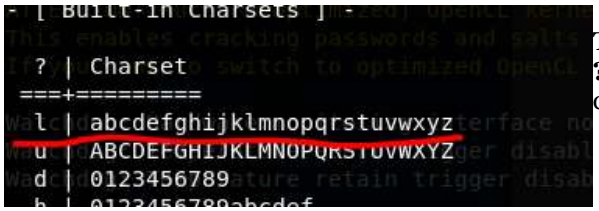
Options Short / Long	Type	Description	Example
-m, --hash-type	Num	Hash-type, see references below	-m 1000
-a, --attack-mode	Num	Attack-mode, see references below	-a 3
-V, --version		Print version	
-h, --help		Print help	
--quiet		Suppress output	
--hex-charset		Assume charset is given in hex	
--hex-salt		Assume salt is given in hex	
--hex-wordlist		Assume words in wordlist are given in hex	
--force		Ignore warnings	

Το **3** είναι brute-force



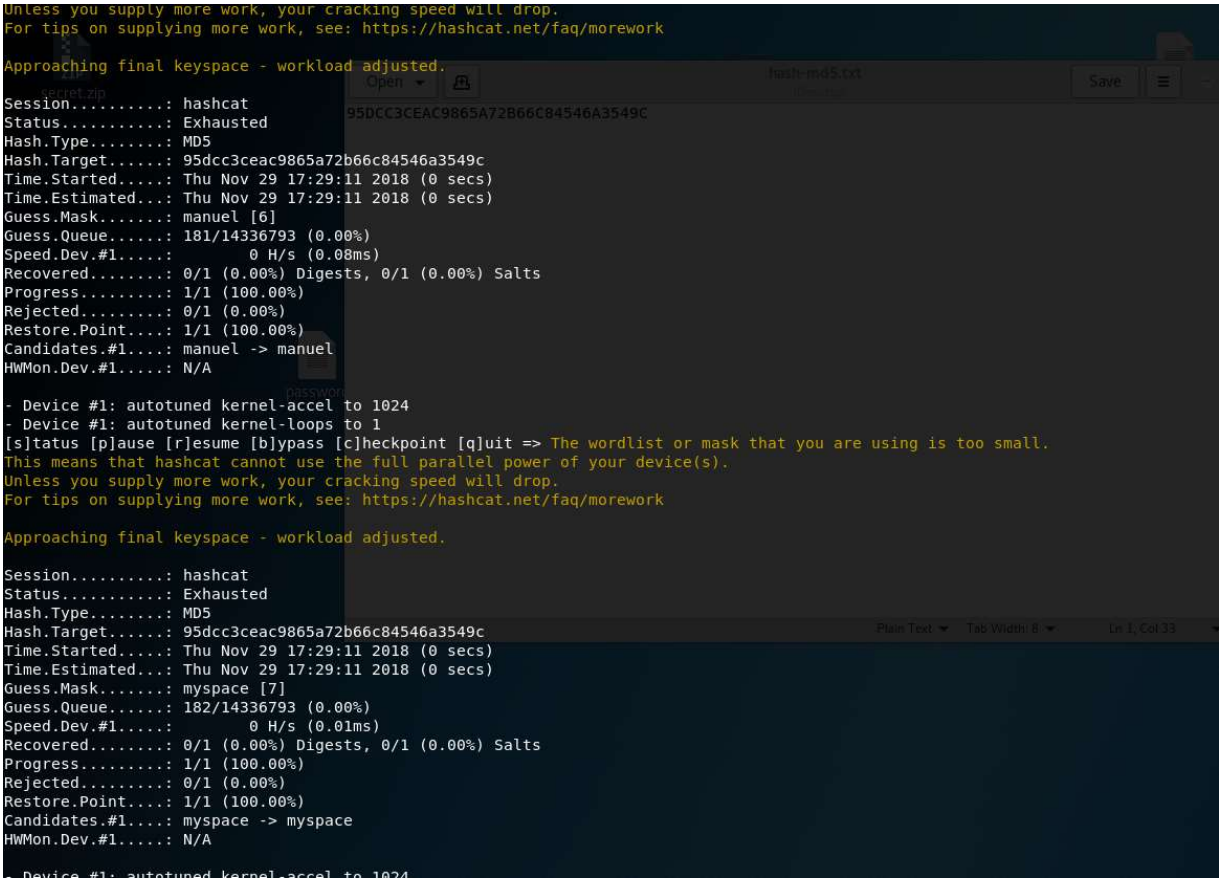
-1 ?l?l?l?l?l?l?l είναι για να βάλουμε μικρά γράμματα και να περιέει 7 χαρακτήρες



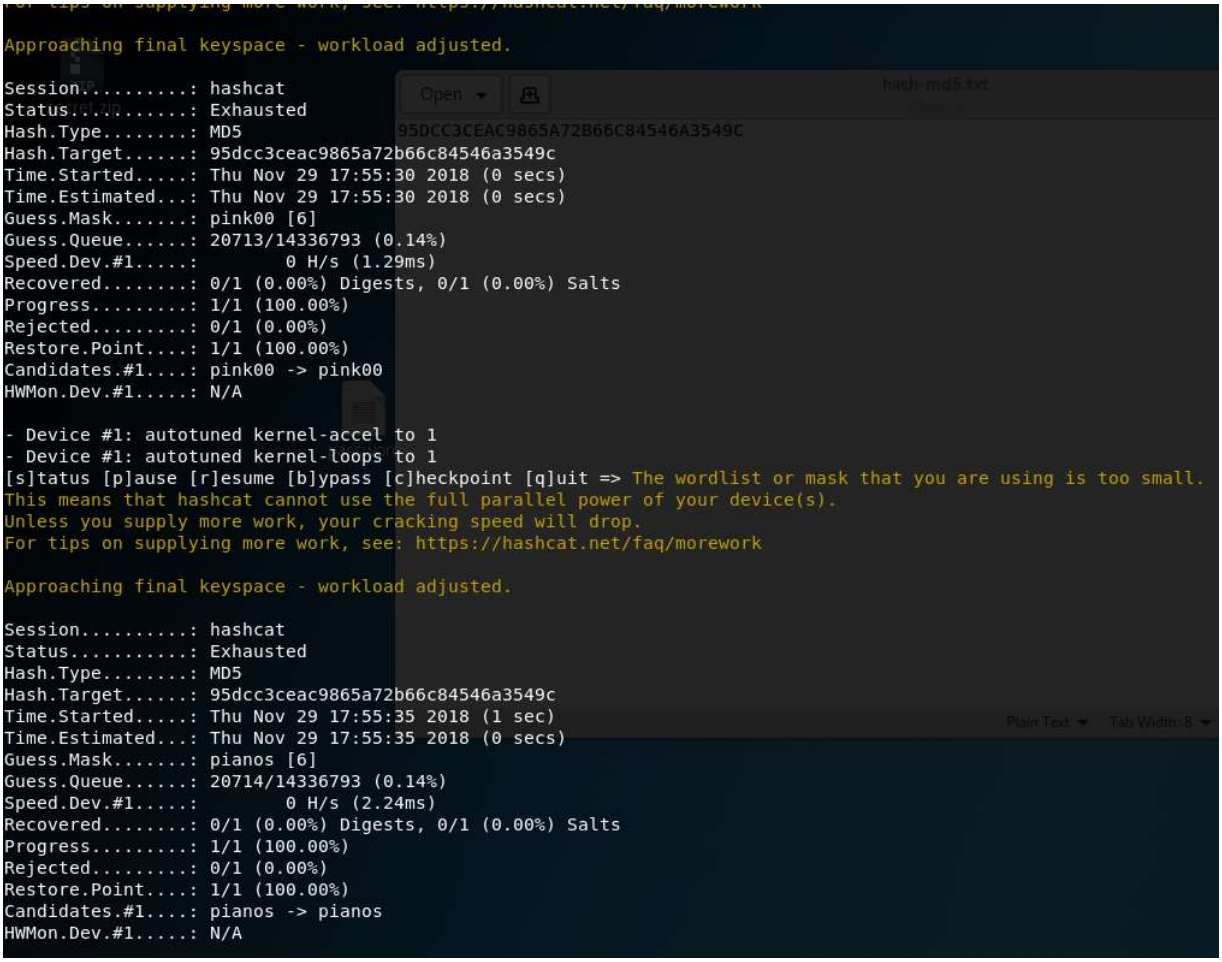


Το l είναι για τα μικρά γράμματα.Και οτι επανλαμβάνω το **?l 7 φορές** τοτε το hashcat περιέχει 7 γράματα μικρά ακριβώς.

hash-md5.txt Ειναι το αρχείο που αποθηκεύσαμε τον κωδικό
rockyou.txt Εχουμε το λεξικό που χρησιμοποιεί ο hashcat

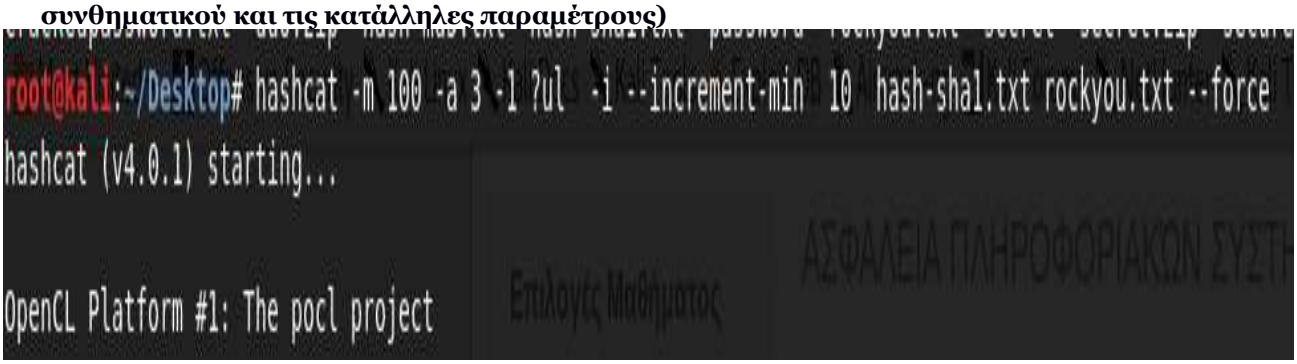


Το Hashcat έχει ξεκινήσει .



Οπως βλέπουμε είναι στο 0.14% ειναι θα πρέπει να το αφησουμε να συνεχίσει μεχρι να βρει τον κωδικό.

3)B54B9E2BE205AB4D239258FEE9735952D19C9762 : Πρόκειται για SHA-1 συνθηματικό, το οποίο είναι πάνω από 10 χαρακτήρες. Είναι passphrase το οποίο περιλαμβάνει μόνο γράμματα, μικρά και κεφαλαία. (Υπόδειξη: διαλέξτε την κατάλληλη μέθοδο ανάκτησης του συνθηματικού και τις κατάλληλες παραμέτρους)



Με αντίστοιχο τρόπο έχουμε την εντολή:

hashcat -m 100 -a 3 -1 ?ul -i –increment-min 10 hash-md5.txt rockyou.txt –force

-m 100 είνια sha1

```
   5100 | Half MD5                                                  | Raw Hash
    100 | SHA1                                                      | Raw Hash
   1300 | SHA-224                                                   | Raw Hash
   1400 | SHA-256                                                   | Raw Hash
```

Το **-α** είναι το είδος της επίθεσης

```
Options Short / Long          | Type | Description                                          | Example
==============================+======+======================================================+=======================
-m, --hash-type               | Num  | Hash-type, see references below                      | -m 1000
-a, --attack-mode             | Num  | Attack-mode, see references below                    | -a 3
-V, --version                 |      | Print version                                        |
-h, --help                    |      | Print help                                           |
    --quiet                   |      | Suppress output                                      |
    --hex-charset             |      | Assume charset is given in hex                       |
    --hex-salt                |      | Assume salt is given in hex                          |
    --hex-wordlist            |      | Assume words in wordlist are given in hex            |
    --force                   |      | Ignore warnings                                      |
```

Το **3** είναι brute-force

```
# | Mode
===+======
0 | Straight
1 | Combination
3 | Brute-force
6 | Hybrid Wordlist + Mask
7 | Hybrid Mask + Wordlist

- [ Built-in Charsets ] -
```

-1 ?ul συμβολίζει οτι μπορεί να είναι μικρά ή κεφαλαία

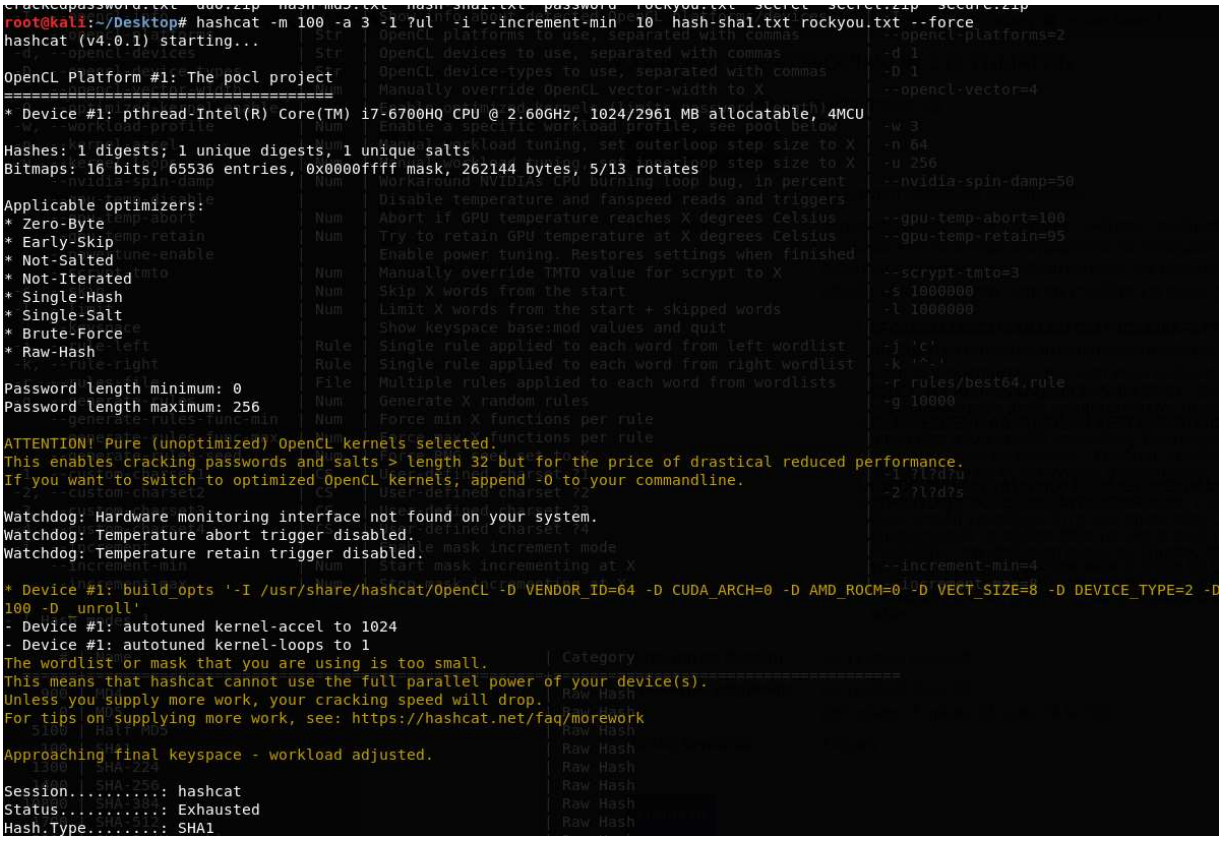
```
  ? | Charset
 ===+=========
  l | abcdefghijklmnopqrstuvwxyz
  u | ABCDEFGHIJKLMNOPQRSTUVWXYZ
  d | 0123456789
  h | 0123456789abcdef
```

-i –increment-min 10

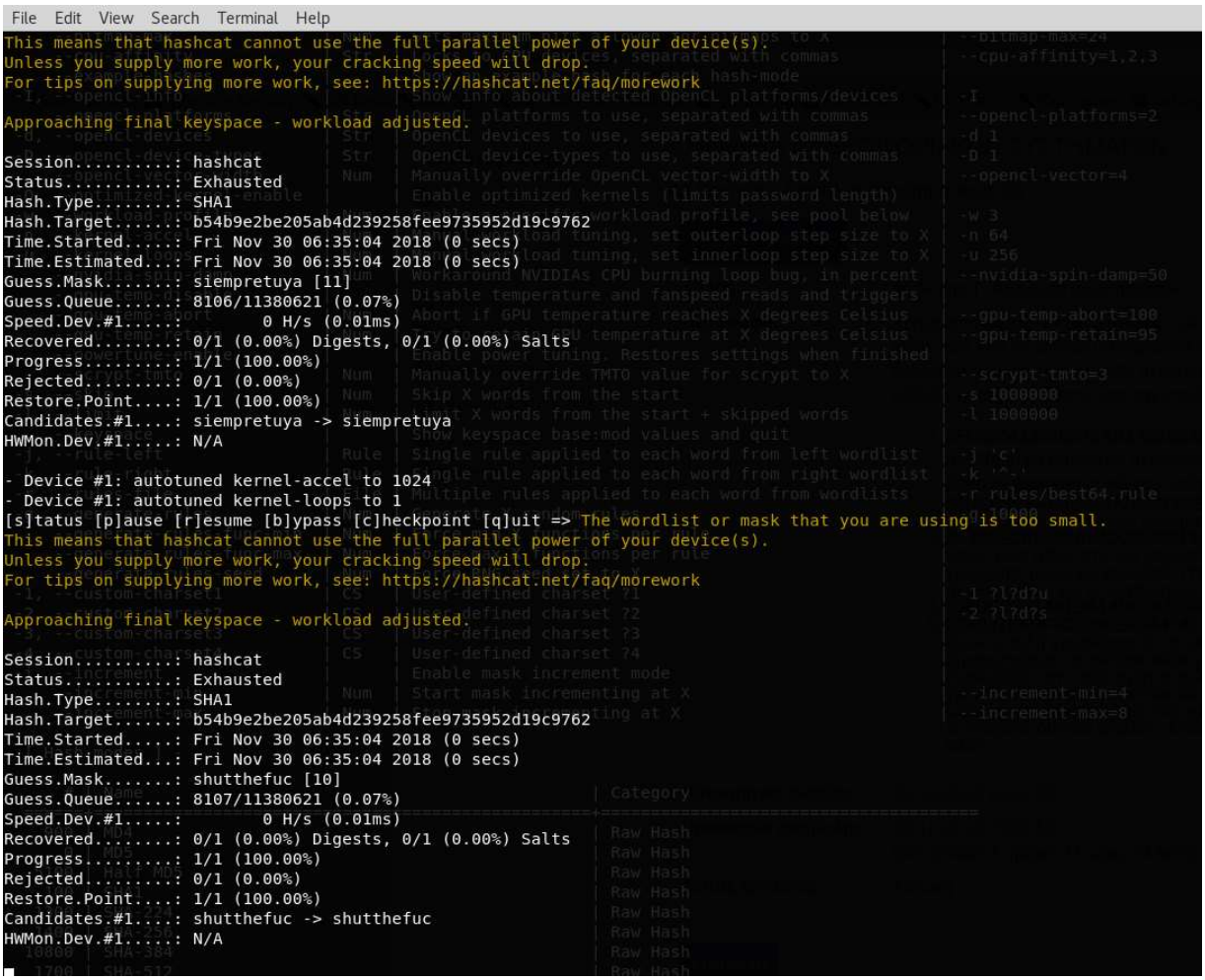
```
-3, --custom-charset3         | CS   | User-defined charset ?3                              |
-4, --custom-charset4         | CS   | User-defined charset ?4                              |
-i, --increment               |      | Enable mask increment mode                           |
    --increment-min           | Num  | Start mask incrementing at X                         | --increment-min=4
    --increment-max           | Num  | Stop mask incrementing at X                          | --increment-max=8

- [ Hash modes ] -
```

Εδω θέλουμε να είναι ο κωδικός μεγαλύτερος απο 10 χαρακτήρες.

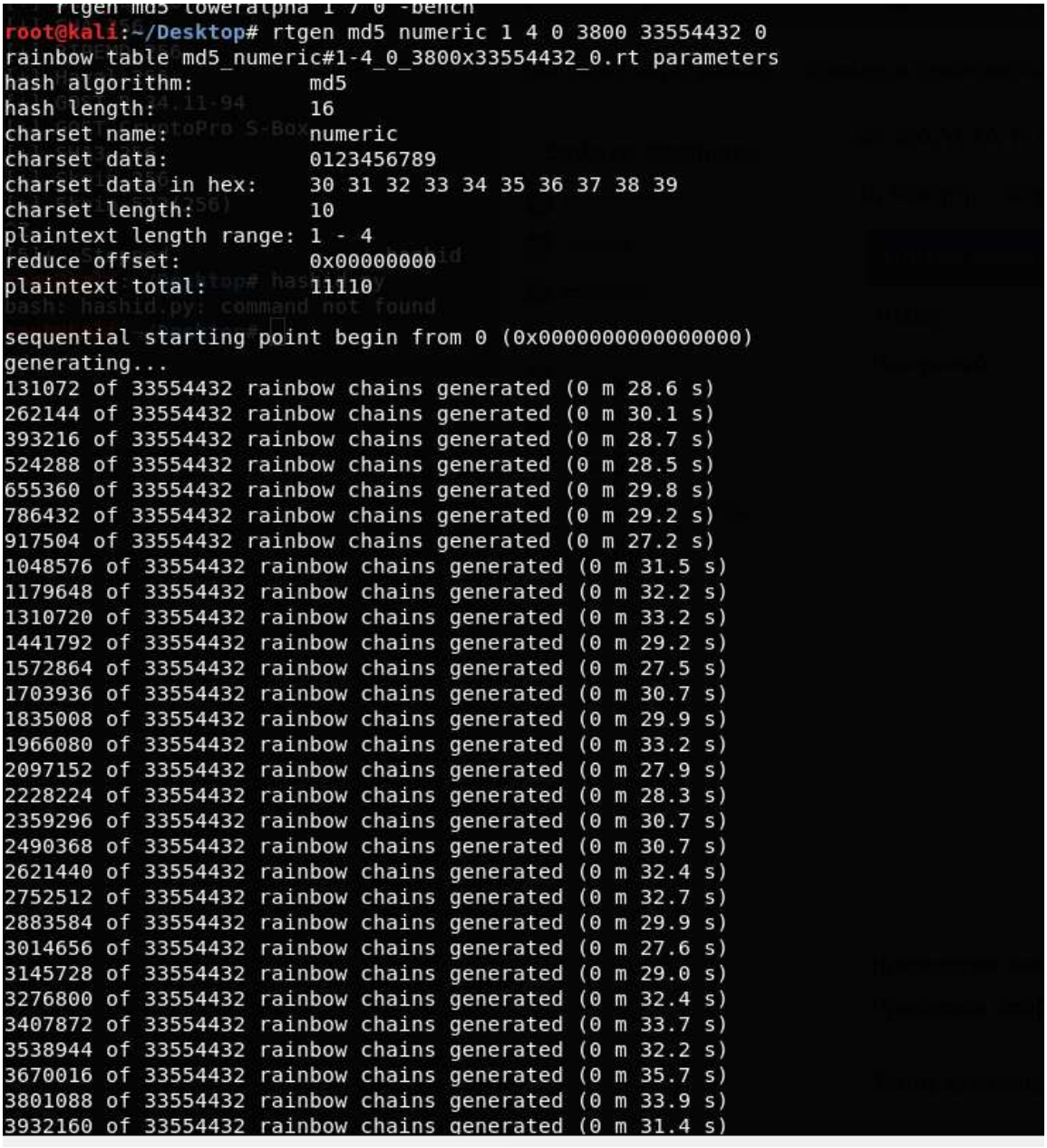


Έχει ξεκινήσει η αποκρυπτογράφηση του κωδικού.



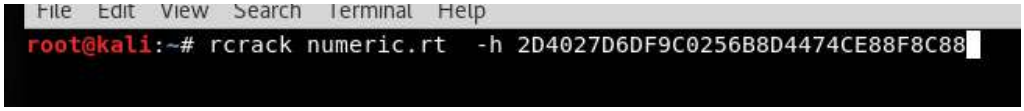
Οσο τρέχει το πρόγραμμα βλέπουμε οτι οι χαρακτήρες που χρησιμοποιεί είναι 10 και πάνω.
Το πρόγραμμα είναι στο 0.7%

4)2D4027D6DF9C0256B8D4474CE88F8C88 : Πρόκειται για το MD5 hash του συνθηματικού. Όμως επειδή γνωρίζουμε ότι το σύστημα-στόχος χρησιμοποιεί μόνο 4-ψήφια PIN, καλείστε να δημιουργήσετε το rainbow table για όλα τα συνθηματικά-PIN 4 ψηφίων για τη συνάρτηση MD5. Περιλάβετε στην απάντηση αυτού του βήματος πόσος χρόνος απαιτήθηκε στο σύστημά σας για να υπολογιστεί το rainbow table το οποίο θα έχει δημιουργηθεί με τέτοιες παραμέτρους ώστε (α) να παρέχει 100% επιτυχία για την εύρεση οποιουδήποτε PIN 4 ψηφίων και (β) να έχει το ελάχιστο δυνατό μέγεθος. Επίσης περιλάβετε screenshot από την δημιουργία του rainbow table.



Δημιουργώ τους rainbowtables με την εξής εντολή:
rtgen md5 numeric 1 4 0 3800 33554432 0

θελω να περιέχει 4 ψηφία που να είναι αριθμοί.



Μολις φτιάξουμε τον rainbow table χρησιμοποιουμε την εντολή rcrack το όνομα του rainbow table που μολις φτιαξαμε και το τέλος τον κωδικο που θέλουμε να αποκρυπτογραφήσουμε.