

Forum:[Hack Forums](#)

Thread: [\[The Brotherhood\] Windows Recovery Environment Tutorial](#)

Freebooter - July 25, 2014, 9:52 am

Windows Recovery Environment

Hello HF members with this tutorial I will intrudes troubleshooting utility's in Windows Recovery Environment (WinRE) for troubleshooting Windows Operating System while it is offline.

Windows Recovery Environment is available with Windows Vista, Windows 7, Windows 8 and Windows 8.1 installation DVD and starting with Windows 8, 8.1 the Windows Recovery Environment is installed in a recovery partition also Windows Recovery Environment can also be installed to a hard drive partition by OEMs.

Windows System Repair Disc can be created containing the WinRE i recommend creating a Windows Repair Disc to anybody without a Windows OS installation DVD.

Create a Windows Vista System Repair Disc

The Service Pack 1 must be install to create a Windows System Repair Disc from Windows Vista. Program that creates a Windows System Repair Disc can be started from "Start Menu --> All Programs --> Maintenance --> Create a Recovery Disc". Follow the instructions to create a Windows System Repair Disc you will need either a blank CD or DVD.

Create a Windows 7 System Repair Disc

Open the "Backup and Restore" by clicking the "Start Menu --> Control Panel --> System and Maintenance --> Backup and Restore" and In the left pane, click "Create a system repair disc". You will need a blank CD or DVD and then just follow the instructions to create a Windows Repair Disc.

Create a Windows 8, 8.1 System Repair Disc

Open the Search charm by dragging your mouse to the top or bottom right corners of the screen or press WinKey + Q keys and type Recover into Search charm and click Create a recovery drive to create USB recovery drive which will include WinRE and optionally Windows OS factory recover image.

You will need empty USB Flash Drive or blank CD or DVD if you click "Create a system repair disk with a CD or DVD" option on the Connect USB flash drive screen.

Create a Windows 10 Recovery Drive

Even if your PC can't start, you can use the Recovery drive to reset it or troubleshoot problems. If you back up system files to this drive, you'll also be able to use it to reinstall Windows.

Open your Start menu, type RecoveryDrive.exe in the search box, press Enter key.

Check or Uncheck the Back up system files to the recovery drive box for what you want to do, and click on Next button.

Select the USB flash drive (ex: "E:\ (USB)") you want to make a recovery drive, and click on Next button.

When ready to start, click on Create button.

Quote:Back up system files to the recovery drive will require that the USB flash drive is large (at least 8-16 GB) enough for this.

Some people are getting a We can't create the recovery drive - A problem occurred while creating the recovery drive error message with Back up system files to the recovery drive checked.

If you have this issue, then leaving Back up system files to the recovery drive unchecked should allow it to successfully create a recovery drive

Start WinRE from HDD

In Windows 8, 8.1 press WinKey + I and click the Power icon hold down Shift and click Restart. Restart your computer and while Windows Vista / Windows 7 boots repeatedly press F8 key on your keyboard and at the Advanced Boot Option menu select "Repair your Computer".

Boot Computer into WinRE With Windows Setup DVD

1. Insert the System Repair Disc into your CD or DVD drive.
2. Configured the BIOS boot device order setting to start from a CD/DVD optical drive.

3. If prompted, press any key to start the computer from the System Repair Disc.
4. Choose your language settings, and then click Next.
5. Click "Repair your computer".

6 . To access WinRE environment from Windows Vista and Windows 7 select the Windows installation you want to repair, and then click Next.

After you click Next, the System Recovery Options menu appears.

7. To access WinRE from Windows 8 and Windows 8.1 click "Troubleshoot".

After you click Troubleshoot the Troubleshoot screen appears.

WinRE environment in Windows 8 and Windows 8.1 have changed compared to previous versions of Window OS.

Troubleshoot screen has three options.

Refresh your PC : Reinstall Windows OS using the installation DVD or factory recover image on the hard disk drive while retaining users personal files, personalization settings, and apps installed from the Windows Store.

Reset your PC : Reinstall Windows OS using the installation DVD or factory recover image on the hard disk drive but removes all personal data, apps, and settings from the PC.

Click "Advanced options" on the Troubleshoot screen to access more WinRE recovery utility's in

“Advanced options” screen.

The Advanced Options screen except for “Windows Memory Diagnostics” utility have same recovery utility’s as the previous versions of Windows OS WinRE environment.

System Restore : Restores Windows OS to a previous state that was without any system errors.

System Image Recovery : You can restore the contents of the hard disk drive using previously created system image .

Automatic Repair (Startup Repair) : Windows will attempt to diagnose and correct common boot problems It corrects issues, such as corrupt registry hives, missing system files and drivers, disk boot sector corruptions, and other startup issues.

Windows Memory Diagnostics : Use for checking computer memory for errors. Windows 8, 8.1 WinRE does not have this utility but can be started by typing mdsched.exe into Command Prompt.

Command Prompt : Use for executing many commands that can be use for repairing Windows OS and recovering personal files.

Freebooter - July 25, 2014, 9:54 am

The Command Prompt list of commands

Attrib Use for changing attributes of files and folders.

Example The following command clears the read-only, system, and hidden attributes from example.txt file.

```
attrib -r -s -h example.txt
```

BCDboot Used for copying critical boot files to the system partition and to create a new system BCD store.

Example The following command replaces the system partition boot environment files with new copies of these files from the Windows partition.

```
Bcdboot C:\Windows
```

Bcdedit View and manage the BCD store boot entries.

Example The following command enables the system boot log. This log is stored in the Ntbtlog.txt file in the Windows directory. It includes a list of loaded and unloaded drivers in text format.

```
Bcdedit /set {current} bootlog on
```

Bootsect Updates the master boot code (MBR) for hard disk partitions to switch between BOOTMGR and NTLDR. Not available in Vista WinRE environment but can be started from Windows Vista installation DVD.

Example If the computer display a “NTLDR is missing” message then following command updates the master boot code that is compatible with BOOTMGR.

```
Bootsect /nt60 SYS
```

Bootrec Use for repairing the master boot record (MBR), boot sector and Boot Configuration Data (BCD) store.

Example The following command writes new master boot record but does not overwrite partition table.

```
Bootrec /Fixmbr
```

Cd Changes the current directory to another directory.

Example The following command changes the Command Prompt current directory path to the C:\Windows.

```
Cd C:\windows /d
```

Cls Clears the screen

Chkdsk Checks the hard disk drive partition (NTFS/FAT) file system for errors and attempts to repair them.

Example The following command repairs the C:\ partition file system errors.

Chkdsk C: /f

Chkntfs Displays or modifies the checking of disk for error at boot time.

Example The following command excludes C:\ partition from default boot time error check.

Chkntfs /x C:

Copy Copies one or more files from one location to another.

Example The following command copies "Example.txt" file on the C:\ partition to the directory named "MyFolder" on the D:\ partition.

Copy C:\Example.txt D:\MyFolder

Del Deletes a file or multiple files.

Example The following command deletes a file named "Example.txt" on the C:\ partition.

Del C:\Example.txt

Dir Lists the files and folders in the current directory or specified partition letter and directory.

Example The following command list directory's and files on the C:\ partition.

Dir C:\

Diskpart Command line utility use for creating and working with disks, partitions, and volumes.

Example The Following commands in the Diskpart screenshot use for shrinking a partition.

DISM Use for servicing and maintaining offline and online Windows OS images. Note Dism command is not included with the Windows Vista WinRE.

Example Following command will revert the pending actions, useful if the Windows Update appears to be in a hung state.

Dism.exe /image:D:\ /cleanup-image /RevertPendingActions

Drvload Use for adding drivers to a Windows Preinstallation Environment (Windows PE) image.

Example The following command adds a driver to WinRE.

Drvload Driver.inf

Diskraid Use for configuring and managing redundant array of independent disks (RAID) storage subsystems.

Exit Use for exiting Command Prompt and interactive mode commands .

Format Use for formatting a partitions

Example The following command use for quick formatting D: partition with NTFS file system.

Format D: /FS:Ntfs /q

Find Searches for a text string in files.

Example The following command displays all lines from "example.txt" file that contain the string "Pencil Sharpener" .

Find "Pencil Sharpener" example.txt

Icacls Use for changing file and folder permissions.

Example The following command grants Administrators group a full access permission to a file named example.txt.

Icacls example.txt /grant Administrators:F

Md Use for creating a new folder.

Example The following command creates a folder named “MyFolder” on the C:\ partition.

Md C:\MyFolder

Manage-bde BitLocker drive encryption configuration tool.

Example The following command enables BitLocker on drive C with the option of a recovery password.

Manage-bde –on C: -recoverypassword

More Displays the command output one screen at a time.

Example The following command displays the content of a file one page at a time.

More C:\Example.txt

Move Moves one or more files or directory from one directory to another directory.

Example The following command moves the “example.txt” file located in MyFolder on the C:\ partition to the destination “Backup” folder on the D:\ partition.

Move C:\example.txt D:\Backup

Mountvol Creates, deletes, or lists a volume mount point.

Example The following command creates a mount point.

Mountvol C:\Mount \\?\Volume{9ce1c381-27db-4141-89c4-1ab4f2cf1c21}\

Notepad Opens the Notepad.

Path Displays or sets a search path for executable files in the current command window.

Example The following command adds “C:\Utility” folder to the current search path.

Path=%Path%;C:\Utility

Recover Recovers readable information from a bad or defective disk.

Example The following command recovers the file named Example.txt in the MyFolder directory on the D: partition.

Recover D:\MyFolder\Example.txt

Replace Replaces files in the destination directory with files in the source directory that have the same name.

Example The following command replaces the registry hives in the C:\Windows\System32\Config directory with the backup version of the registry hives stored in the C:\Windows\System32\Config\RegBack directory.

Replace C:\Windows\System32\Config C:\Windows\System32\Config\RegBack*

Robocopy Robust File and Folder Copier.

Example The following command copies all files and folders including empty ones from the MyFolder directory to the Backup directory.

Robocopy C:\MyFolder C:\Backup /e

Reg Adds, changes, and displays registry subkey information and values in registry entries.

Example The following example loads the SYSTEM hive into a temporary subkey named Temp in the registry.

Reg Load HKLM\Temp C:\Windows\System32\Config\SYSTEM

Regedit Microsoft Registry Editor use for searching and changing settings in the system registry hives, which contains information and setting for Windows OS , Applications and Hardware.

Ren Renames files or directories.

Example The following command renames the Example.txt file as MyExample.txt.

Ren Example.txt Renamed.txt

Rd Deletes a directory.

Example The following command deletes MyFolder directory and all subdirectories and files in the MyFolder directory.

Rd /s /q MyFolder

Sfc Scans the integrity of all protected system files and replaces incorrect versions with correct Microsoft versions.

Example The following command scans integrity of all protected system files and repairs files with problems when possible.

Sfc /OFFBOOTDIR=D:\ /OFFWINDIR=D:\Windows

Type Displays the contents of a text file.

Example The following command displays the content of the Example.txt file.

Type Example.txt

Takeown Use for taking ownership of files and folders.

Example The following command gives ownership to the administrators group for the MyFolder directory.

Takeown /F MyFolder /A

Taskmgr Starts the Windows Task Manager.

Xcopy Copies directories, including subdirectories and their contents.

Example The following command copies all files and subfolders in the "MyFolder" directory located on C:\ partition in to D:\ partition.

Xcopy C:\MyFolder D:\MyFolder /I /s

To get help on how to use these commands and there parameters, you can use /? argument. For example to get help for Copy command type Copy /? and then press Enter on your keyboard.

When computer boots into WinRE environment the drive letter assign to Windows partition may not be C: drive letter because Windows 7, 8, 8.1 creates a separate system partition when it's installed from scratch. The system partition contains boot files WinRE assigns the system partition the C: drive letter and the Windows installed partition will be assign any other drive letter usually D: drive letter is assign to Windows installed partition. The Bcdedit /enum | find "osdevice" command can be use to find out the drive letter of the Windows installed partition the output of the Bcdedit command is similar to this osdevice partition=D:. The drive letter after partition= is the drive letter of the Windows partition.

Freebooter - July 25, 2014, 9:56 am

Registry

Windows registry editor program can be started within WinRE by typing Regedit into Command Prompt the registry editor can be use to mount the offline Windows registry hives and modify the settings that is store in the registry hives.

The \Windows\System32\Config directory contains the registry hives the Windows\System32\Config directory includes the following set of registry hive files.

COMPONENTS

DEFAULT

SAM

SECURITY

SOFTWARE

SYSTEM

All hive files, except for NTUSER.DAT are stored in the Windows\System32\Config directory the NTUSER.DAT is store at user profile directory which is at the \Users\UserName directory.

Visit [Wikipedia](https://en.wikipedia.org/wiki/Windows_registry_hive) to learn information about registry hives.

RegIdleBackup task is scheduled to run every ten days to backup registry hives into “Windows\System32\Config\RegBack” directory these registry hives backups can be use to replace damage registry hives.

WARNING: Modifying registry settings incorrectly can cause serious problems that may require you to reinstall Windows OS.

How to Backup Registry

Before making any changes in registry you should backup the register key settings.

From registry editor select the registry key which you want to backup and from menu bar click “File --> Export” select the location you want to backup registry and give the registry backup a file name. Registry will be backup with the “.reg” file extension and to undo the changes you have made in registry click “File --> Import” from menu bar and select the registry backup file.

How to Disable Boot Driver or Service

The SYSTEM hive contains information on controlling the system startup, the loading order of device drivers and system services, and on the operating system behavior.

The SYSTEM hive can be loaded into registry editor by selecting “HKEY_LOCAL_MACHINE” and then from registry menu bar click “File --> Load Hive” temporary name must given to a registry key where register hive will be loaded you can name it as TEMP or any other name you want.

Navigate to “HKEY_LOCAL_MACHINE\TEMP>Select” the Default value contains the number of the ControlSet that Windows uses by default when booting.

The above screenshot of the Default value has a data value of number one this indicates the ControlSet001 key that Windows uses by default when booting.

Navigate to “HKEY_LOCAL_MACHINE\TEMP\ControlSet001\Services key the subkeys under the Services key contain settings for the device drivers and Windows services.

The Start Value data specifies the starting values for the service and to disable a service or driver that is causing Windows not booting change the Start value to 4 by double clicking the Start value.

After modifying the loaded registry hive apply the changes by selecting the temporary key name where the registry hive is loaded and from menu bar click “File --> Unload Hive”.

Uninstall Drivers With Dism Command

The following command lists out-of-box drivers.

```
Dism /Image:D: /Get-Drivers
```

The following command displays information about a specific driver.

```
Dism /Image:D: /Get-DriverInfo /Driver:oem1.inf
```

The following command removes the specified out-of-box driver.

```
Dism /Image:D: /Remove-Driver /Driver:oem1.inf
```

WARNING: Removing a boot-critical driver package can make the offline Windows unbootable.

How to Enable Windows Build-in Administrator Account

Windows OS has a Administrator user account which is disable by default this account can be enable with in WinRE registry editor and within administrator account any Windows user account password can be resetted or change from Command Prompt by typing `Net User UserName *` replace the "UserName" with name of the user account and pressing Enter key twice for each password prompt to reset the user account password.

Enable Administrator account by selecting the HKEY_LOCAL_MACHINE and load the SAM Registry hive from Windows\System32\Config directory.

Navigate to "SAM\Domains\Accounts\Users\Names\Administrator" key .

The Type column of the Default value indicates the registry key name under the "SAM\Domains\Accounts\Users" key select the key indicated by the Type column.

Edit the "F" value data navigate to position 0038 move the cursor to the beginning of position 0038 and press Del key and then type 10 click OK button and then unload the SAM hive by selecting the temporary key name where SAM is loaded and then from File menu click Unload Hive.

After you reboot, you can log on using the built-in administrator and reset the password of other user accounts.

Please post any question that you may have i will do my best to answer the question. Thank you?

[\[The Brotherhood\] Recovering Windows 2000, Windows XP Os - Tutorial](#) by [Freebooter](#)

Aura - July 25, 2014, 9:57 am

Alright, time to get some proofreaders in it Freebooter ?

Excellent job. Once the banner is ready, you can add the Windows Subsector banner at the beginning of the tutorial and tag it BHCPU.

[BHCPU] Windows Recovery Environment Tutorial

Here's for the definitions in the first post :

Refresh your PC : Reinstall Windows OS using the installation DVD or factory recover image on the hard disk drive while retaining users personal files, personalization settings, and apps installed from the Windows Store.

Reset your PC : Reinstall Windows OS using the installation DVD or factory recover image on the hard disk drive but removes all personal data, apps, and settings from the PC.

Click "Advanced options" on the Troubleshoot screen to access more WinRE recovery utility's in "Advanced options" screen.

The Advanced Options screen except for "Windows Memory Diagnostics" utility have same recovery utility's as the previous versions of Windows OS WinRE environment.

System Restore : Restores Windows OS to a previous state that was without any system errors.

System Image Recovery : You can restore the contents of the hard disk drive using previously created system image.

Automatic Repair (Startup Repair) : Windows will attempt to diagnose and correct common boot

problems It corrects issues, such as corrupt registry hives, missing system files and drivers, disk boot sector corruptions, and other startup issues.

Windows Memory Diagnostics : Use for checking computer memory for errors. Windows 8, 8.1 WinRE does not have this utility but can be started by typing mdsched.exe into Command Prompt.

Command Prompt : Use for executing many commands that can be use for repairing Windows OS and recovering personal files.

Copy/paste this :

Code [color=red][b]Refresh your PC : [/b][[/color][font=Tahoma]Reinstall Windows OS using the installation DVD or factory recover image on the hard disk drive while retaining users personal files, personalization settings, and apps installed from the Windows Store.[/font]

[color=red][b]Reset your PC : [/b][[/color][font=Tahoma]Reinstall Windows OS using the installation DVD or factory recover image on the hard disk drive but removes all personal data, apps, and settings from the PC.[/font]

[font=Tahoma]Click “[b]Advanced options[/b]” on the Troubleshoot screen to access more WinRE recovery utility’s in “Advanced options” screen.[/font]

[img]https://i.imgur.com/yD4hCmT.png[/img]

[font=Tahoma]The Advanced Options screen except for “Windows Memory Diagnostics” utility have same recovery utility’s as the previous versions of Windows OS WinRE environment.[/font]

[color=red][b]System Restore : [/b][[/color][font=Tahoma]Restores Windows OS to a previous state that was without any system errors.[/font]

[color=red][b]System Image Recovery : [/b][[/color][font=Tahoma]You can restore the contents of the hard disk drive using previously created system image .[/font]

[color=red][b]Automatic Repair (Startup Repair) : [/b][[/color][font=Tahoma]Windows will attempt to diagnose and correct common boot problems It corrects issues, such as corrupt registry hives, missing system files and drivers, disk boot sector corruptions, and other startup issues.[/font]

[color=red][b]Windows Memory Diagnostics : [/b][[/color][font=Tahoma]Use for checking computer memory for errors. Windows 8, 8.1 WinRE does not have this utility but can be started by typing [b]mdsched.exe[/b] into Command Prompt.[/font]

[color=red][b]Command Prompt : [/b][[/color][font=Tahoma]Use for executing many commands that can be use for repairing Windows OS and recovering personal files.[/font]

Freebooter - July 25, 2014, 10:07 am

(Jul 25, 2014 09:57 AM)Aur? Wrote: [\[CITE\]](#) Alright, time to get some proofreaders in it Freebooter ? Excellent job. Once the banner is ready, you can add the Windows Subsector banner at the beginning of the tutorial and tag it BHCPU.

[BHCPU] Windows Recovery Environment TutorialThank you Aura still checking for mistakes if any body see one please tell me.

Aura - July 25, 2014, 10:08 am

(Jul 25, 2014 10:07 AM)Freebooter Wrote: [\[CITE\]](#) Thank you Aura still checking for mistakes if any body see one please tell me.

No problem buddy, asked for proofreaders in our Lounge (BH).

Also, copy/paste what's inside the code tags to replace your current text, I fixed the formatting.

Antigen - July 25, 2014, 1:10 pm

I just skimmed through tutorial, looking great and detailed, you got it all covered.

Banish - July 25, 2014, 1:10 pm

<https://hackforums.net/showthread.php?tid=4221327>

Here're the official banners if you want them.

Freebooter - July 25, 2014, 1:33 pm

(Jul 25, 2014 01:10 PM)Antigen Wrote: [\[CITE\]](#) I just skimmed through tutorial, looking great and detailed, you got it all covered. Thank you for the positive feedback.

(Jul 25, 2014 01:10 PM)Banish Wrote: [\[CITE\]](#) <https://hackforums.net/showthread.php?tid=4221327>

Here're the official banners if you want them. Thanks i change the BH banner i use the banner from your link.

mxx518 - September 13, 2014, 11:25 am

Nice article. Well written and organized. There are a few things on here that can be accomplished by means of more efficient methods and different ways, but it's important for any IT tech to be knowledgeable and proficient with the Windows registry and command line; and you did miss out on some minor things. But overall, if I had to grade this, I'd give it a 92%. Nice job.

Freebooter - September 13, 2014, 11:34 am

(Sep 13, 2014 11:25 AM)mxx518 Wrote: [\[CITE\]](#) Nice article. Well written and organized. There are a few things on here that can be accomplished by means of more efficient methods and different ways, but it's important for any IT tech to be knowledgeable and proficient with the Windows registry and command line; and you did miss out on some minor things. But overall, if I had to grade this, I'd give it a 92%. Nice job. Thank you, can you tell me what i have not included or what is missing so i can add them in the tutorial.

cyberducky - September 13, 2014, 3:50 pm

Very good tutorial Freebooter. I have seen you helping out a lot in this section.

Freebooter - September 13, 2014, 4:11 pm

(Sep 13, 2014 03:50 PM)Abide Wrote: [\[CITE\]](#) Very good tutorial Freebooter. I have seen you helping out a lot in this section. Thank you Abide and yes i do my best to help HF members with there PC problems.