



IT Alley
4742 42nd Ave SW #272
Seattle, WA 98116-4553
www.italleypllc.com
sales@italleypllc.com



Article by How-To Geek

[How to Crack Your Forgotten Windows Password](#)



Here at How-To Geek, we've covered many different ways to reset your password for Windows—but what if you can't reset your password? Or what if you're using drive encryption that would wipe out your files if you changed the password? It's time to crack the password instead.

To accomplish this, we'll use a tool called Ophcrack that can crack your password so you can login without having to change it.

Download Ophcrack

The first thing we will need to do is download the CD image from Ophcrack's website. There are two options to download, XP or Vista, so make sure you grab the right one. The Vista download works with Windows Vista or Windows 7, and the only difference between XP and Vista is the "tables" Ophcrack uses to determine the password.

Download ophcrack LiveCD

The latest version of ophcrack LiveCD is 2.3.1 (including ophcrack 3.3.1)



ophcrack XP LiveCD

ophcrack-xp-livecd-2.3.1.iso

md5sum: 1332a09a351b3f05a7524dded9cdecb1

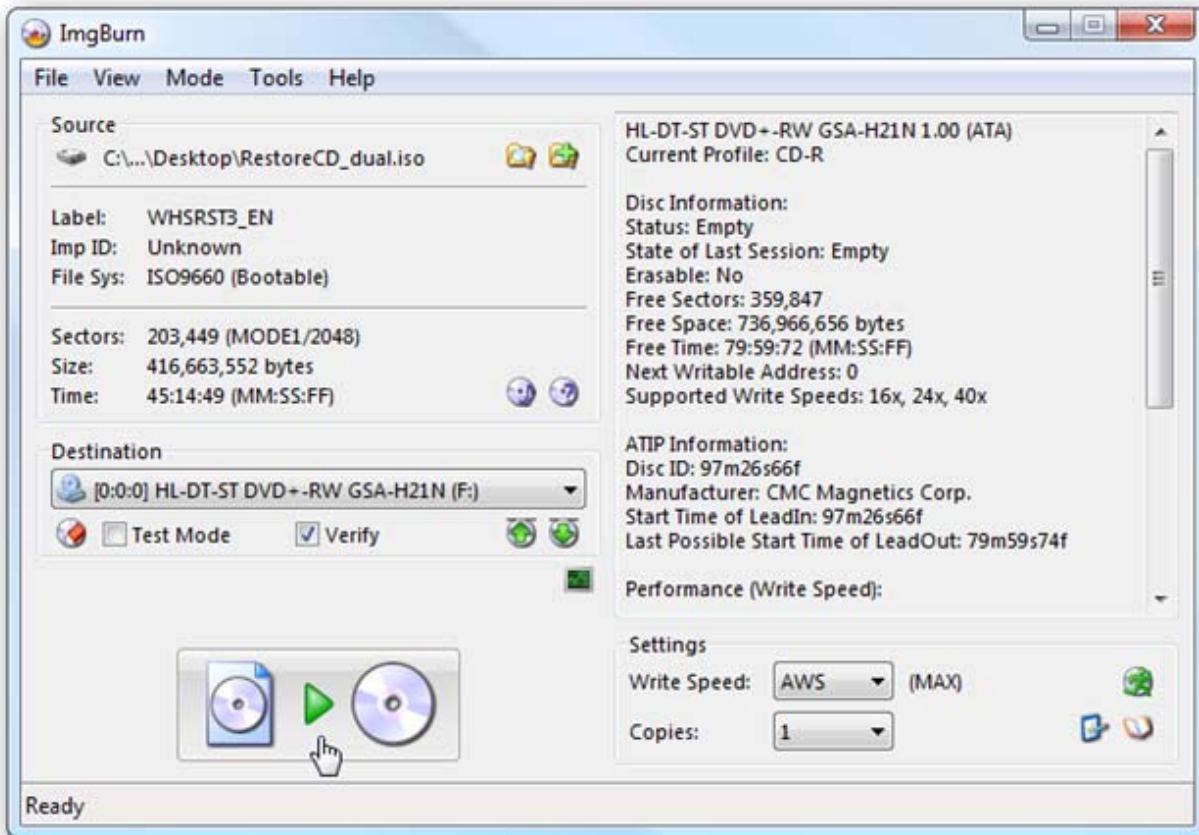


ophcrack Vista LiveCD

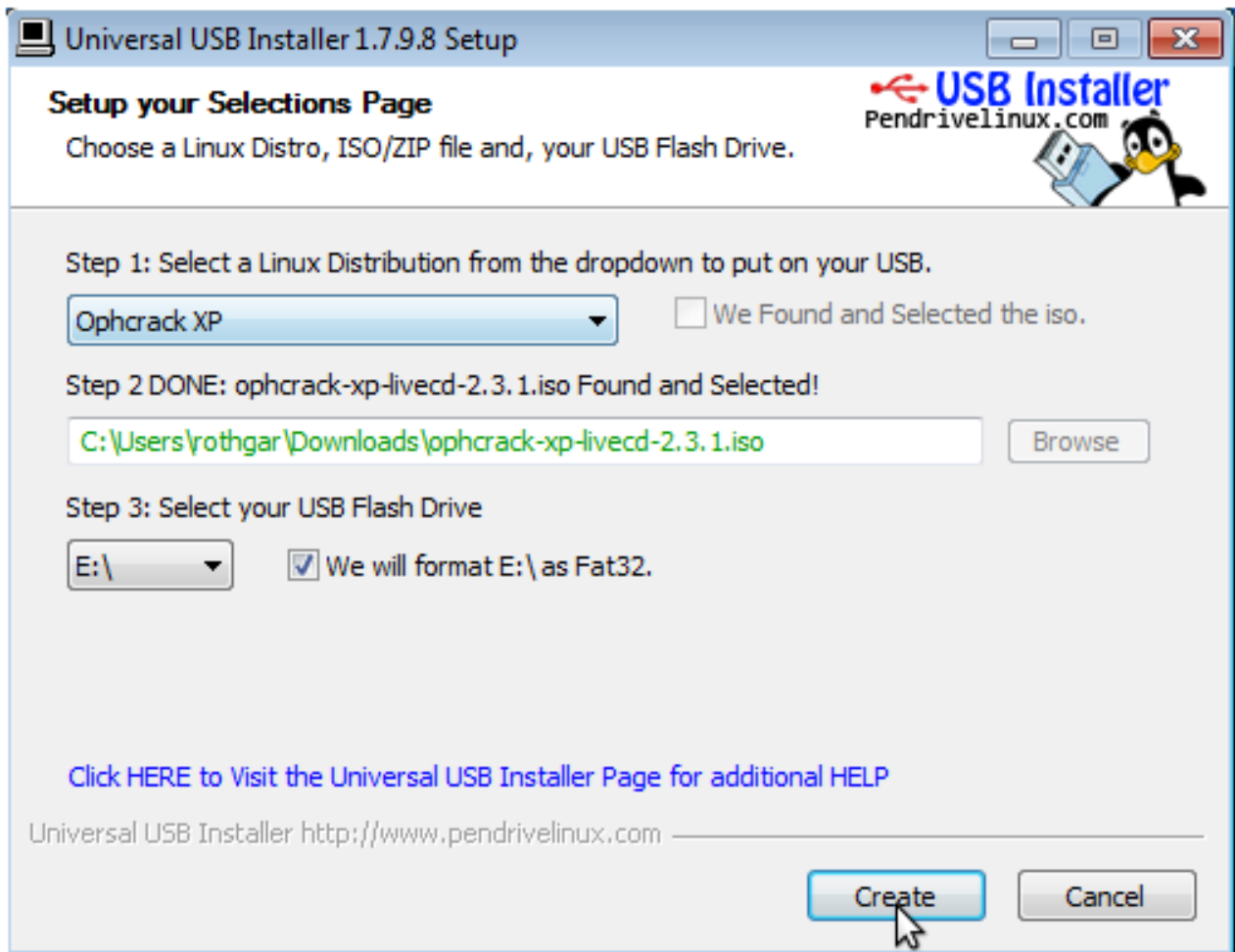
ophcrack-vista-livecd-2.3.1.iso

md5sum: 080a75ed7af82b58b1659ec1a88a15c4

Once the .iso file is downloaded, burn it to a CD using the guide below.

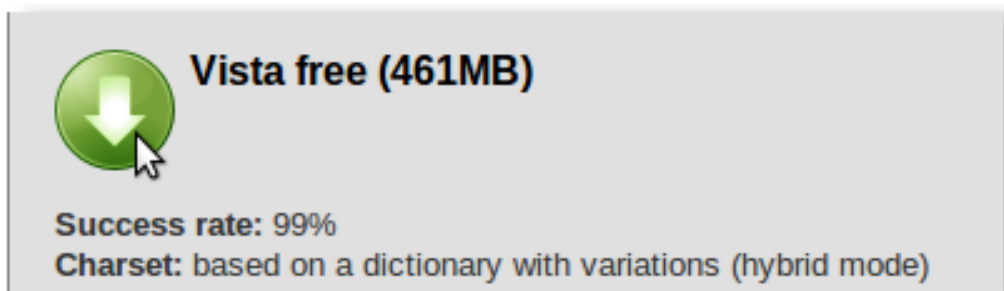


If you are going to be cracking your password on something that doesn't have a CD drive, such as a netbook, download the universal USB creator from PenDrive Linux (Link Below). A USB drive will not only run faster but you can also use a single USB drive for Windows XP, Vista, and 7 if you copy the needed tables to the drive.

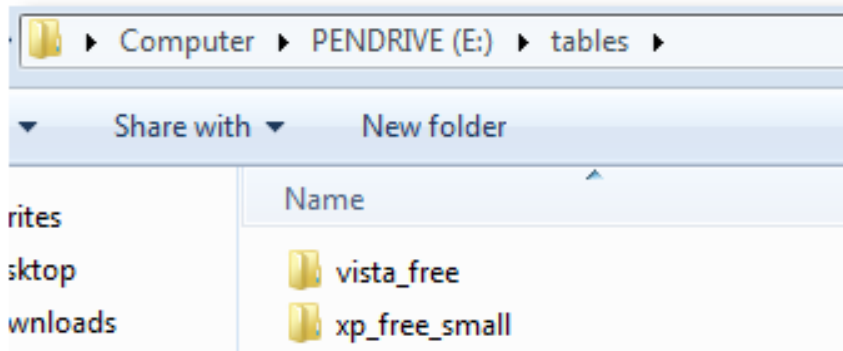


To create a USB drive that works with all versions of Windows, download the free password tables from Ophcrack's website.

Note: There are free tables available on Ophcrack's website and there are paid tables, the paid tables will typically get the job done faster and will be able to crack more complex passwords but the paid tables may not fit on a USB drive because they range in size from 3 GB to 135 GB.



Now extract the tables to \tables\vista_free on the USB drive and they will be used automatically by Ophcrack.



Boot from CD/USB

Boot the computer from the CD or USB drive that you created.

Note: On some computers you may have to go into the BIOS settings to change the boot order or push a key to show the boot menu.

ophcrack LiveCD



running on...



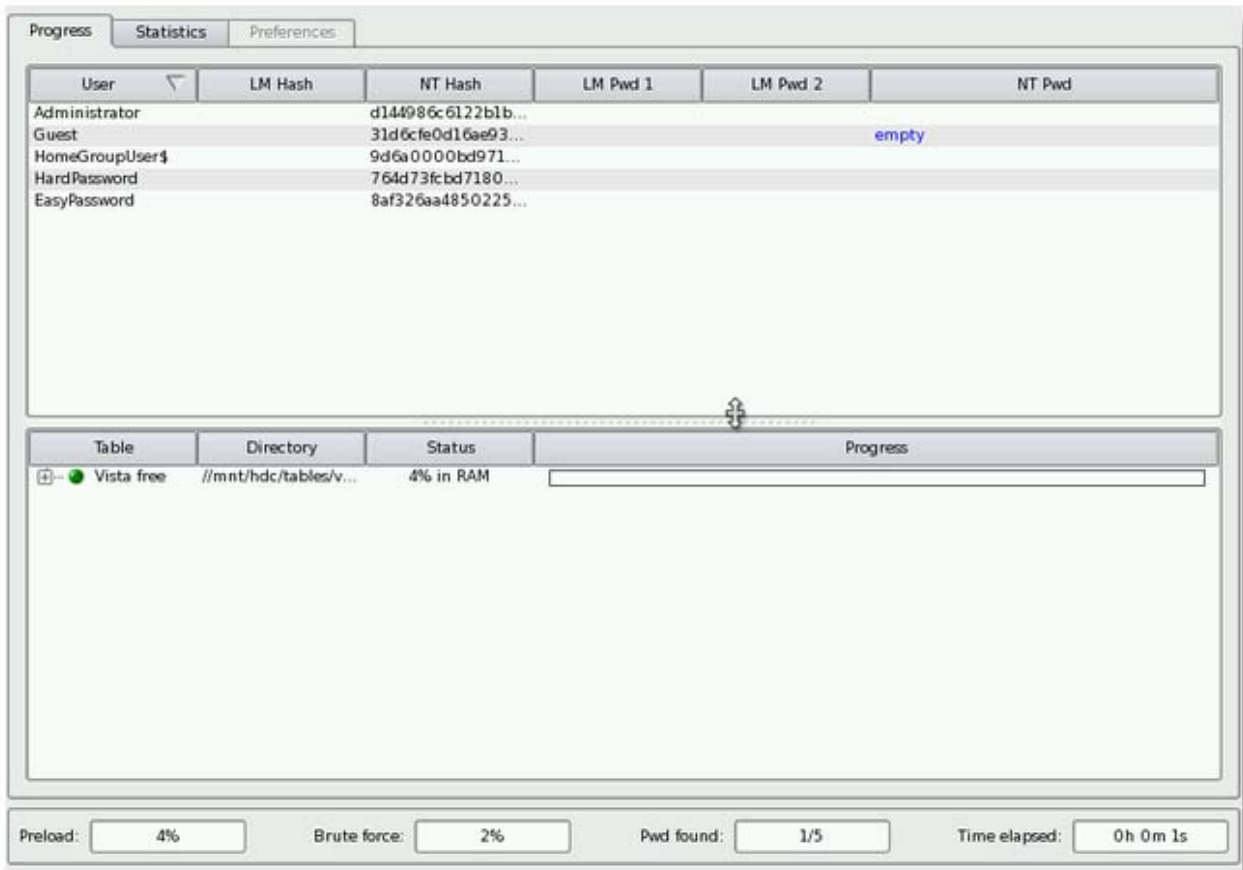
```
Ophcrack Graphic mode - automati
Ophcrack Graphic mode - manual
Ophcrack Graphic mode - low RAM
Ophcrack Text mode
```

Run ophcrack GUI automatically:

```
Graphics mode 1024x768
English language
and US keyboard
```

Once the disk is done booting, Ophcrack should start automatically and will begin cracking the passwords for all of the users on your computer.

Note: If the computer boots and you only have a blank screen or Ophcrack doesn't start, try restarting the computer and selecting manual or low RAM options on the live CD boot menu.



If you have a complex password it will take a lot longer than simple passwords, and with the free tables your password may never be cracked. Once the crack is done you will see the password in plain text, write it down and reboot the machine to login. If your password isn't cracked, you can also log in as one of the other users with admin rights and then change your password from within Windows.

User	LM Hash	NT Hash	LM Pwd 1	LM Pwd 2	NT Pwd
Administrator		d144986c6122b1b...			Administrator
Guest		31d6cfe0d16ae93...			empty
HomeGroupUser\$		9d6a0000bd971...			not found
HardPassword		764d73fcbd7180...			not found
EasyPassword		8af326aa4850225...			1234567890

With the free tables available you will not be able to crack every password, but the paid tables range from \$100 to \$1000 so you may be better off just resetting your password with on of these tutorials:

- [Reset password with Ubuntu live CD](#)
- [Change password with Linux System Rescue CD](#)

- [Reset password with Ultimate Boot CD](#)
- [Reset password with password reset disk](#)

You can get all of the software needed for password cracking from these links.

- [Ophcrack homepage](#)
- [Burn an iso file to disc](#)
- [Pendrive Linux Universal USB creator](#)

If you aren't using drive encryption and you've got a tough password, it's usually much faster to reset the password using one of the tools above, but we like to show you all the different techniques that you can use.

This article was originally written on 09/28/10

Pasted from <<http://www.howtogeek.com/howto/29694/how-to-crack-your-forgotten-windows-password/>>