Tugas Keamanan Jaringan Komputer

Disusun Oleh :
Candra Adi Winanto
0912101001042

Jurusan Sistem Komputer
Fakultas Ilmu Komputer
Universitas Sriwijaya
Tahun 2016

Cracking Password Windows 7

Abstract

Hacking password merupakan teknik yang digunakan untuk mengetahui password user yang terdaftar pada suatu sistem. Password pada sekarang ini menggunakan algoritma enkripsi yang kuat, yang mana setelah menjadi hash (ciphertext) tidak dapat kembali lagi menjadi text asli. Dari beberapa teknik hacking password yang paling sering digunakan adalah teknik bruteforce. Teknik menggunakan kombinasi password dengan menebak satu persatu kombinasi yang dimungkinkan, kecepatan cracking tipe ini bergantung pada kecepatan komputer. Percobaan menunjukkan kekuatan password tidak hanya bergantung pada algoritma enkripsi, namun juga bergantung pada kerumitan password yang digunakan.

1. Dasar Teori

Password merupakan sebuah kata atau kalimat yang digunakan untuk masuk ataupun membuka sesuatu. Password juga dapat diartikan sebagai sebuah kunci bagi seseorang yang ingin memasuki ataupun membuka sesuatu. Password ada yang berupa plaintext (tidak terenksripsi) dan adapula yang berbentuk ciphertext (terenkripsi). Password yang terenkripsi biasa disebut dengan hash. Hash merupakan sebuah password yang dienkripsi menggunakan algoritma hashing yang mana algoritma ini tidak dapat di dekripsi sesudah menjadi hash, sehingga akan menyulitkan orang yang tidak berhak untuk mengetahui password yang tersimpan dalam sebuah sistem yang dimasukinya. Cara kerja authentikasi password jenis ini adalah, ketika user memasukkan passwordnya maka password yang diketikkan oleh user tersebut akan dirubah dengan algoritma hash yang sama dengan hash password yang tersimpan, kemudian kedua hash ini di cocokkan, jika cocok maka user tersebut dapat mengakses sistem, sebaliknya jika tidak maka sistem akan menolak. Password tipe hash ini sangat sulit untuk ditembus, satu-satunya cara yang dapat digunakan untuk menyerang ciphertext tipe ini adalah degan menggunakan teknik bruteforce. Bruteforce merupakan sebuah teknik yang menggunakan sebauh dictionary yang berisi kemungkinan-kemungkinan password yang mungkin untuk ciphertext tersebut, teknik ini mencoba satu persatu dari kemungkinan password yang ada, hingga kata dalam dictionary (kamus) habis jika tidak ditemukan satu kombinsai password pun yang sama. Pada sistem operasi windows memiliki 2 tipe hashing password yang digunakan yaitu LAN Manager (LM) dan NT LAN Manager (NTLM).

1.1 Hash LM

LAN Manager (LM) merupakan algoritma hashing pertama yang digunakan oleh sistem operasi windows, versi windows yang menggunakan hash tipe ini adalah windows 2000, xp, vista dan 7. Namun pada windows vista dan windows 7 tipe hash ini sudah di matikan secara default. LM hash memiliki 6 tahapan komputasi dalam pembuatan hash :

1. Seluruh password yang user masukkan di ubah ke huruf kapital

2. Password yang memiliki karakter null ditambahkan hingga sama dengan 14 karakter
3. Password tersebut dibagi menjadi 2 dengan masing-masing 7 karakter
4. Hasil pemisahan password digunakan untuk membuat 2 kunci enkripsi DES, satu dari setiap separuh bit paritas ditambah dengan bit untuk membuat kunci 64 bit.
5. Setiap kunci DES digunakan untuk melakukan enkripsi string ASCII sebelumnya, yang menghasilkan 2 nilai ciphertext sebesar 8-byte
6. Dua ciphertext 8-byte digabungkan menjadi satu yang akan menghasilkan nilai hash 16-byte, yang menyelesaikan hash LM.

1.2 Hash NTLM

NT LAN Manager (NTLM) merupakan protokol autentikasi yang merupakan pengganti dari hash LM. NTLM ini digunakan untuk authentikasi pada Windows NT 4. Pembuatan hash NTLM sebenarnya memiliki proses yang lebih sederhana dalam artian dari seperti apa ayng dilakukan oleh sistem operasi, dan mengandalkan pada lagoritma hasing MD4 untuk membuat hash berdasarkan pada serangkaian kalkulasi matematika. Setelah mengubah password menjadi Unicode, algoritma MD4 digunakan untuk membuat hash NT. MD4 merupakan algoritma password hashing yang lebih kuat ketimbang algoritma DES, yang mana MD4 mengijinkan password yang panjang, mengijinkan huruf kecil dan huruf kapital, dan tidak memecah password menjadi 2 bagian yang kecil.

2. Tools yang digunakan

2.1 Virtualbox

Virtualbox merupakan sbuah tools yang digunakan untuk memebuat virtualisasi sistem operasi, sehingga terdapat lebih dari satu sistem operasi yang dapat digunakan pada saat yang bersamaan.

2.2 Pwdump

Pwdump merupakan tools yang digunakan untuk melakukan dumping password windows yang tersimpan pada file sistem windows pada C:\Windows\System32\config\SAM. Untuk melakukan dumping password hash ini, diperlukan mode administrator agar tools dapat melakukan dumping password.

2.3 Cain and Abel

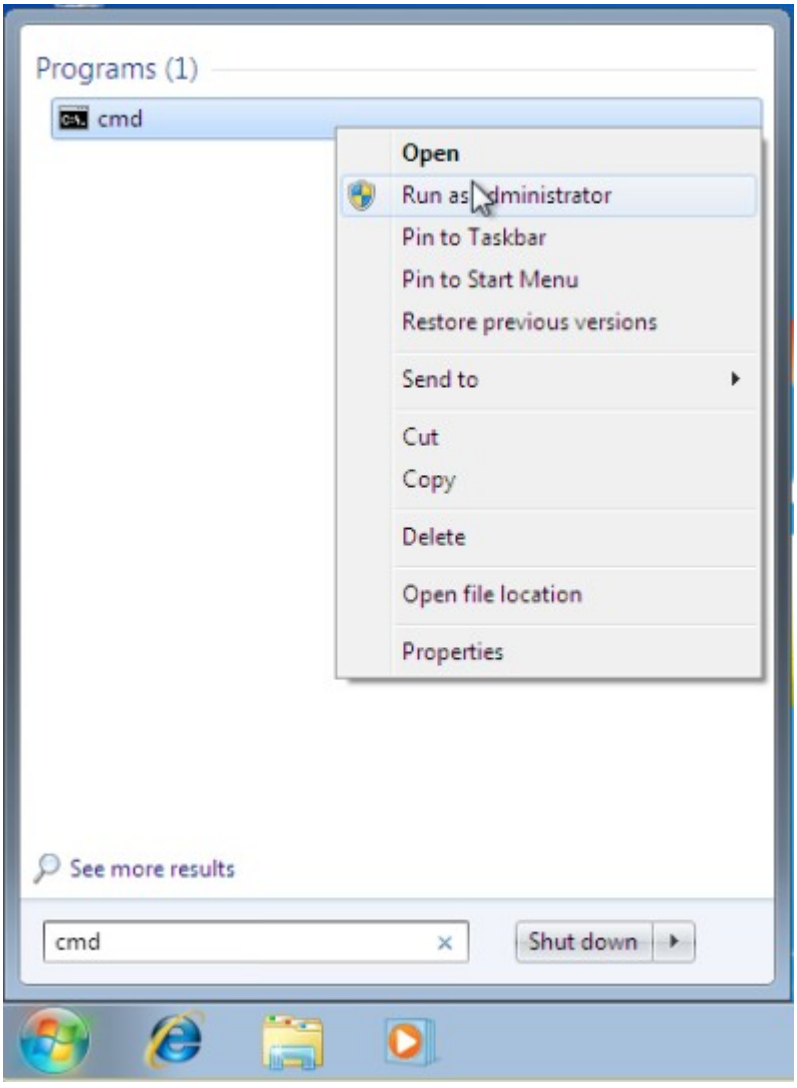
Cain & Abel merupakan tool multifungsi yang dapat digunakan untuk sniffing, cracking password dan yang lainnya.

3. Langkah kerja

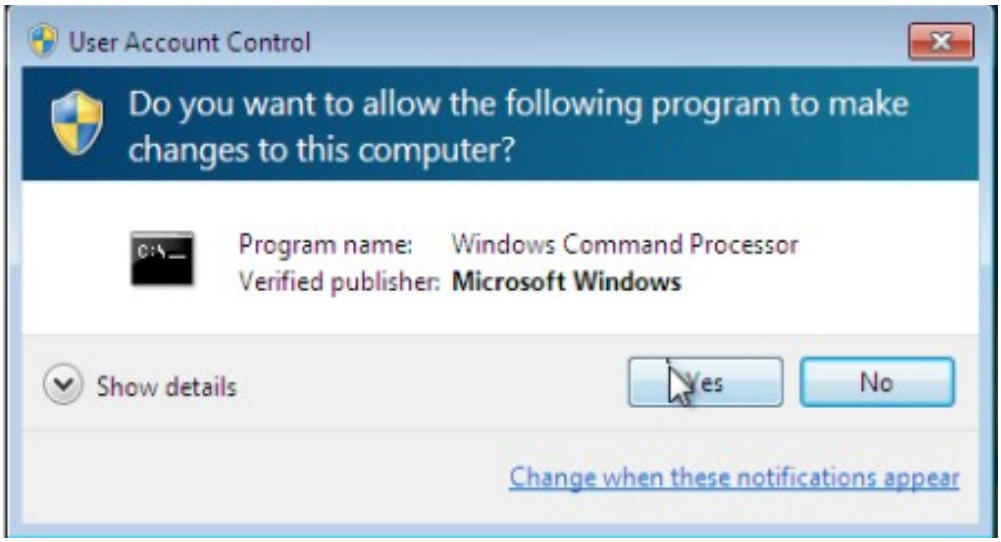
- Melakukan dump terhadap password target menggunakan pwdump
- Melakukan cracking hash password dengan menggunakan tools chain and abel

4. Hasil dan Analisa

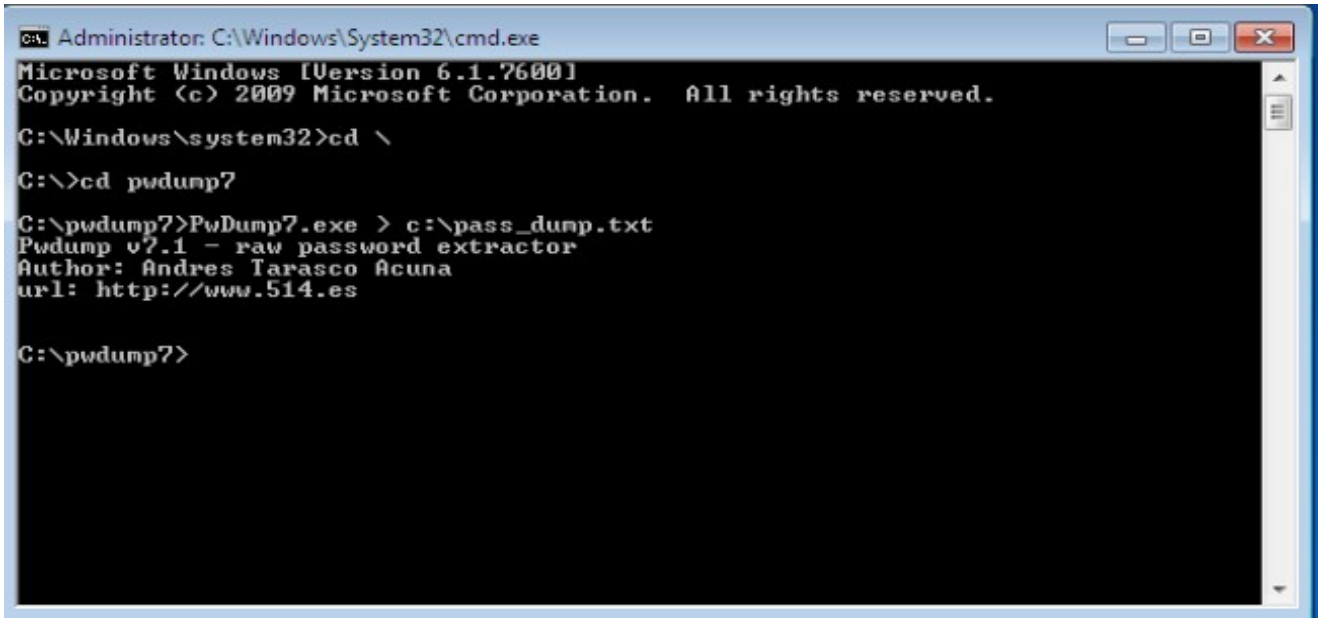
4.1 Hasil



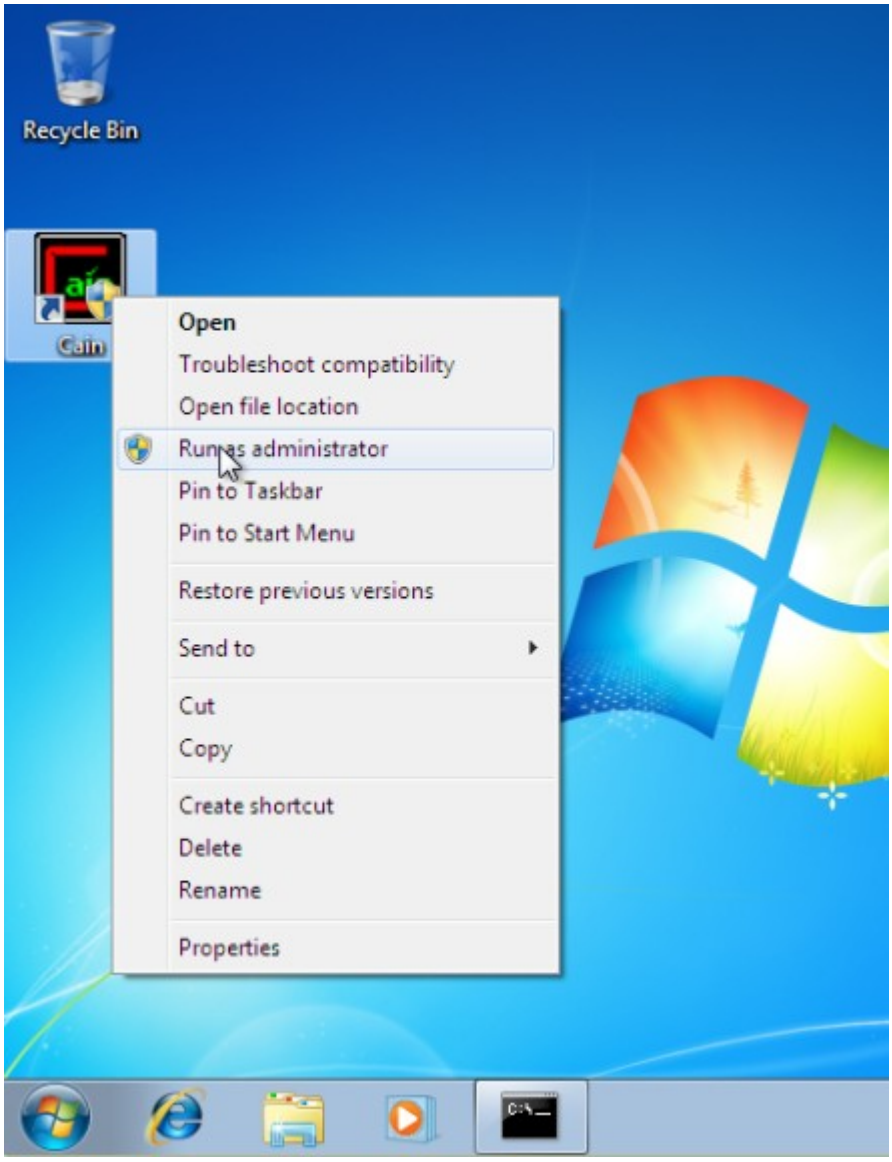
Gambar 1



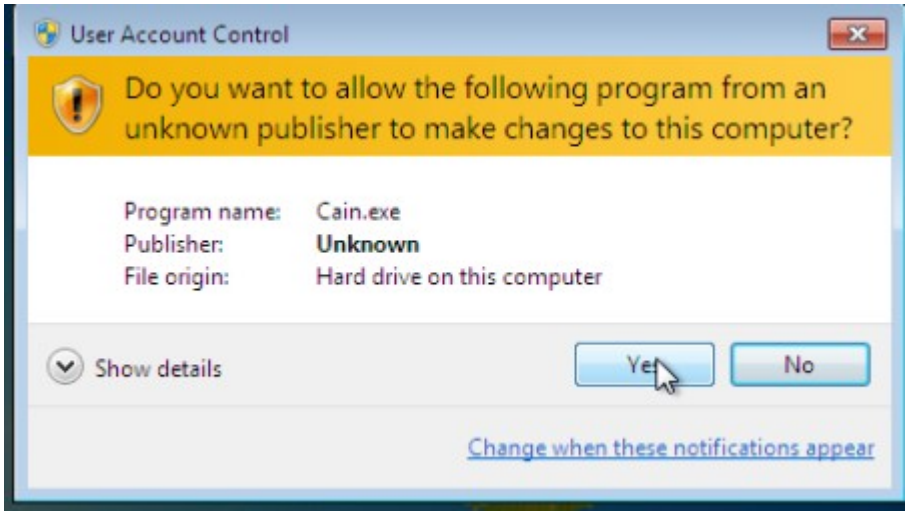
Gambar 2



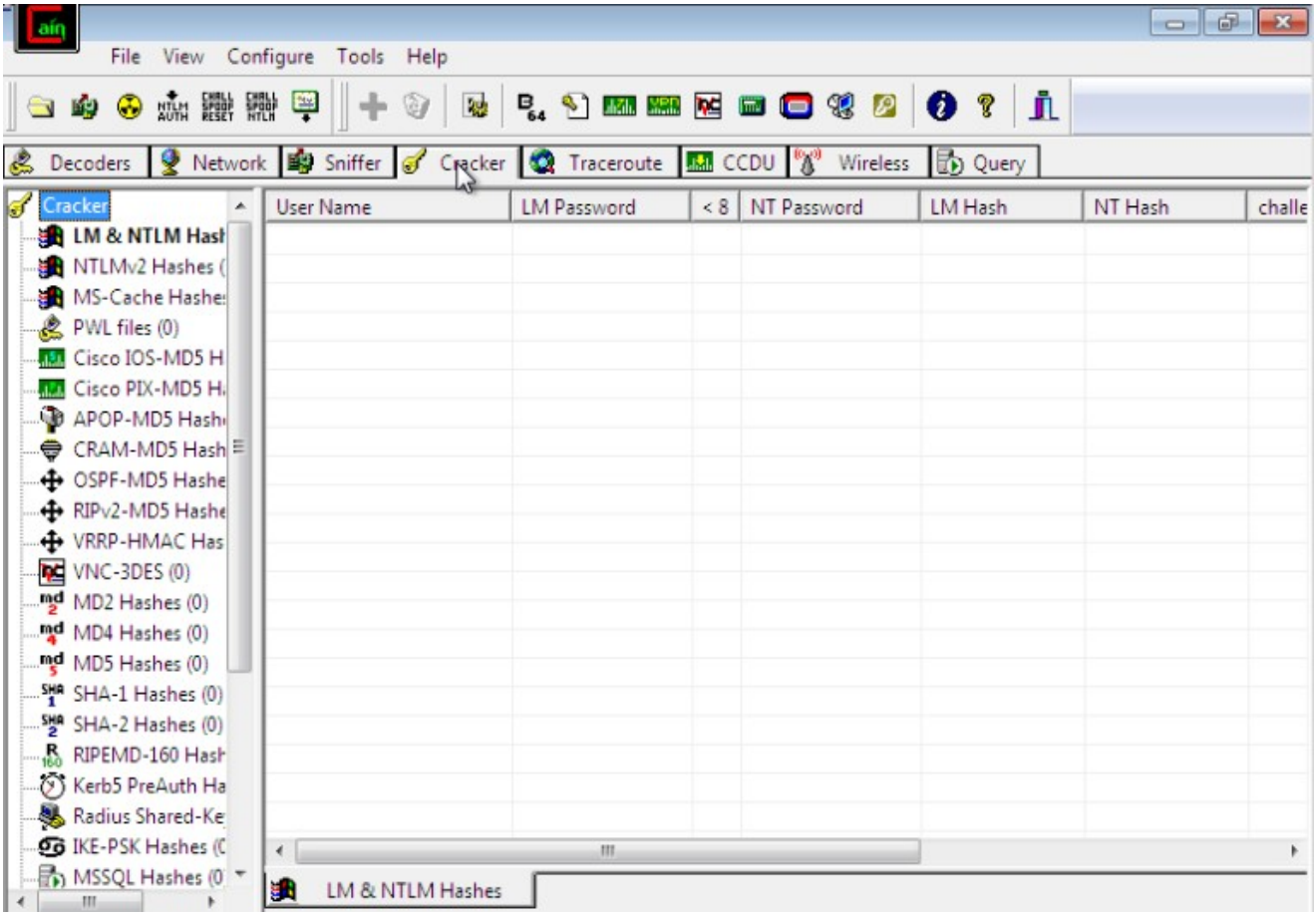
Gambar 3



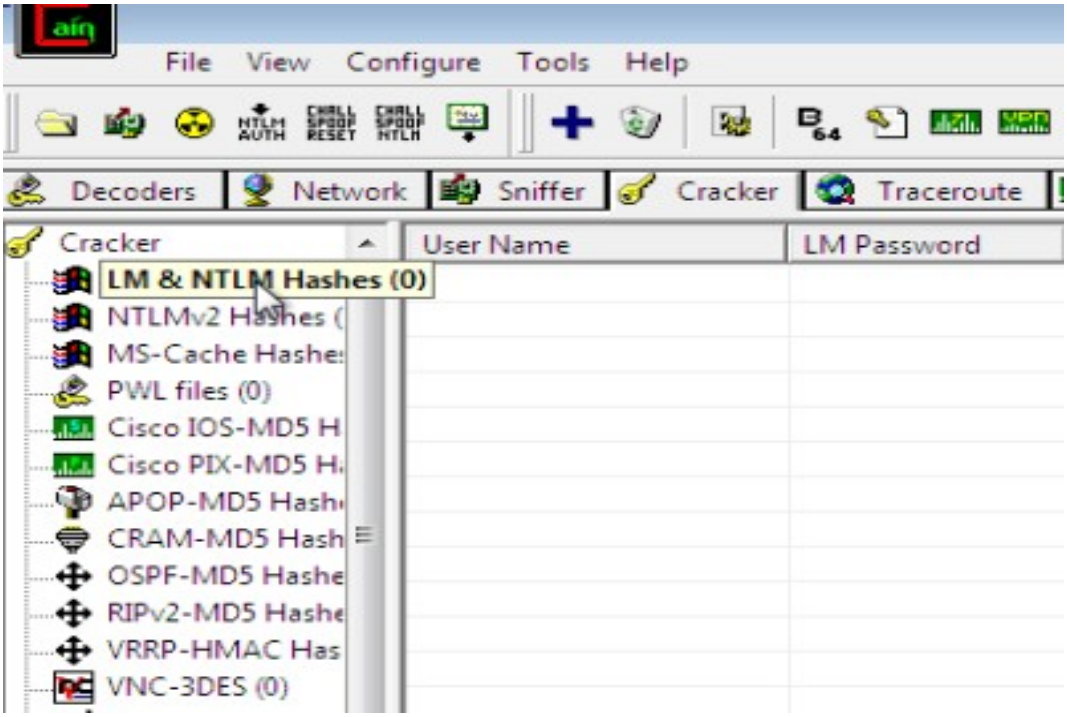
Gambar 4



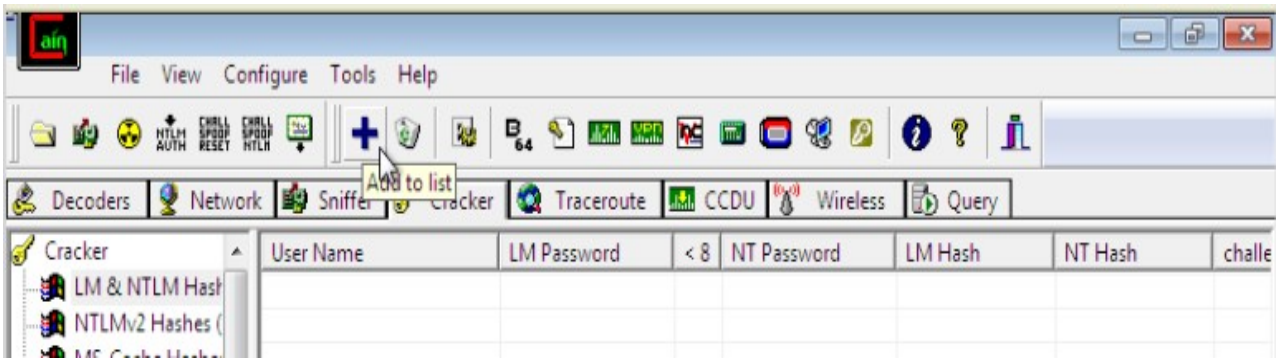
Gambar 5



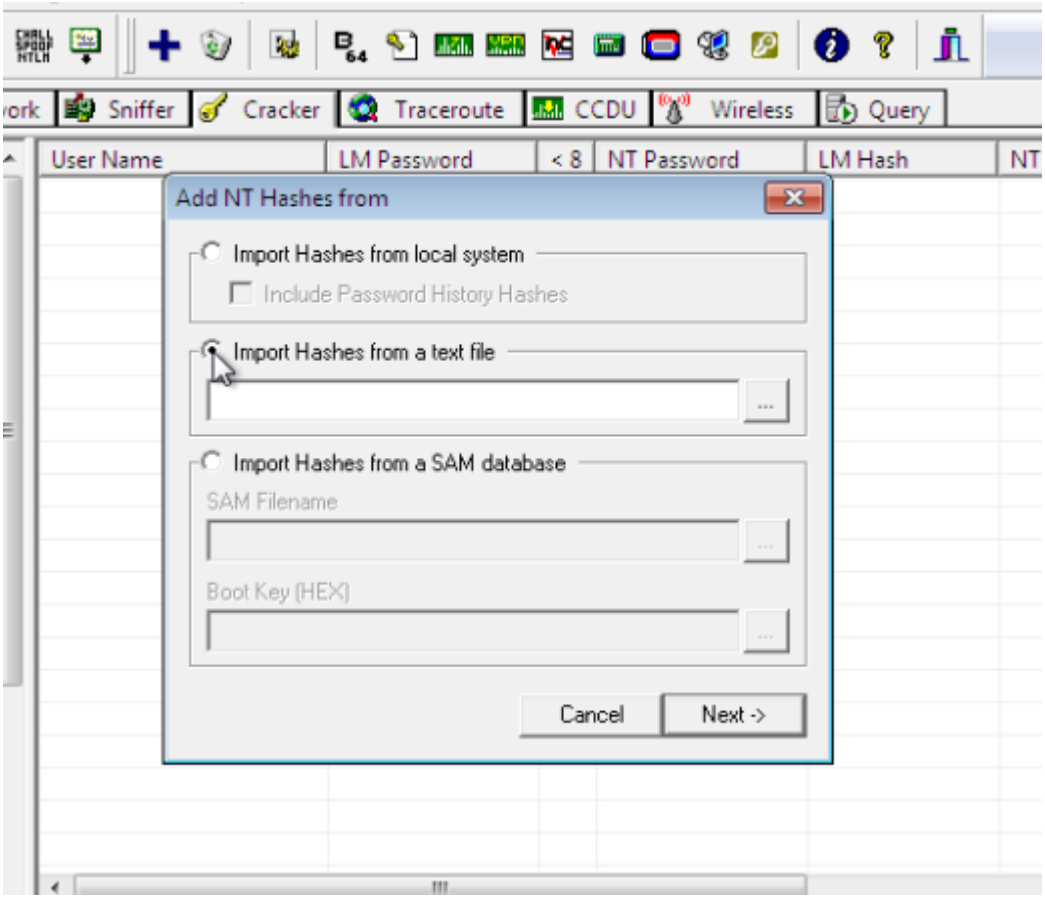
Gambar 6



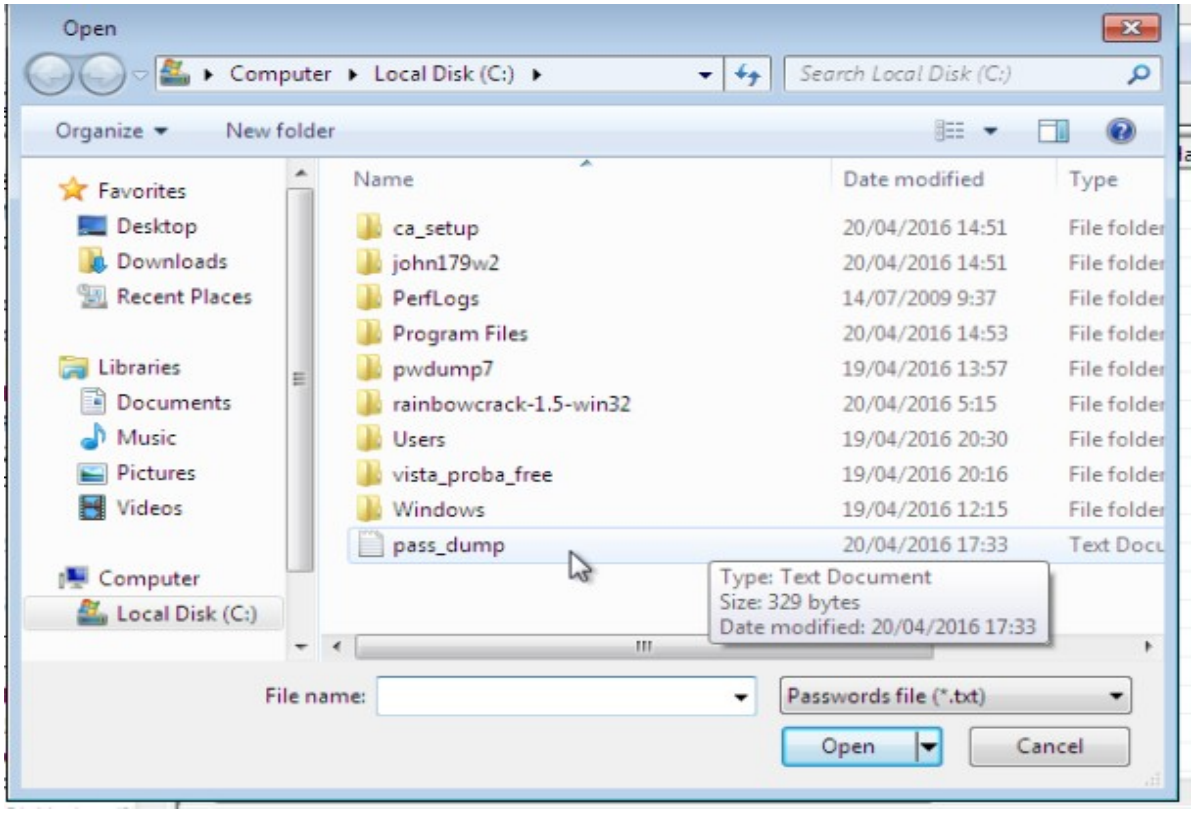
Gambar 7



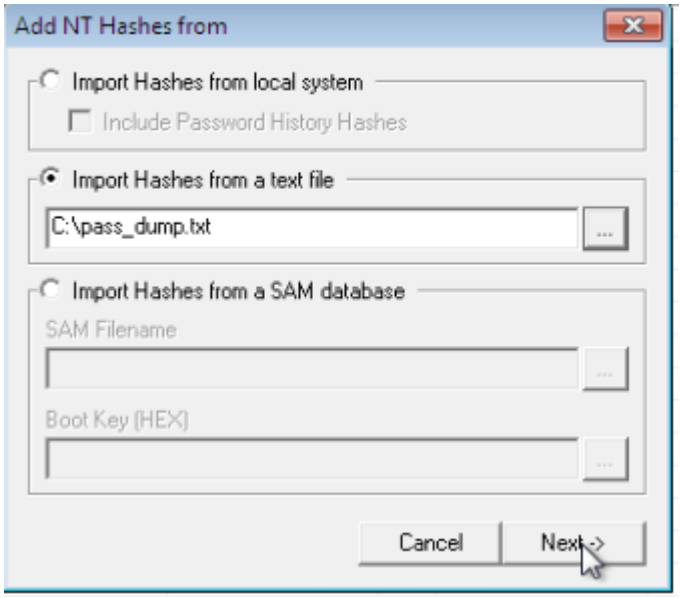
Gambar 8



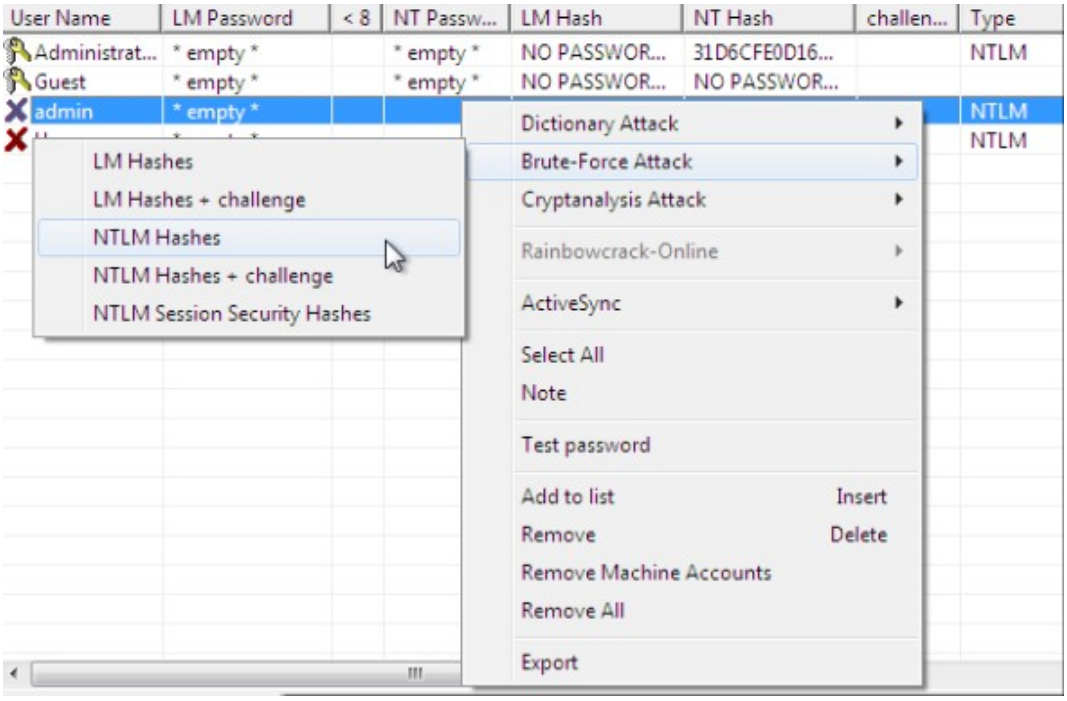
Gambar 9



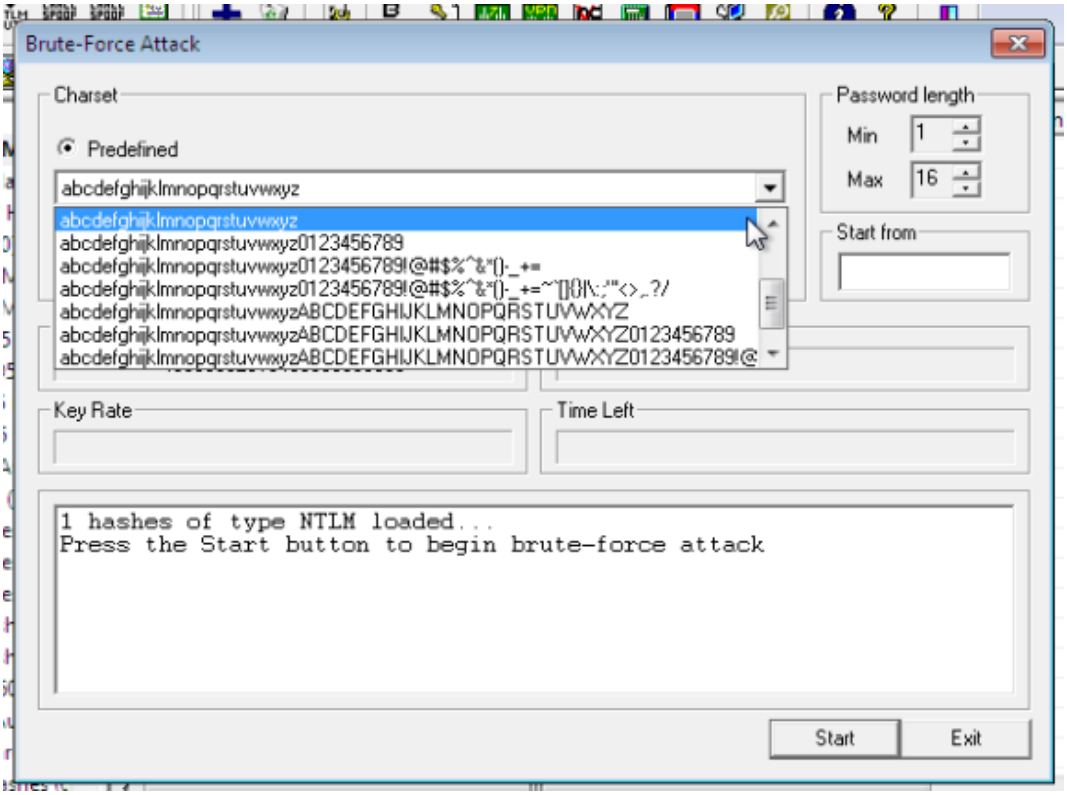
Gambar 10



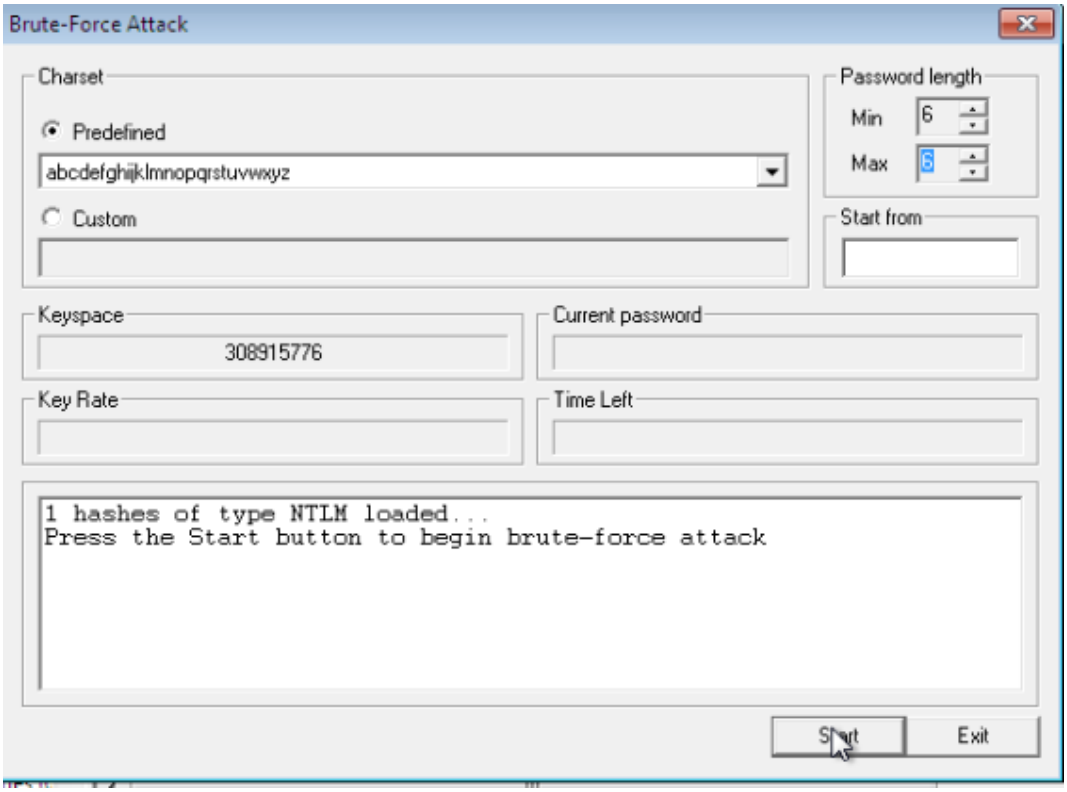
Gambar 11



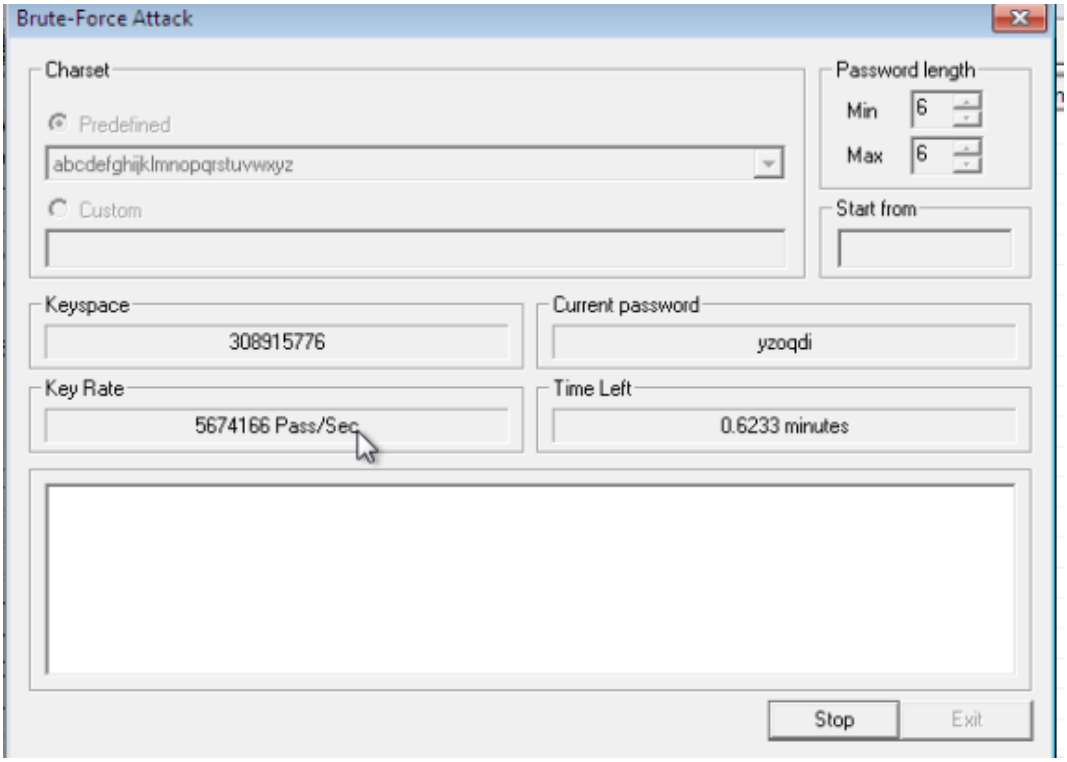
Gambar 12



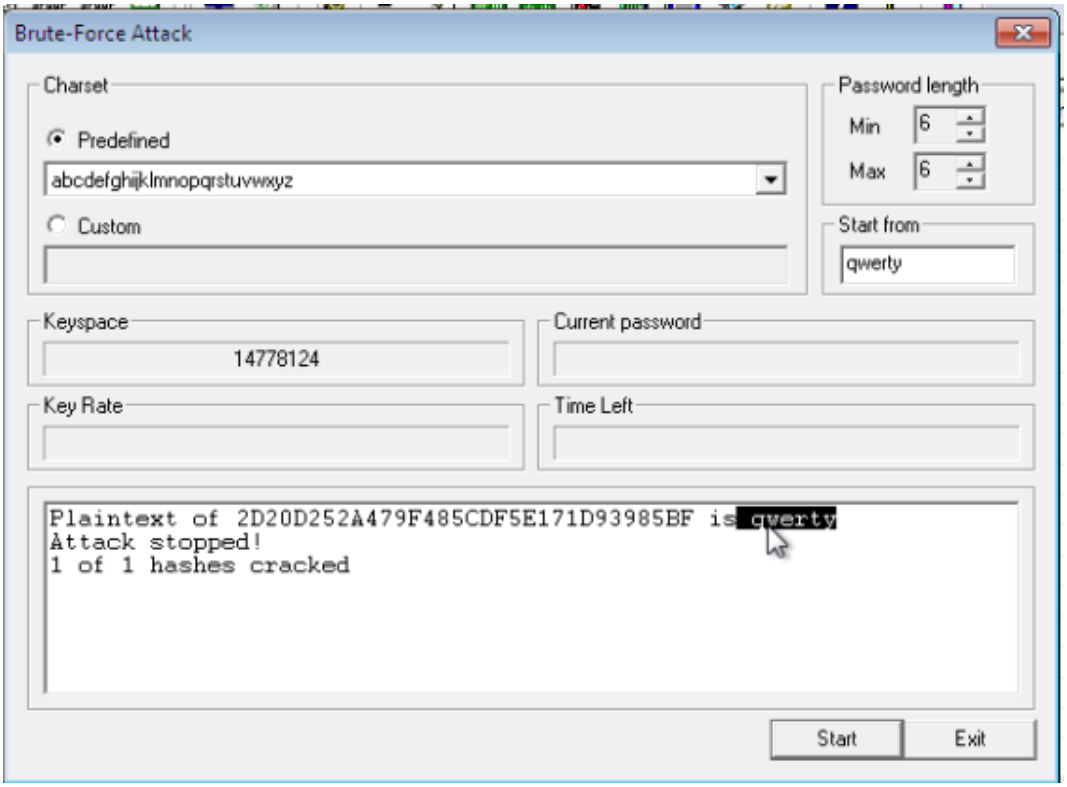
Gambar 13



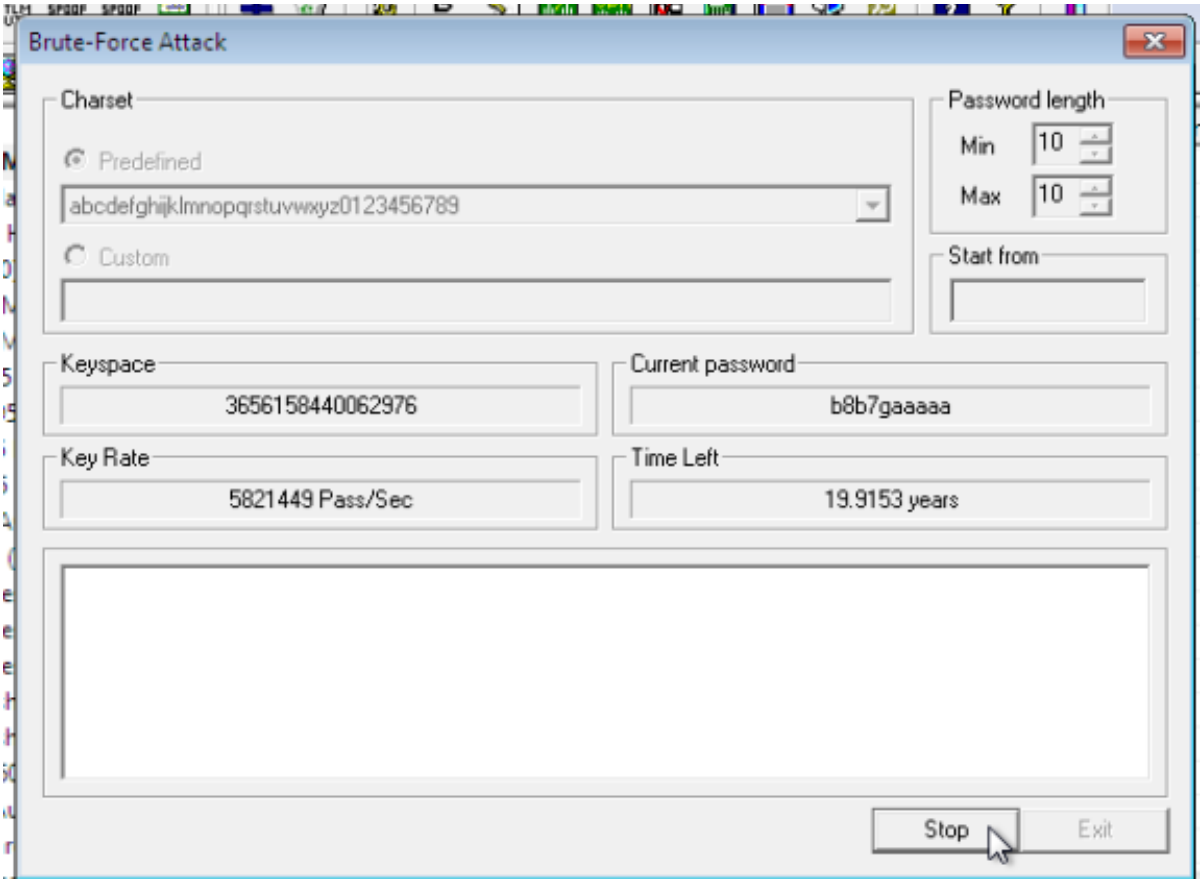
Gambar 14



Gambar 15



Gambar 16



Gambar 17

4.2 Analisa

Dari hasil yang didapat software password dump (Pwdump) dapat mengambil hash password yang tersimpan pada directory databasae yang berada pada sistem C:\Windows\System32\config\SAM. Namun untuk melakukan dump password pwdump harus menggunakan izin administrator dari sebuah sistem. Pada gambar 15 dan 17 merupakan proses cracking password dengan menggunakan cain & abel, yang mana pada gambar 15 dengan panjang string minimal 6 dan maximal 6 serta charset huruf kecil tanpa ada campuran dari kombinasi lain, password 6 karakter tersebut dengan mudah di pecahkan dengan waktu yang terbilang cepat, bahkan estimasi waktu yang dibutuhkan hanyalah beberapa menit. Namun pada gambar 17 yang merupakan proses pemecahan password milik User dengan username User yang mana menggunakan kombinasi angka dan abjad serta panjang string passwordnya sebanyak 10 karakter dibutuhkan waktu hingga 19 tahun lebih untuk memecahkan password tersebut (menurut estimasi waktu chain & abel). Sehingga dapat disimpulkan bahwa sekuat apapun algoritma enkripsi yang digunakan untuk enkripsi password, jika user memberikan password yang mudah untuk ditebak, maka algoritma yang kuat tersebut menjadi sia-sia.