Password Labs

Use ForSec Lab Computer

For this Password lab you will use your ForSec lab computer

You won’t use RADISH directly

But you will use files that you will load from your N: drive

Boot into Win8.1 on your ForSec Lab computer

Create a Win7 VM

Open VirtualBox (shortcut on your desktop)

Click on file>Import Appliance

Navigate in your N: drive to the folder named ***Shares*** and select ***Windows7Pro_OVAwtools***

Reset the MAC address

Take the defaults and click ***Import***

Wait until your machine is created. This will take up to 20 minutes

You should now see a Win7 VM on the left of the VirtualBox window

Start Win7

Install Guest Additions

To have easy access to the *Password Cracking* folder you can use a “share folder” between the host Win8.1 and the Win7 VM, but for this you will need to install the ***Guest Additions*** package.

- *In your Win 7 VM go to >Devices> Insert Guest Additions CD image*
- *Follow the installer instructions*
- *Then reboot your Win7 VM*
- *Go to Devices menu>Share Folders Settings> on the right top of the window there is a folder icon with a green plus sign, click on it and navigate to the* Password Cracking *folder.*
- *Now this folder will be mount as a drive in the VM (E:/)*

Disable Microsoft Security Essentials

Disable ***Microsoft Security Essentials***

Right click on ***green*** *castle icon on Toolbar*

A menu will pop up

*Click on the “***Settings***”* tab

Highlight “Real-time protection” in the left pane

Uncheck “Turn on real-time protection”

Save the changes

Wait until the icon shows that it is disabled by turning ***red***

Disable Windows Defender

To disable Windows Defender

Start > type defender and select Windows Defender

Go to tools menu click on Options > Realtime protection>

Uncheck all items

Click on the save button

Create Directories

Create a directory **on your desktop** named *passCrack*

Within it create the following directories and subdirectories as indicated

- \ophcrack\
  - *\software*
  - *\tables*
    - \vistaFree\
    - \vistaProbaFree\
- \pwdump7\

Populate the Directories

Navigate to ***N:\Password Cracking***

Copy ***ophcrack-win32-installer-3.6.0.exe*** into your ***passCrack\ophcrack\software\*** folder on your desktop

Copy ***pwdump7.zip*** into your ***passCrack\pwdump7\*** folder on your desktop

Copy ***vista_free.zip*** into your ***passCrack\tables\tablesVistaFree\*** folder on your desktop

Copy ***vista_proba_free.zip*** into your ***vistaProbaFree*** folder

This will take some time

Create Login Accounts

1. Right click on the *Start* icon in Windows 7
2. Navigate: *Start* -> *Control Panel* -> *Administrative Tools* -> *Computer Management* -> *Local Users and Groups* -> *Users*
3. Select *Action* -> *New user...*
4. Enter the 4 user names and passwords that are specified on the next slide
5. For each user name

   Enter the User name

   Leave **Full name** *and* **Description** *blank*

   Enter a password

   Uncheck "User must change password at next login"

Create Login Accounts

Using the instruction on the previous slide, create four simple user accounts on your computer using **<u>exactly</u>** the following

<u>names</u>	***<u>passwords</u>***
fredferd	*fred12*
<yourLastName>	*mydogspot*
<yourFirstName>	*tea4two*
charlie	*9simb0L1**

Lab 11b-1

pwdump7

Unzip pwdump7

Pwdump7 extracts the password hashes from the SAM files in Windows Vista, Win7 and, I think, Win8.

Doesn't need to be installed

Navigate to your ***pwdump7***\ folder

Unzip ***pwdump7.zip*** into this folder

You'll get 3 files: **pwdump7.exe**, **libeay32.dll**, **readme.txt**

pwdump7.exe needs libeay32.dll in the same directory

Run pwdump7

Open a command window **<u>as</u> <u>administrator</u>**

In your command window navigate to your desktop passCrack\pwdump7\ folder

Run the command

```
pwdump7 > pass.txt
```

This extracts all the login names and passwords and outputs them the the file *pass.txt* in your pwdump7 folder

This file will contain the account records including both the LM and NT password hashes

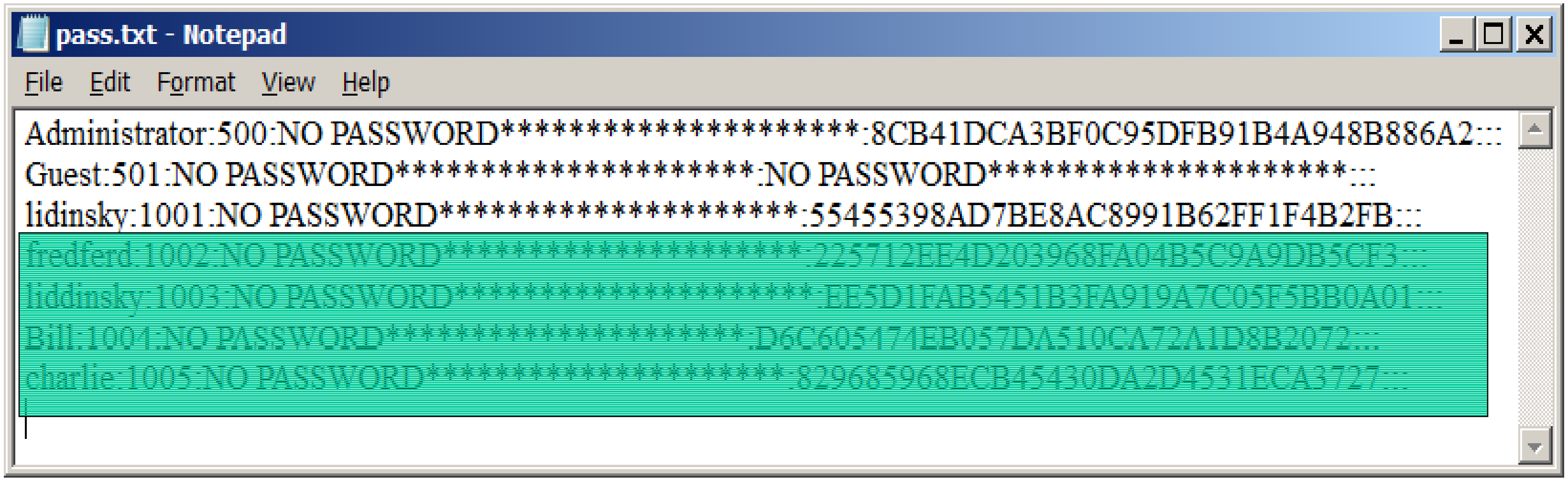
But in Win7 the default should be no LM hashes

View pass.txt

View the *pass.txt* file with Notepad

Expand the Notepad window horizontally to get 1 line per password

Here's my pass.txt file with the 4 test users



```
Administrator:500:NO PASSWORD*********************:8CB41DCA3BF0C95DFB91B4A948B886A2:::
Guest:501:NO PASSWORD*********************:NO PASSWORD*********************:::
lidinsky:1001:NO PASSWORD*********************:55455398AD7BE8AC8991B62FF1F4B2FB:::
fredferd:1002:NO PASSWORD*********************:225712EE4D203968FA04B5C9A9DB5CF3:::
liddinsky:1003:NO PASSWORD*********************:EE5D1FAB5451B3FA919A7C05F5BB0A01:::
Bill:1004:NO PASSWORD*********************:D6C605474EB057DA510CA72A1D8B2072:::
charlie:1005:NO PASSWORD*********************:829685968ECB45430DA2D4531ECA3727:::
```

Of course your last and first names will be different than mine

And I purposely misspelled my last name

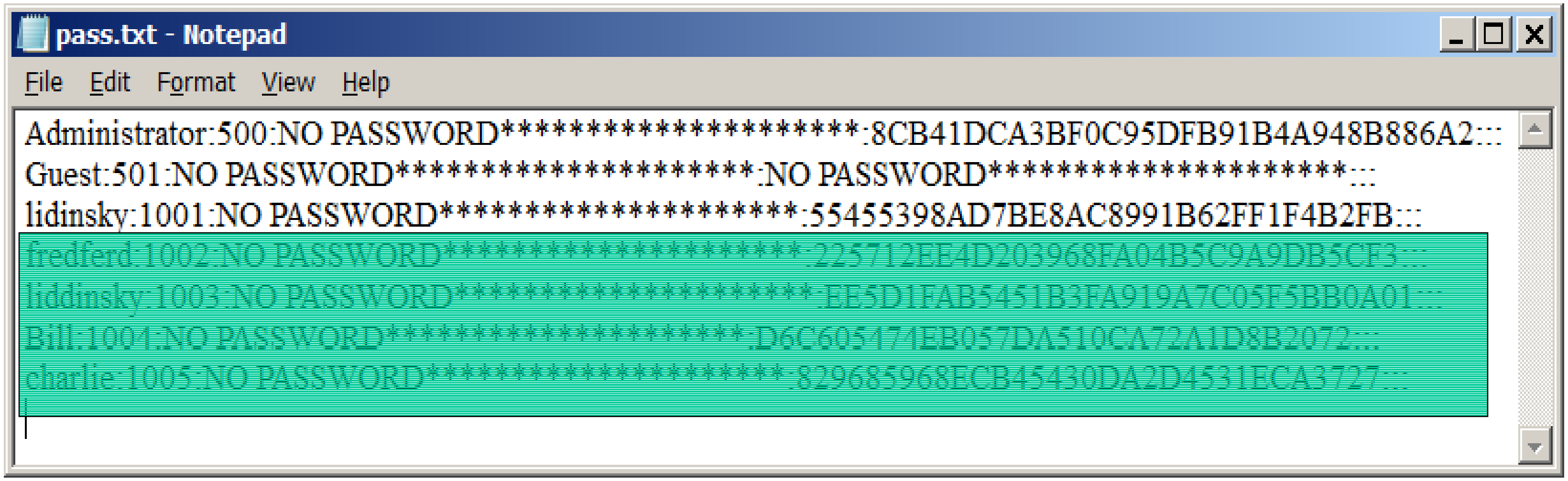
Interpreting the pass.txt file

Colons delimit the parts of the password

Format

Name : userID : LMhash : NThash : LMpwd1 : LMpwd2 : NTpwd

Note that there is no LM hash



```
Administrator:500:NO PASSWORD*********************:8CB41DCA3BF0C95DFB91B4A948B886A2:::
Guest:501:NO PASSWORD*********************:NO PASSWORD*********************:::
lidinsky:1001:NO PASSWORD*********************:55455398AD7BE8AC8991B62FF1F4B2FB:::
fredferd:1002:NO PASSWORD*********************:225712EE4D203968FA04B5C9A9DB5CF3:::
liddinsky:1003:NO PASSWORD*********************:EE5D1FAB5451B3FA919A7C05F5BB0A01:::
Bill:1004:NO PASSWORD*********************:D6C605474EB057DA510CA72A1D8B2072:::
charlie:1005:NO PASSWORD*********************:829685968ECB45430DA2D4531ECA3727:::
```

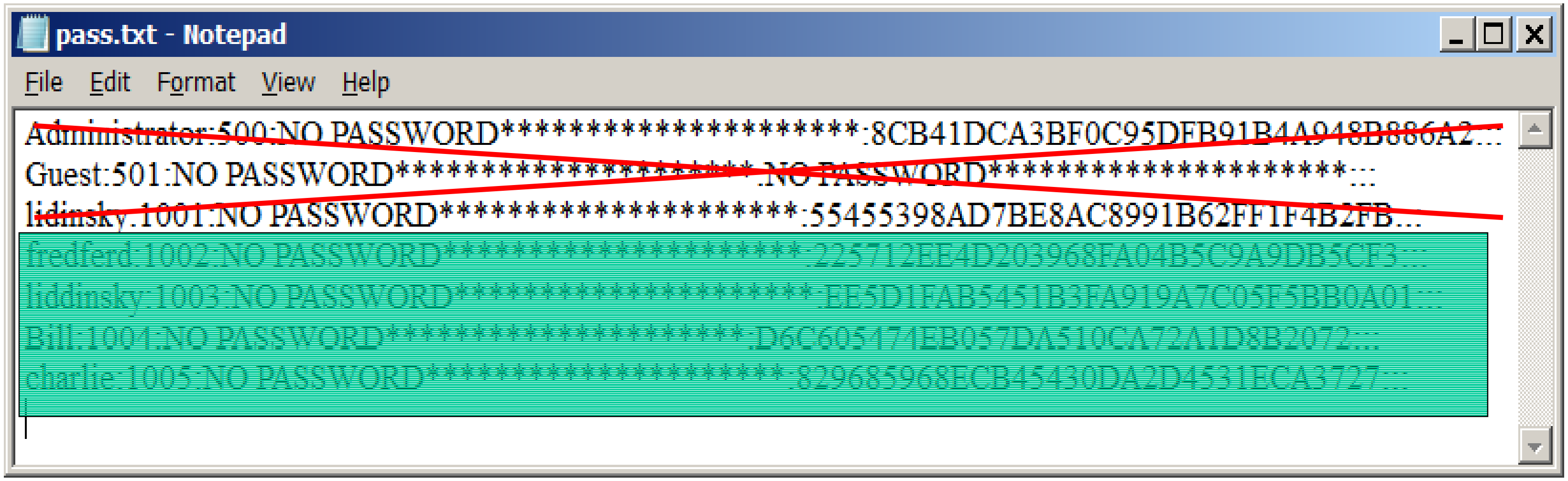
Culling pass.txt

Keep all the lines shown with a green overlay

fredferd , *yourLastName* , *yourFirstName* ***and*** *charlie*

Delete all other lines

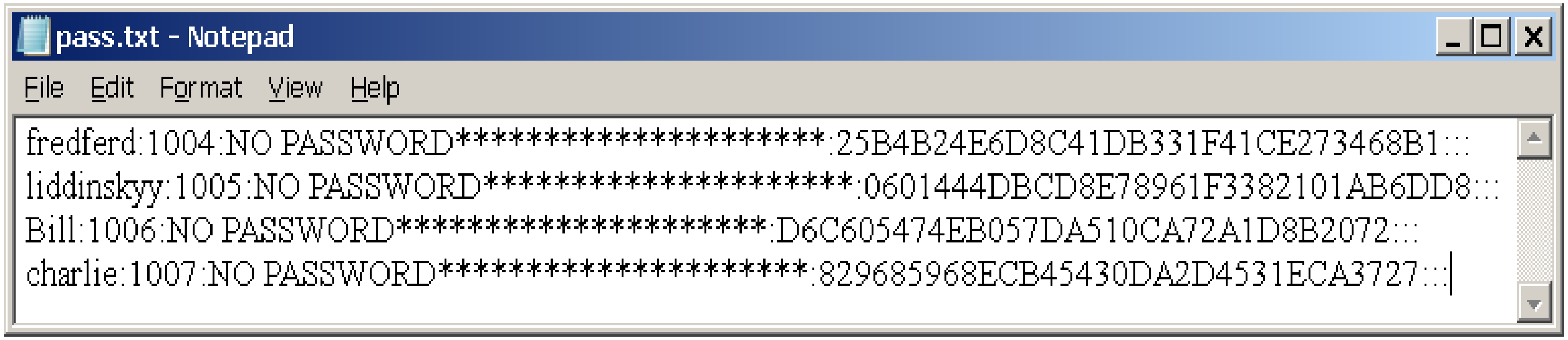
Also make sure that there are no blank lines at the beginning of the file



~~Administrator:500:NO PASSWORD*********************:8CB41DCA3BF0C95DFB91B4A948B886A2:::~~
~~Guest:501:NO PASSWORD*********************:NO PASSWORD*********************:::~~
~~lidinsky:1001:NO PASSWORD*********************:55455398AD7BE8AC8991B62FF1F4B2FB:::~~
fredferd:1002:NO PASSWORD*********************:225712EE4D203968FA04B5C9A9DB5CF3:::
liddinsky:1003:NO PASSWORD*********************:EE5D1FAB5451B3FA919A7C05F5BB0A01:::
Bill:1004:NO PASSWORD*********************:D6C605474EB057DA510CA72A1D8B2072:::
charlie:1005:NO PASSWORD*********************:829685968ECB45430DA2D4531ECA3727:::

Culling pass.txt

You now should have only 4 lines as shown



```
fredferd:1004:NO PASSWORD*********************:25B4B24E6D8C41DB331F41CE273468B1:::
liddinskyy:1005:NO PASSWORD*********************:0601444DBCD8E78961F3382101AB6DD8:::
Bill:1006:NO PASSWORD*********************:D6C605474EB057DA510CA72A1D8B2072:::
charlie:1007:NO PASSWORD*********************:829685968ECB45430DA2D4531ECA3727:::
```

Save this file on your desktop in

passCrack\pwdump7\4testPwds.txt

Lab 11b-2

ophcrack

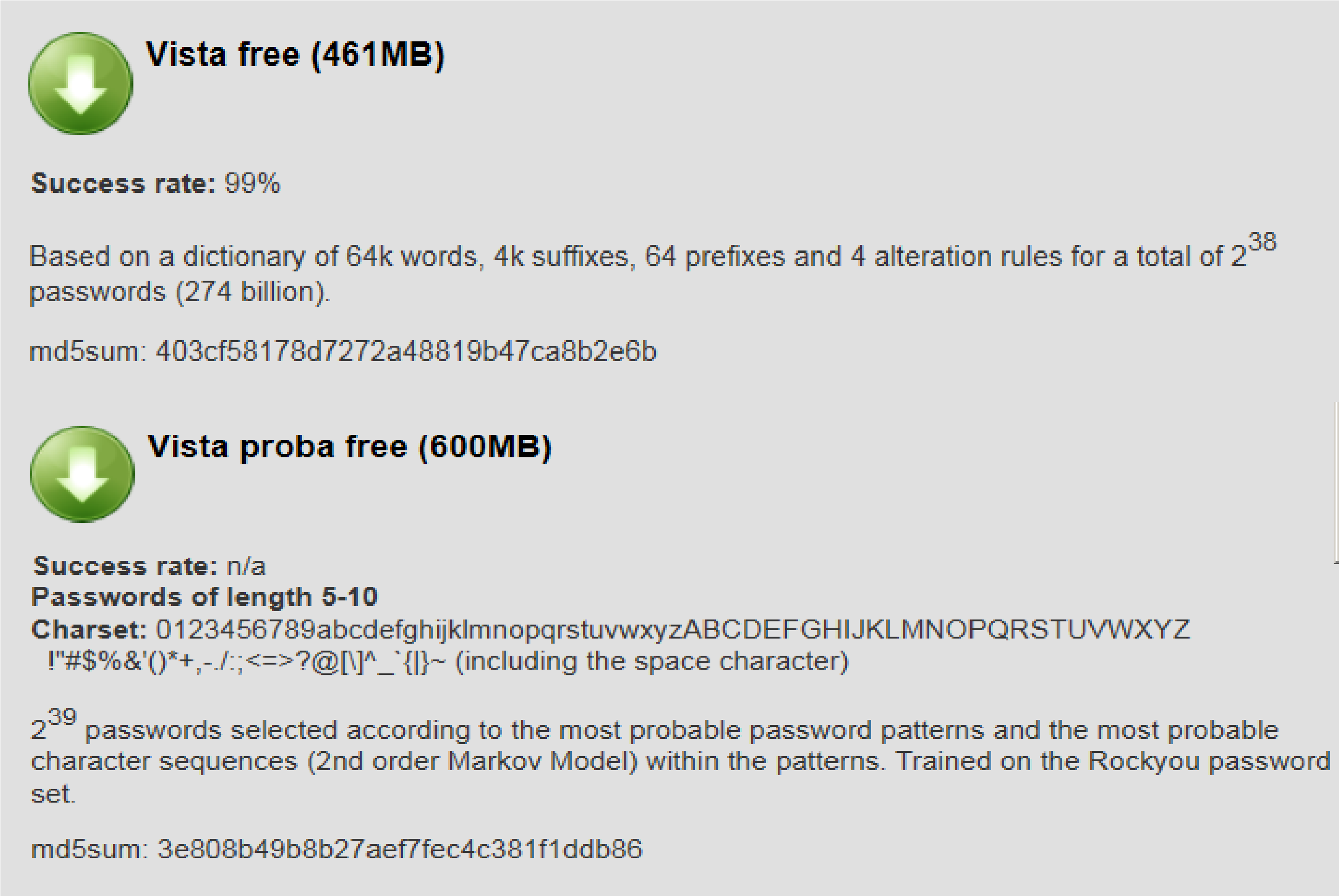
Overview of ophcrack

Ophcrack comes in several different forms

- *An executable*
  - For vista and later
  - For XP
  - For Linux
  - Needs one or more sets of tables to use
  - Tables are different for XP and vista
- *A bootable CD*
  - Includes a small set of tables

We will use vista in this session

Ophcrack Claims



Vista free (461MB)

Success rate: 99%

Based on a dictionary of 64k words, 4k suffixes, 64 prefixes and 4 alteration rules for a total of 2^{38} passwords (274 billion).

md5sum: 403cf58178d7272a48819b47ca8b2e6b

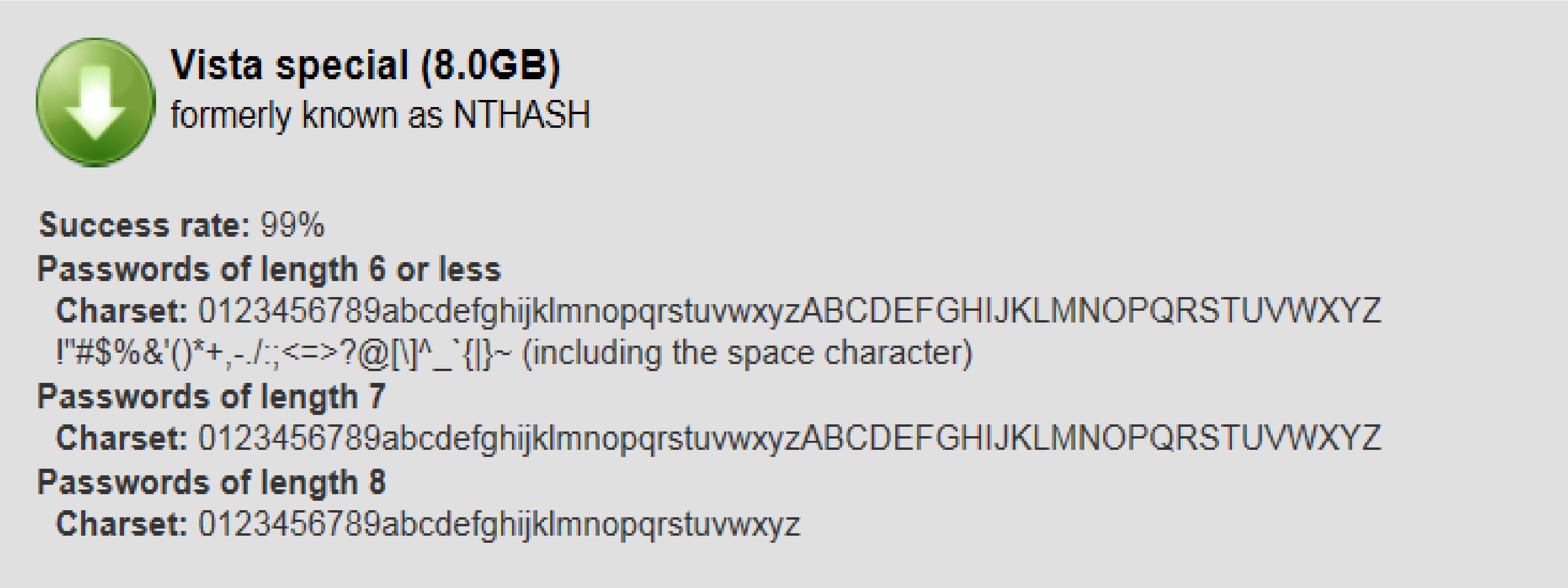
Vista proba free (600MB)

Success rate: n/a
Passwords of length 5-10
Charset: 0123456789abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ
!"#$%&'()*+,-./:;<=>?@[\]^_`{|}~ (including the space character)

2^{39} passwords selected according to the most probable password patterns and the most probable character sequences (2nd order Markov Model) within the patterns. Trained on the Rockyou password set.

md5sum: 3e808b49b8b27aef7fec4c381f1ddb86

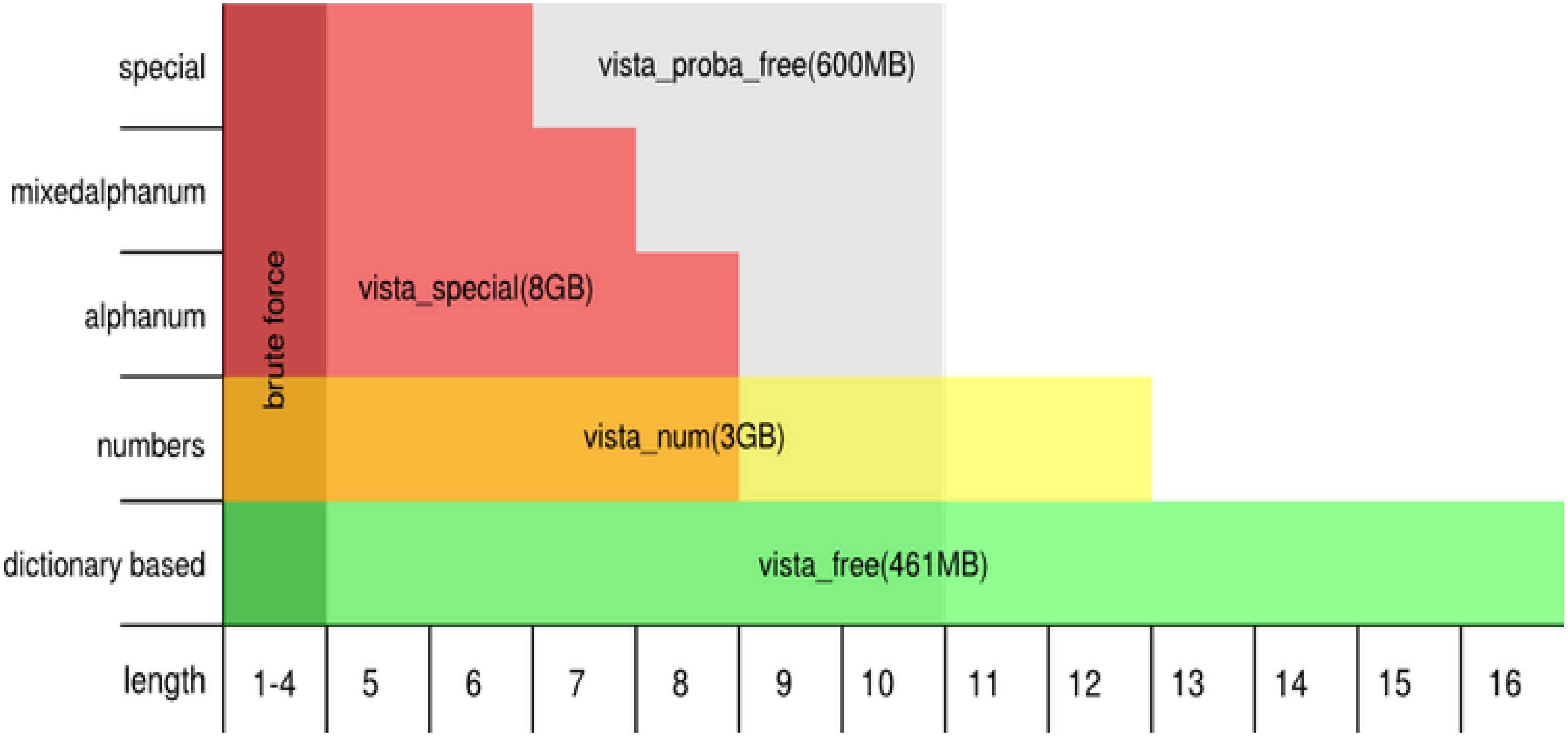
Ophcrack Claims



Vista special (8.0GB)
formerly known as NTHASH

Success rate: 99%
Passwords of length 6 or less
Charset: 0123456789abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ !"#$%&'()*+,-./:;<=>?@[\]^_`{|}~ (including the space character)
Passwords of length 7
Charset: 0123456789abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ
Passwords of length 8
Charset: 0123456789abcdefghijklmnopqrstuvwxyz

Ophcrack Claims



Install ophcrack

Run ***ophcrack-win32-installer-3.6.0.exe*** to install ophcrack

- *Uncheck all the boxes that automatically include tables*
- *Take the defaults for the rest of the choices*

For the .zip files that you copied to your new folders

- *Unzip all of them in their respective folders*

Choose Tables in ophcrack

Now start ophcrack

Click on the *Tables* icon to bring up the *Table Selection* window

Choose *Vista probabilistic free* tables

Click *Install*

Navigate to your folder *vista_proba_free*

Click *Select Folder*

Next choose *Vista free* tables

Click *Install*

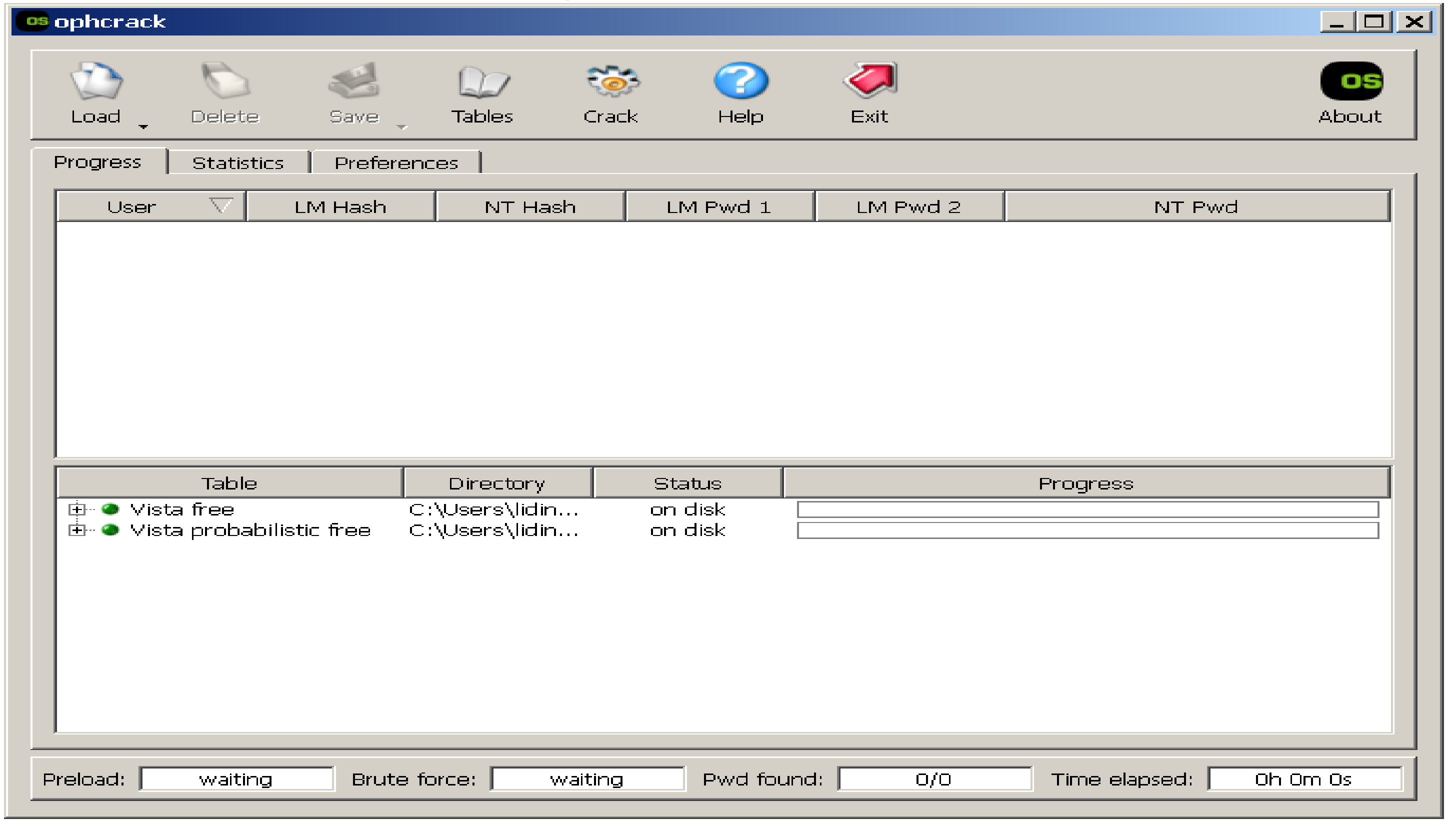
Navigate to your folder *vistaFree*

Click *Select Folder*

Choose Tables in ophcrack

You should now see that the tables have been enabled

Green dot and table entry in the lower pane of ophcrack



User	LM Hash	NT Hash	LM Pwd 1	LM Pwd 2	NT Pwd

Table	Directory	Status	Progress
⊞ ● Vista free	C:\Users\lidin...	on disk	
⊞ ● Vista probabilistic free	C:\Users\lidin...	on disk	

Preload: waiting Brute force: waiting Pwd found: 0/0 Time elapsed: 0h 0m 0s

Load Target File

Choose *Load* > *PWDUMP file*

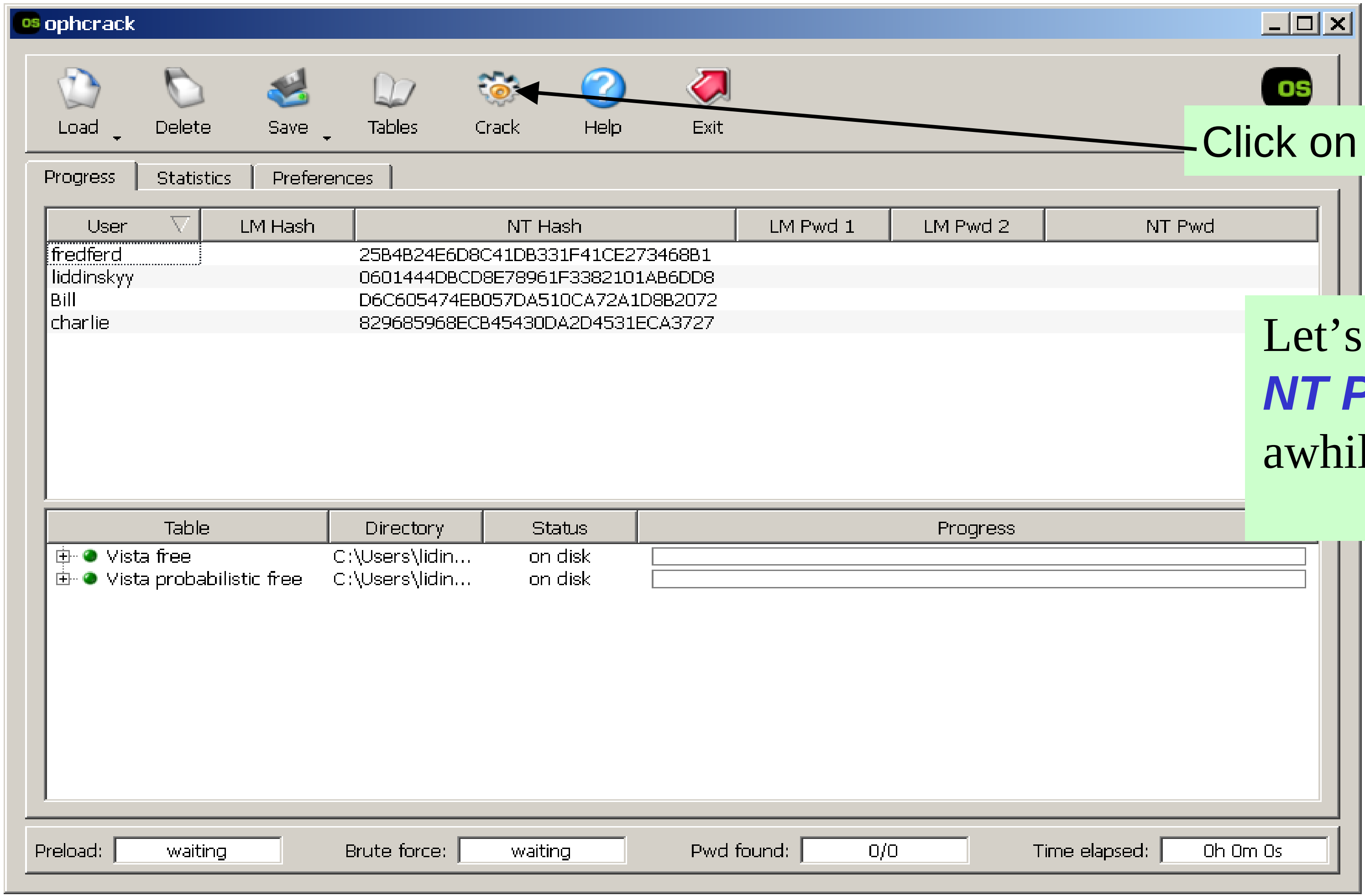
Navigate to *4testPwds.txt*

You should now see the target file in the upper pane of the ophcrack window, both user name and NT hash

__NT Pwd__s are not yet shown

See next slide

Crack Passwords



User	LM Hash	NT Hash	LM Pwd 1	LM Pwd 2	NT Pwd
fredferd		25B4B24E6D8C41DB331F41CE273468B1			
liddinskyy		0601444DBCD8E78961F3382101AB6DD8			
Bill		D6C605474EB057DA510CA72A1D8B2072			
charlie		829685968ECB45430DA2D4531ECA3727			

Table	Directory	Status	Progress
Vista free	C:\Users\lidin...	on disk	
Vista probabilistic free	C:\Users\lidin...	on disk	

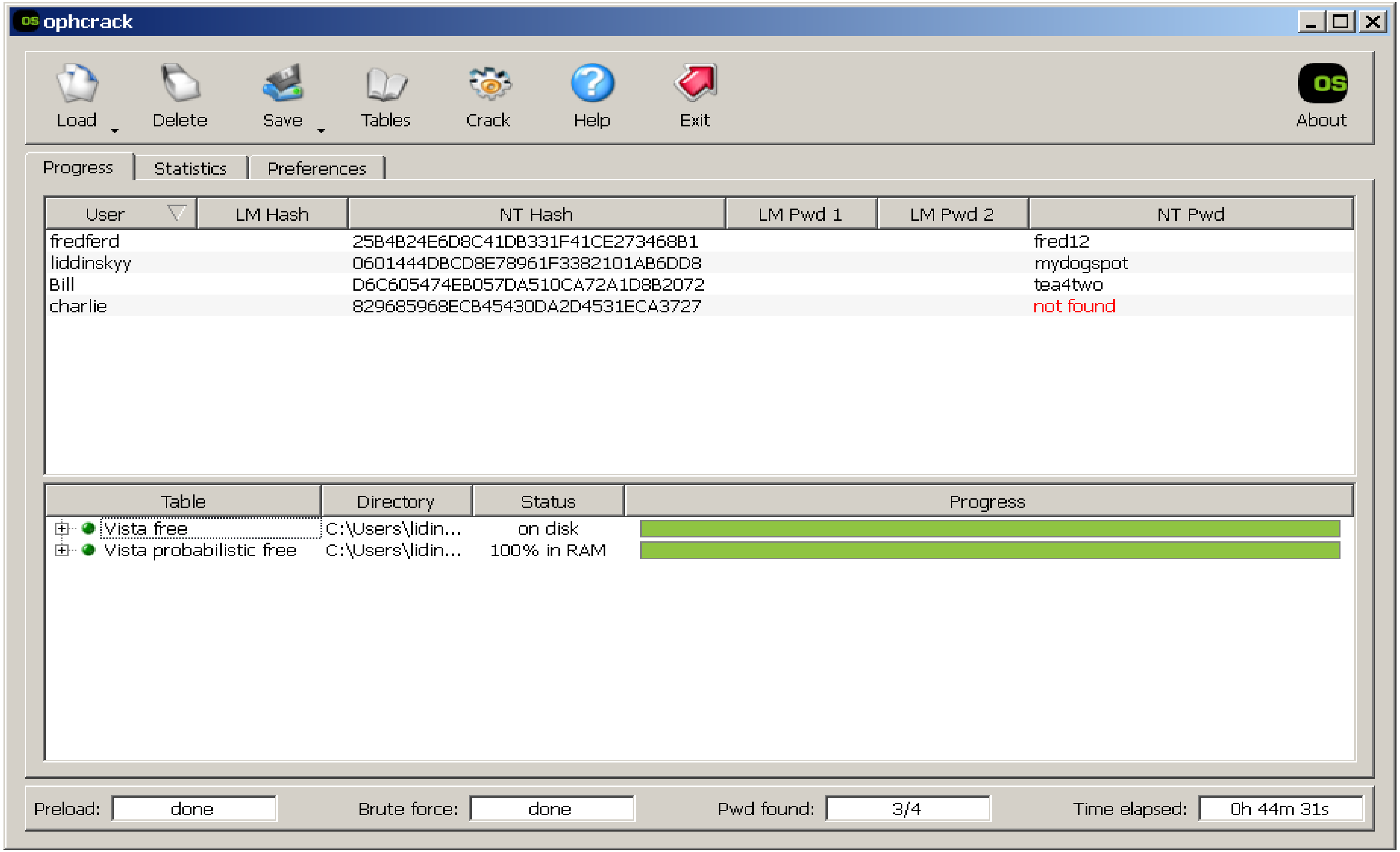
Preload: waiting Brute force: waiting Pwd found: 0/0 Time elapsed: 0h 0m 0s

Click on ***Crack***

Let’s watch ***NT Pwd*** for awhile

Results

Ophcrack

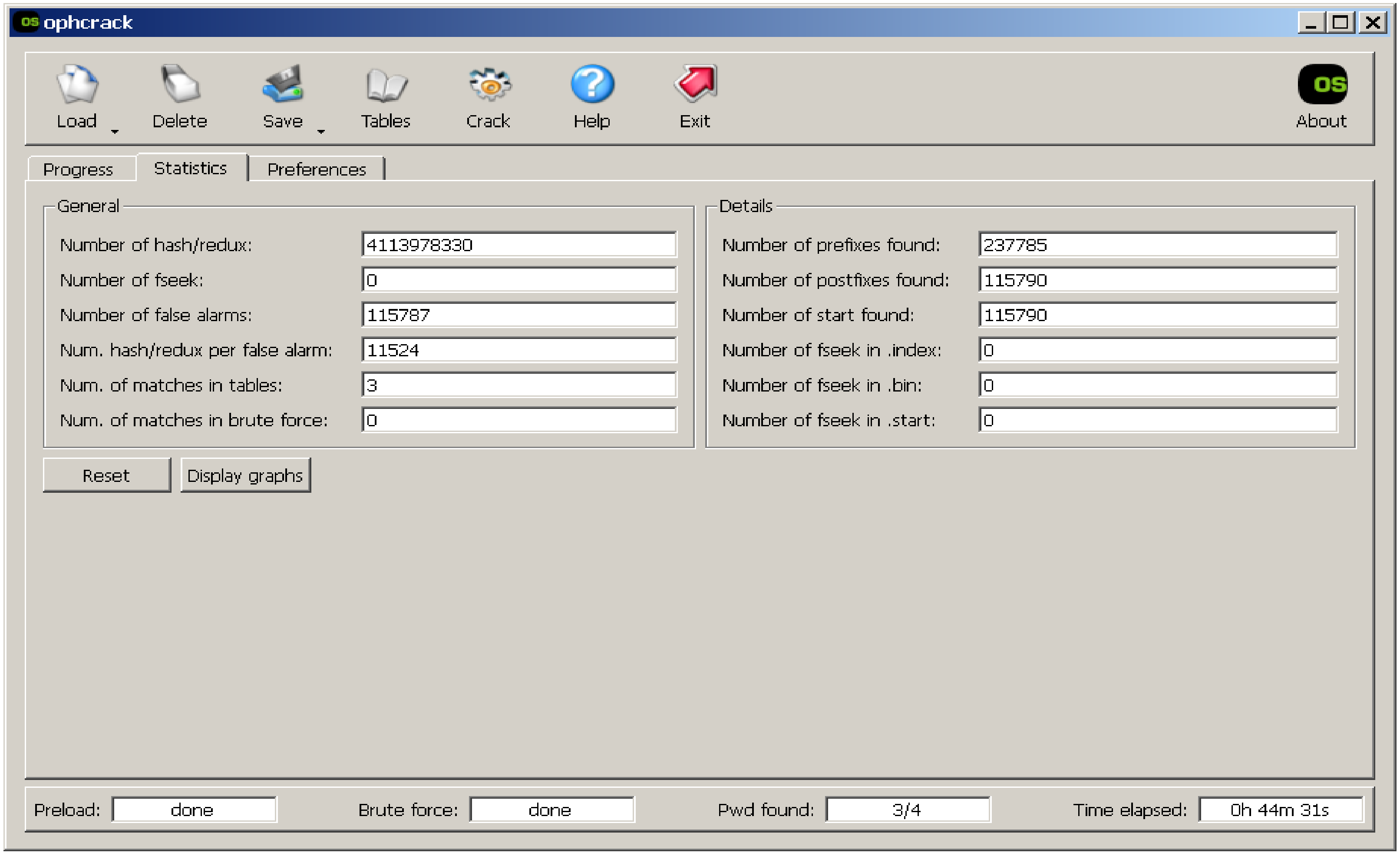


User	LM Hash	NT Hash	LM Pwd 1	LM Pwd 2	NT Pwd
fredferd		25B4B24E6D8C41DB331F41CE273468B1			fred12
liddinskyy		0601444DBCD8E78961F3382101AB6DD8			mydogspot
Bill		D6C605474EB057DA510CA72A1D8B2072			tea4two
charlie		829685968ECB45430DA2D4531ECA3727			not found

Table	Directory	Status	Progress
Vista free	C:\Users\lidin...	on disk	
Vista probabilistic free	C:\Users\lidin...	100% in RAM	

Preload: done Brute force: done Pwd found: 3/4 Time elapsed: 0h 44m 31s

Statistics
Ophcrack



General

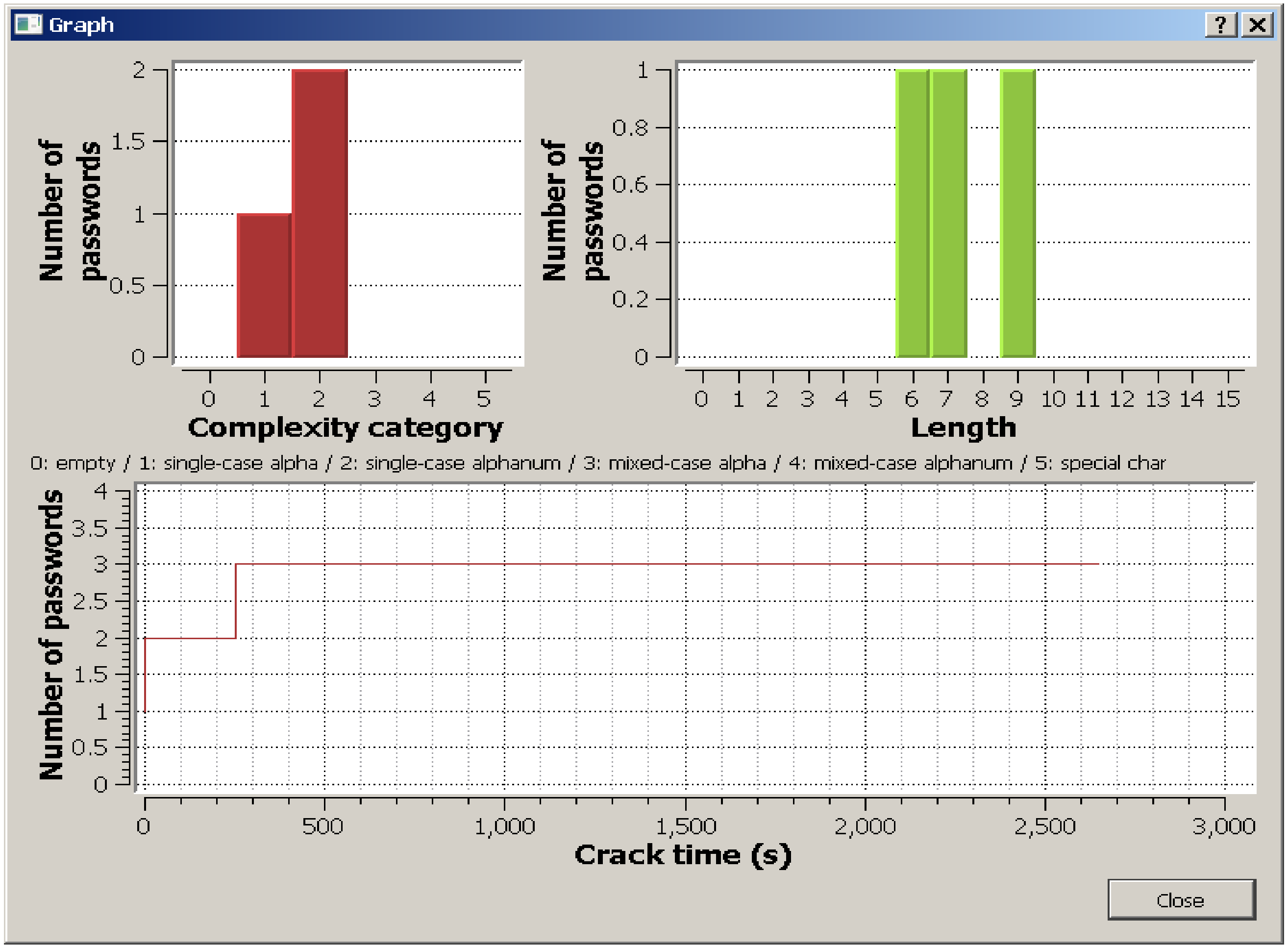
Number of hash/redux:	4113978330
Number of fseek:	0
Number of false alarms:	115787
Num. hash/redux per false alarm:	11524
Num. of matches in tables:	3
Num. of matches in brute force:	0

Details

Number of prefixes found:	237785
Number of postfixes found:	115790
Number of start found:	115790
Number of fseek in .index:	0
Number of fseek in .bin:	0
Number of fseek in .start:	0

Preload: done Brute force: done Pwd found: 3/4 Time elapsed: 0h 44m 31s

Statistics Graphs
Ophcrack


Graph
?
×
Number of passwords
2
1.5
1
0.5
0
0
1
2
3
4
5
Complexity category
Number of passwords
1
0.8
0.6
0.4
0.2
0
0
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
Length
0: empty / 1: single-case alpha / 2: single-case alphanum / 3: mixed-case alpha / 4: mixed-case alphanum / 5: special char
Number of passwords
4
3.5
3
2.5
2
1.5
1
0.5
0
0
500
1,000
1,500
2,000
2,500
3,000
Crack time (s)
Close