Bypassing Windows Passwords with Hiren Boot CD

@mmar

Hiren Boot CD is an alternative utility for Konboot to bypass windows passwords which is totally free. The ISO is based on on Windows 10 PE x64 and contains many tools to repair Windows problems

Attacks

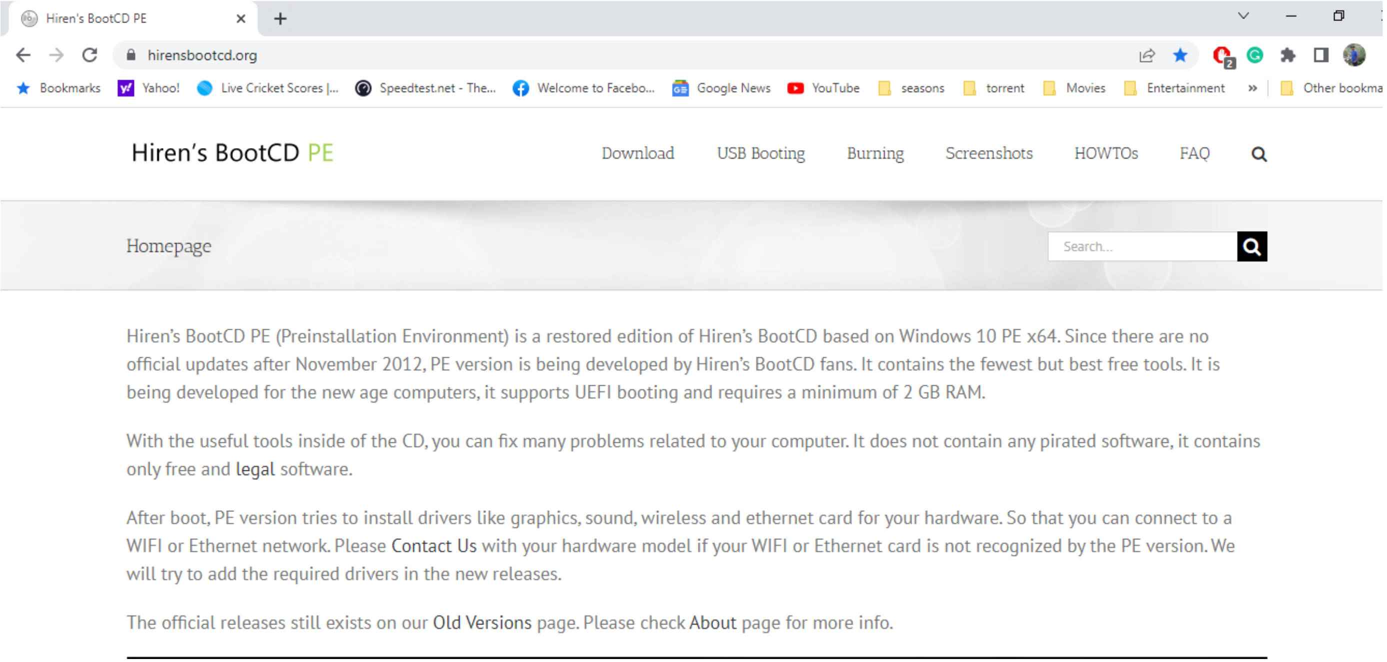
Scenorio

- You have physical access to a system which is **password locked**. The tool can be used to quickly bypass the password

Step- 1

- Download the tool from the official Website

https://www.hirensbootcd.org/



Hiren's BootCD PE (Preinstallation Environment) is a restored edition of Hiren's BootCD based on Windows 10 PE x64. Since there are no official updates after November 2012, PE version is being developed by Hiren's BootCD fans. It contains the fewest but best free tools. It is being developed for the new age computers, it supports UEFI booting and requires a minimum of 2 GB RAM.

With the useful tools inside of the CD, you can fix many problems related to your computer. It does not contain any pirated software, it contains only free and legal software.

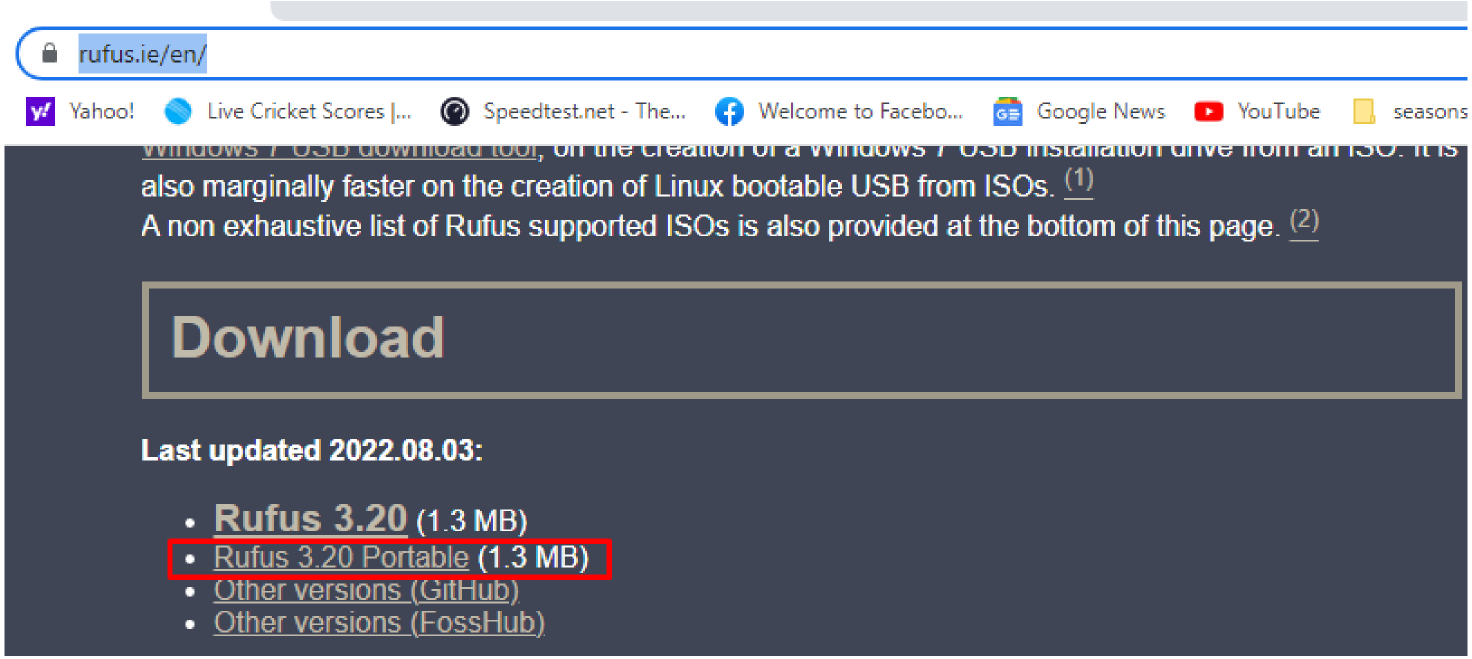
After boot, PE version tries to install drivers like graphics, sound, wireless and ethernet card for your hardware. So that you can connect to a WIFI or Ethernet network. Please Contact Us with your hardware model if your WIFI or Ethernet card is not recognized by the PE version. We will try to add the required drivers in the new releases.

The official releases still exists on our Old Versions page. Please check About page for more info.

Step- 2

- Download Rufus to make bootable USB(choose the portable version)

https://rufus.ie/en/



rufus.ie/en/

Windows 7 USB download tool, on the creation of a Windows 7 USB installation drive from an ISO. It is also marginally faster on the creation of Linux bootable USB from ISOs. (1)
A non exhaustive list of Rufus supported ISOs is also provided at the bottom of this page. (2)

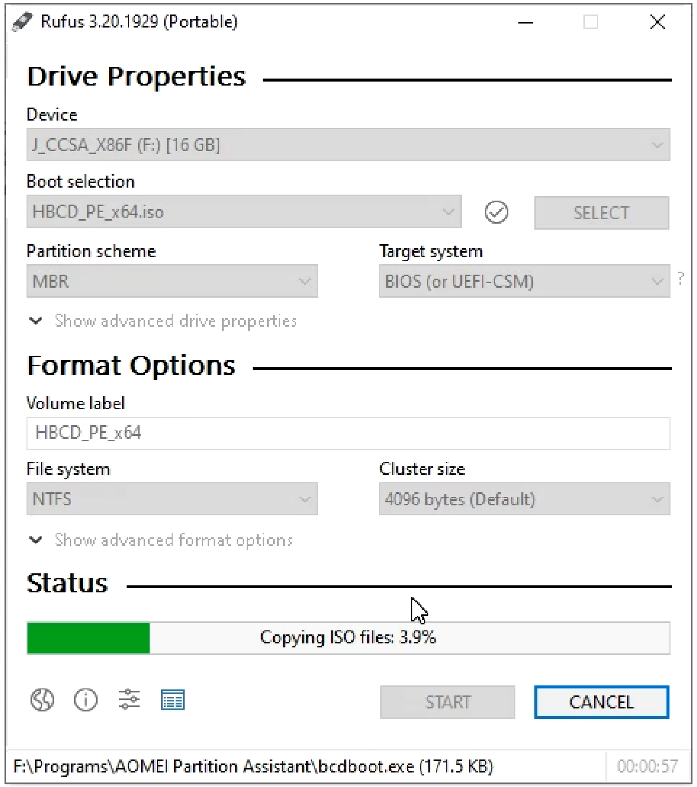
Download

Last updated 2022.08.03:

- **Rufus 3.20** (1.3 MB)
- Rufus 3.20 Portable (1.3 MB)
- Other versions (GitHub)
- Other versions (FossHub)

Step- 3

- Run Rufus, Select your Hiren Boot ISO and USB drive and make it bootable



Rufus 3.20.1929 (Portable)

Drive Properties

Device: J_CCSA_X86F (F:) [16 GB]

Boot selection: HBCD_PE_x64.iso

Partition scheme: MBR

Target system: BIOS (or UEFI-CSM)

Format Options

Volume label: HBCD_PE_x64

File system: NTFS

Cluster size: 4096 bytes (Default)

Status

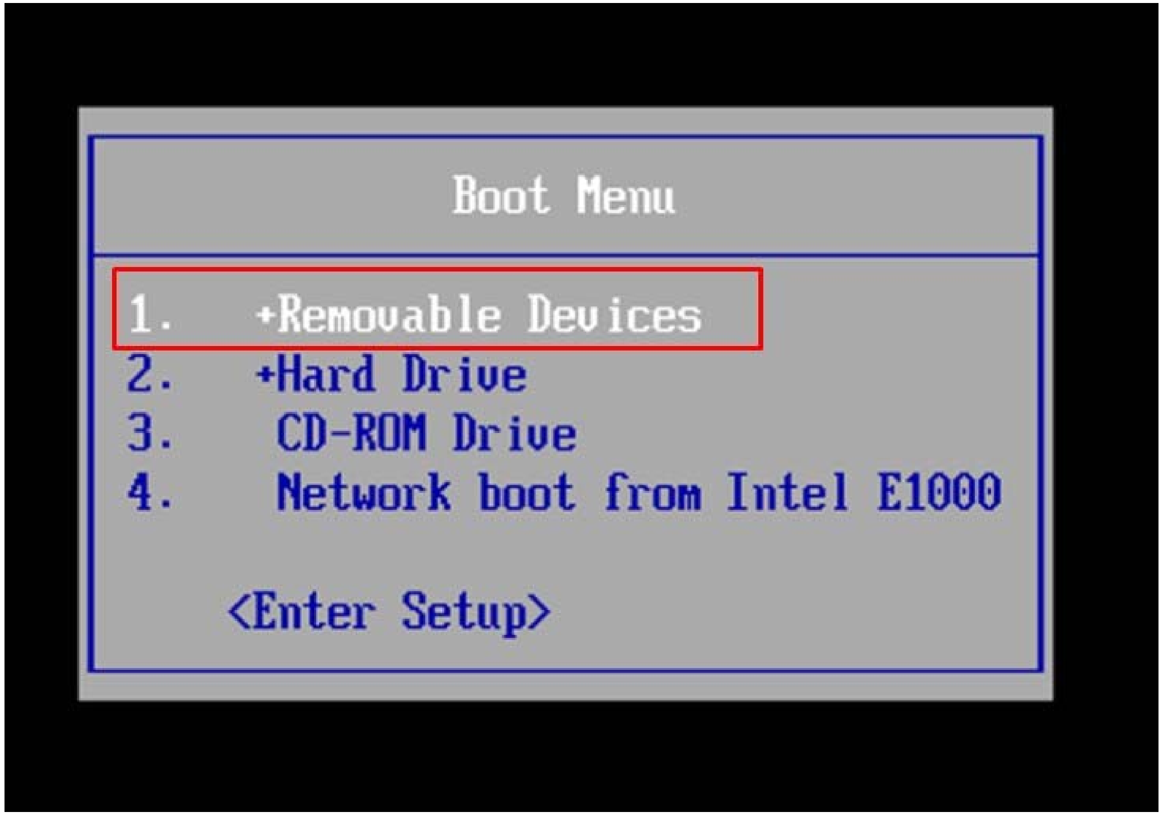
Copying ISO files: 3.9%

F:\Programs\AOMEI Partition Assistant\bcdboot.exe (171.5 KB)

00:00:57

Step- 4

- Plug in your USB, Reboot into USB. You may need to disable secure boot from BIOS settings



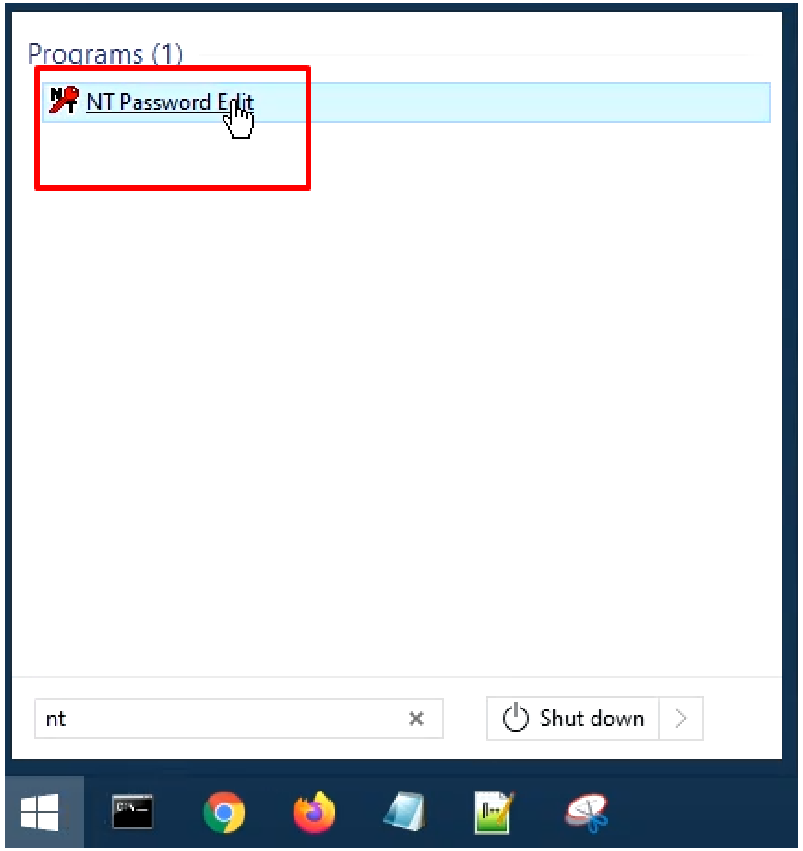
```
Boot Menu

1.    +Removable Devices
2.    +Hard Drive
3.     CD-ROM Drive
4.     Network boot from Intel E1000

    <Enter Setup>
```

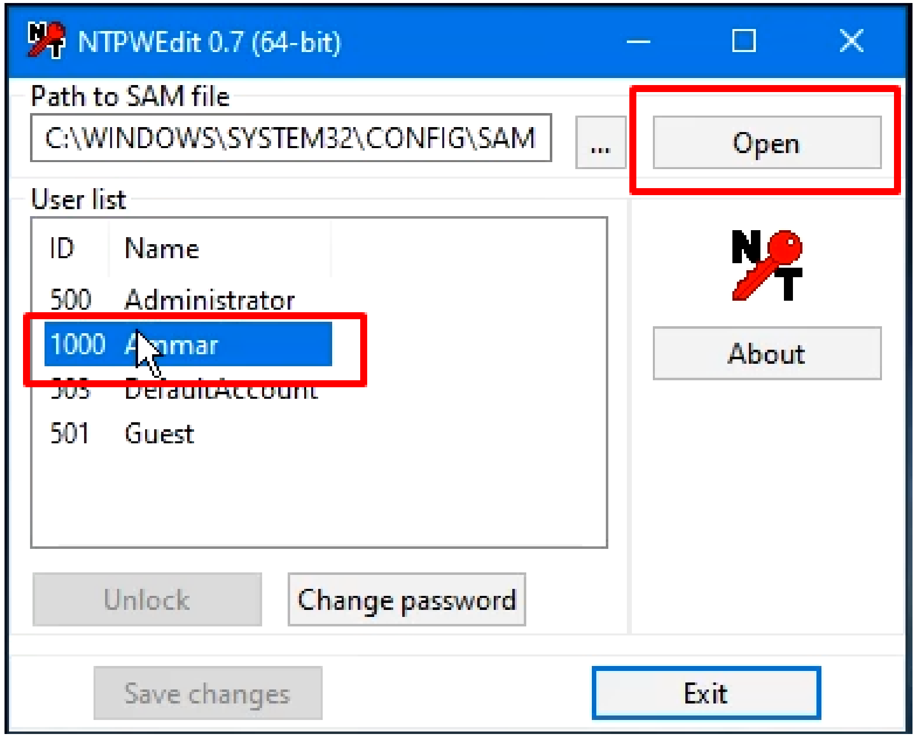
Step- 5

- Once Hiren Boots search for NT Password edit utility and open it



Step- 6

- Choose the option to open SAM file and then choose the username for which you want to clear the password for



Path to SAM file

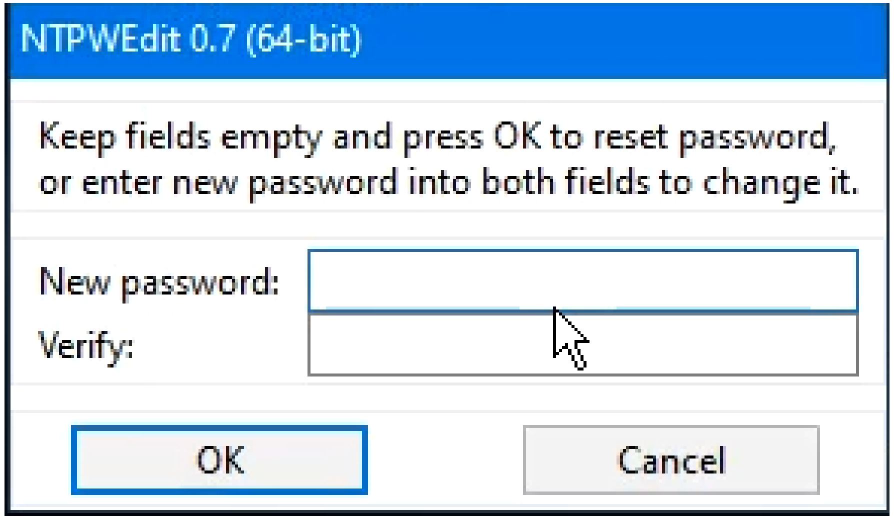
C:\WINDOWS\SYSTEM32\CONFIG\SAM

User list

ID	Name
500	Administrator
1000	Ammar
503	DefaultAccount
501	Guest

Step- 7

- Choose to change the password and once prompted for a new password enter blank password



NTPWEdit 0.7 (64-bit)

Keep fields empty and press OK to reset password, or enter new password into both fields to change it.

New password:

Verify:

- Now reboot the system, You will be logon without any password

DEMO

THANKS