Manually Updating the Norton Recovery Toolkit

Introduction

This guide provides instructions on how to update antivirus definitions, and how to add new or updated network and storage drivers to the Norton Recovery Toolkit.

The steps outlined in this guide require only a medium PC skills level.

Note: To avoid confusion between the Norton Removal Tool (NRT) and the Norton Recovery Toolkit, from here on the solution will be referred to as the Norton Recovery Disc (NRD).

Windows Preinstall Environment

The Norton Recovery Disk (NRD) is based on the Microsoft Windows Preinstall Environment, commonly known as WinPE.

WinPE is a scaled down version of Windows that starts up and runs from a CD or a USB key, and is typically used to deploy Windows installations, or to perform recovery operations on Windows.

By running the Norton scanner from WinPE, and booting WinPE from a CD or USB key, we know the OS is clean and fully functional. This allows the scanner to safely scan all of the drives connected to the system, including the normal XP or Vista operating system drives, without the malware on those drives interfering with the scan.

The NRD CD is the same install CD that comes with a purchased retail product. Or, when the product is downloaded, the registration email includes a link to download the CD image. (A customer can re-download the NRD from Symantec, but should remember to download the correct CD based on which product is owned, i.e. the Norton AntiVirus CD requires a Norton AntiVirus key, while the Norton Internet Security CD requires a Norton Internet Security key).

Norton Internet Security:
ftp://ftp.symantec.com/public/english_us_canada/recovery/2009/NIS/recovery_nis_x86.iso
Norton AntiVirus:
ftp://ftp.symantec.com/public/english_us_canada/recovery/2009/NAV/recovery_nav_x86.iso

Note: Symantec has licensed the usage of WinPE for the Norton Recovery Disc. No other uses, modification, or redistribution of the NRD is allowed.

When to use the Norton Recovery Disc

The Norton Recovery Disc is typically used in one of two situations:

1. When the system is heavily infected and the installation of the Norton security product fails. Install failures typical fall in one of two categories; the install fails because malware destabilized the operating system, or the install fails because malware is actively attacking the installer software.
   By running a scan from the NRD, and removing malware on the system, the system will be clean enough to allow installation to succeed.
2. When the system is infected by malware that cannot be completely removed, or that cannot be safely removed, while the malware is still running.

It is important to note that the NRD is not intended to fix broken Windows installations.

Updating the Norton Recovery Disc

The following section will provide step-by-step instructions on how to update the NRD.

To make things as simple as possible, a script is provided that will accomplish the vast majority of the work.
Save the script to the "C:\CustomNRD" folder, and name the file "MakeNewNRD.cmd".

The script expects to run from the "C:\CustomNRD" directory, and expects the original NRD CD to be in drive "D:".
Any directory can be used to run the script, and the original NRD CD can be in any drive, as long as the paths in the script are changed accordingly, and double quotes are added around paths with spaces.

The steps and scripts use a utility called "robocopy" that is included as standard in Windows Vista.
If running XP, simply download "robocopy", included as part of the Windows Server 2003 Resource Kit Tools from Microsoft: http://www.microsoft.com/downloads/details.aspx?FamilyID=9D467A69-57FF-4AE7-96EE-B18C4790CFFD&displaylang=en

Install the Windows Automated Installation Kit

WinPE is built and updated using the Microsoft Automated Installation Kit (AIK) tools.

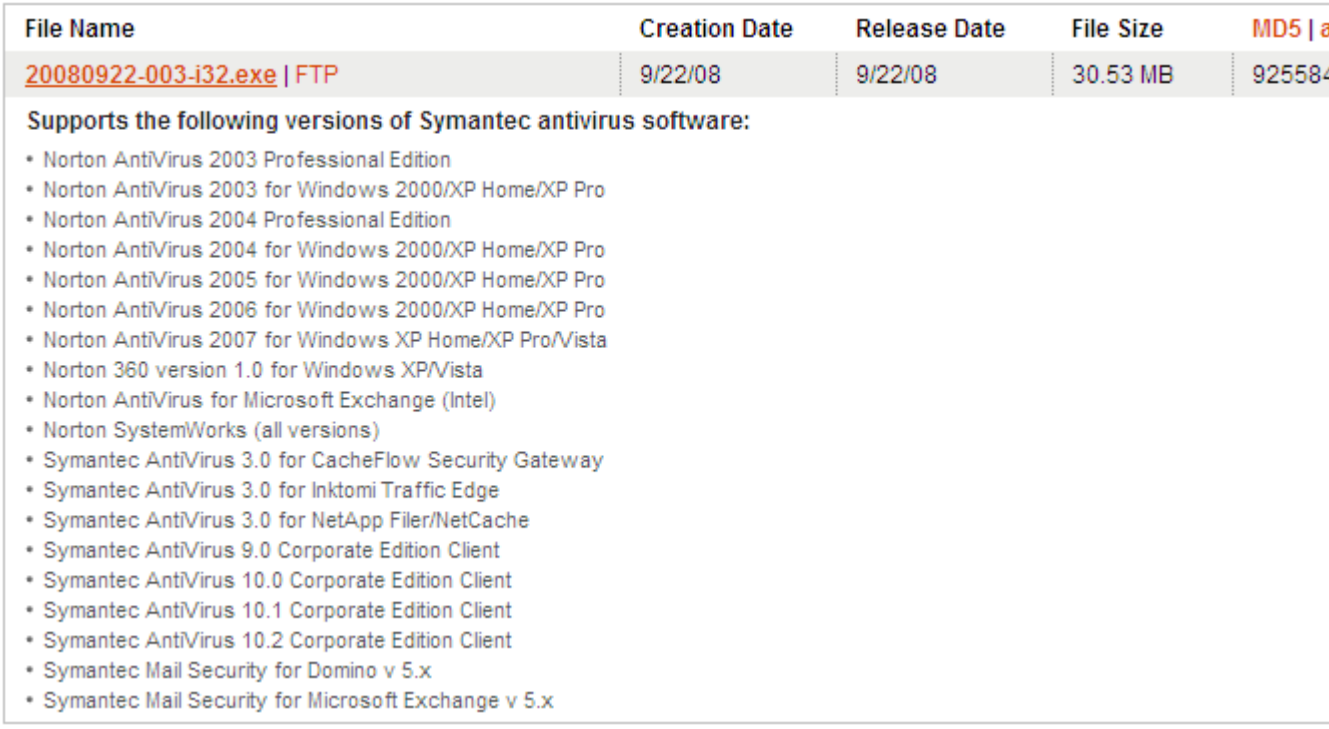
1. Download the Vista SP1 and Server 2008 AIK from Microsoft:
   http://www.microsoft.com/downloads/details.aspx?familyid=94BB6E34-D890-4932-81A5-5B50C657DE08&displaylang=en
   The AIK download is an ISO file. Either burn the ISO to a DVD, or mount the ISO in a virtual DVD drive.
   There are many applications capable of burning ISO images to a DVD. This site provides details on some of these applications:
   http://www.petri.co.il/how_to_write_iso_files_to_cd.htm

2. Install the AIK.

Download the latest virus definitions

1. Download the latest Intelligent Updater virus definitions package from Symantec: http://www.symantec.com/business/security_response/definitions/download/detail.jsp?gid=n95
   The actual package name will be unique, and in the form of "YYYYMMDD-XXX-i32.exe".
   Be sure to download the correct package, which is second on the list. Do not download the v5i32 package.

2. Save the file to the “C:\CustomNRD” folder, and name the file “DefUpdate.exe”.
   The script expects this file to always be named “DefUpdate.exe”.



File Name	Creation Date	Release Date	File Size	MD5 | a
20080922-003-i32.exe | FTP	9/22/08	9/22/08	30.53 MB	925584

Supports the following versions of Symantec antivirus software:

- Norton AntiVirus 2003 Professional Edition
- Norton AntiVirus 2003 for Windows 2000/XP Home/XP Pro
- Norton AntiVirus 2004 Professional Edition
- Norton AntiVirus 2004 for Windows 2000/XP Home/XP Pro
- Norton AntiVirus 2005 for Windows 2000/XP Home/XP Pro
- Norton AntiVirus 2006 for Windows 2000/XP Home/XP Pro
- Norton AntiVirus 2007 for Windows XP Home/XP Pro/Vista
- Norton 360 version 1.0 for Windows XP/Vista
- Norton AntiVirus for Microsoft Exchange (Intel)
- Norton SystemWorks (all versions)
- Symantec AntiVirus 3.0 for CacheFlow Security Gateway
- Symantec AntiVirus 3.0 for Inktomi Traffic Edge
- Symantec AntiVirus 3.0 for NetApp Filer/NetCache
- Symantec AntiVirus 9.0 Corporate Edition Client
- Symantec AntiVirus 10.0 Corporate Edition Client
- Symantec AntiVirus 10.1 Corporate Edition Client
- Symantec AntiVirus 10.2 Corporate Edition Client
- Symantec Mail Security for Domino v 5.x
- Symantec Mail Security for Microsoft Exchange v 5.x

Download network and storage drivers for your hardware

The NRD comes with a subset of commonly used network and storage drivers, but may not provide support for specific hardware. If particular drives are not detected, or the definitions do not automatically update, the correct driver may need to be provided to support the system hardware.

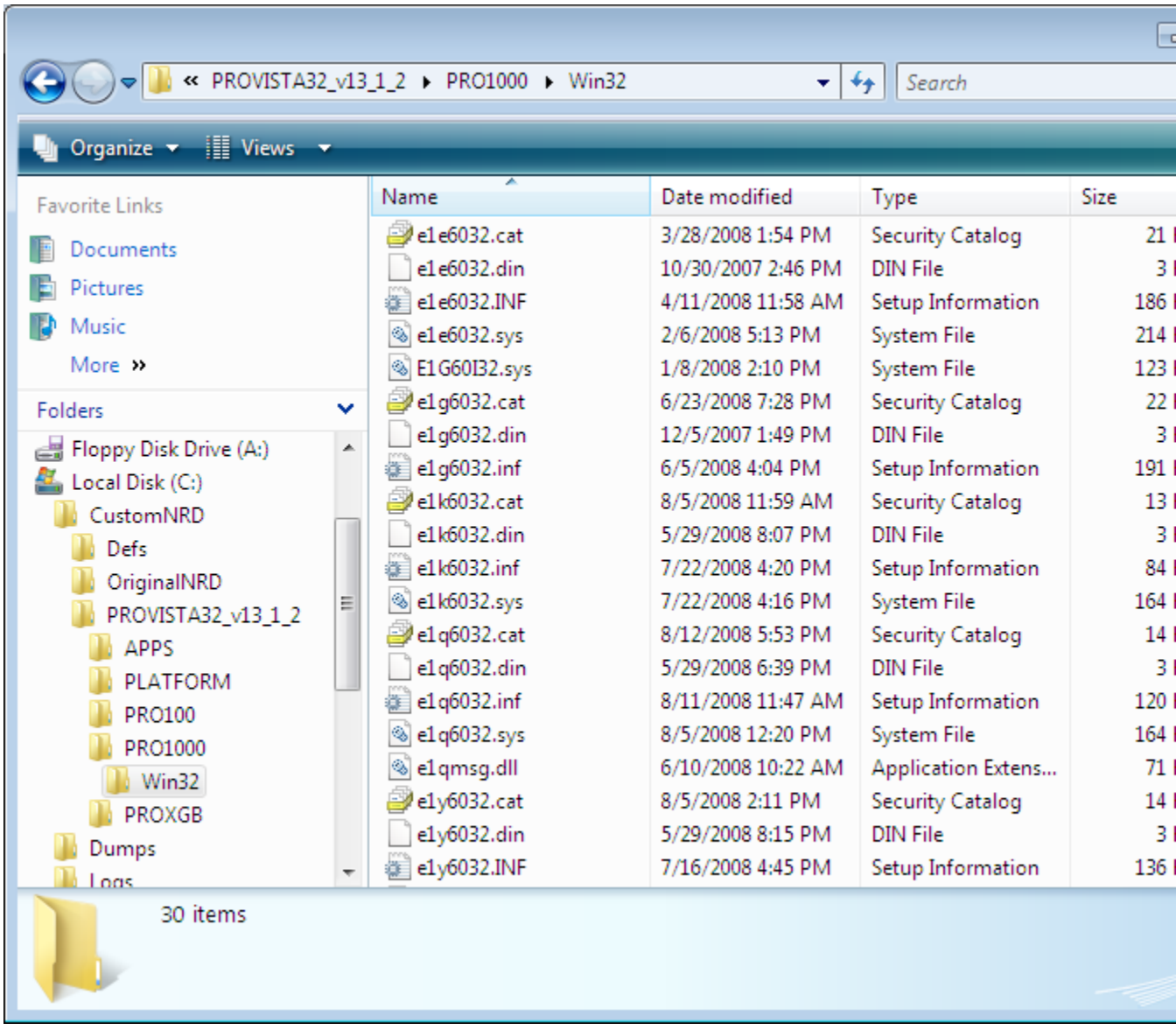
Remember that the NRD uses Vista x86 drivers, so regardless of what operating system is currently running, the Vista x86 drivers for the hardware must be downloaded. Due to the large variety of hardware and methods of driver distribution, it is not possible to provide details on how to obtain all drivers. However, most hardware manufacturers provide downloads that are clearly marked as Vista x86, and can easily be manually extracted. The extracted contents will typically consist of one or more INF and SYS files.

To get started, here is a list of some common manufacturers and their driver download sites:

- Realtek gigabit network drivers: http://www.realtek.com.tw/downloads/downloadsView.aspx?Langid=1&PNid=13&PFid=5&Level=5&Conn=4&DownTypeID=3&GetDown=false
- Broadcom network drivers: http://www.broadcom.com/support/ethernet_nic/netxtreme_desktop.php
- NVidia storage drivers: http://www.nvidia.com/Download/index.aspx?lang=en-us

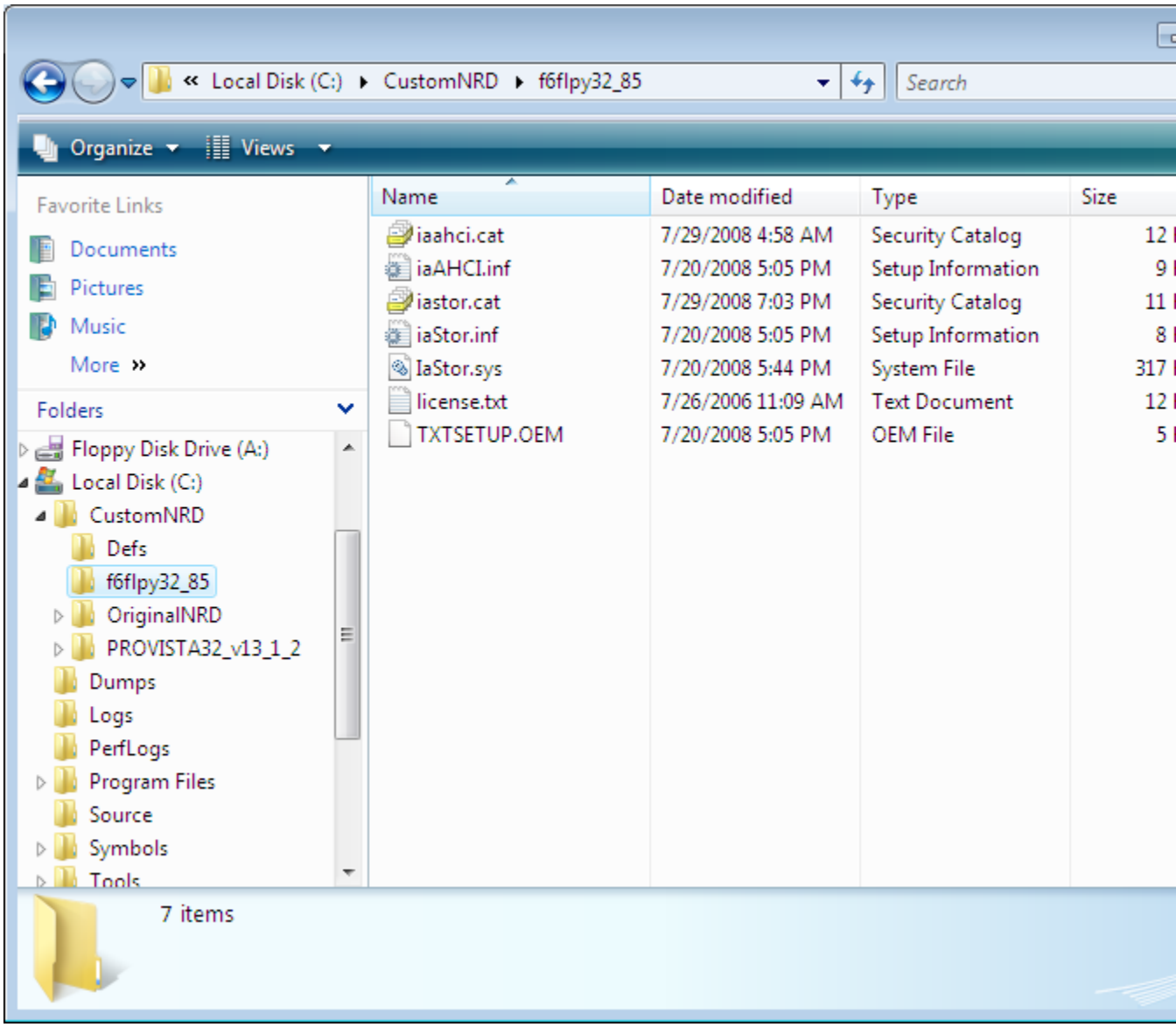
- Intel network and storage drivers:
  http://downloadcenter.intel.com/default.aspx?iid=gg_work+home_dowloads

1. Here is the Intel PRO 1000 drivers as an example of a network driver.
   The file “PROVISTA32_v13_1_2.exe” was downloaded from Intel, and the contents extracted using WinZip.



2. Here is the Intel Matrix Storage Manager RAID drivers as an example of a storage driver.
   For storage drivers, the simplest driver distribution is typically “F6 floppy” packaged version of the drivers.

The file “f6flpy32_85.zip” was downloaded from Intel, and the contents extracted using WinZip.

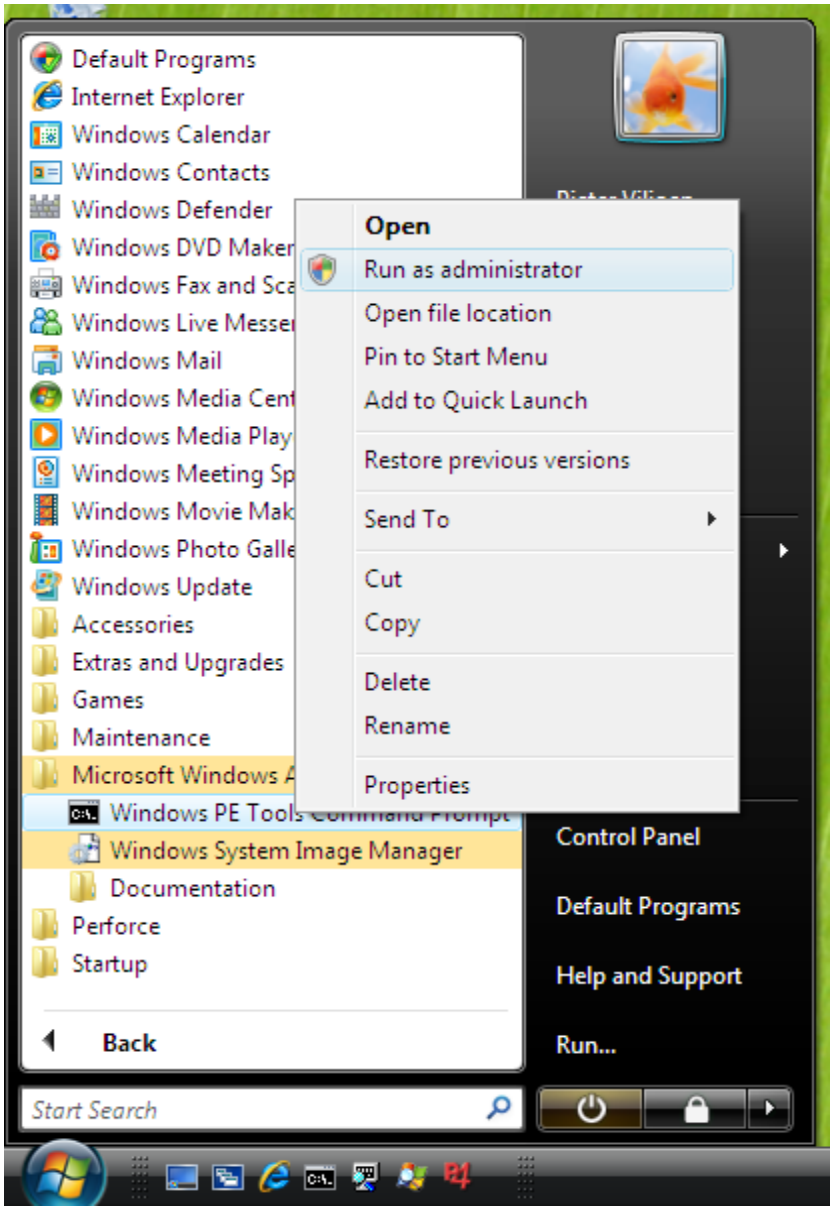


Note: You can download any number of network or storage drivers, and extract them to any location. Just remember to update the script to point to the correct locations. The directory will typically contain one or more INF and SYS files.

Updating the NRD

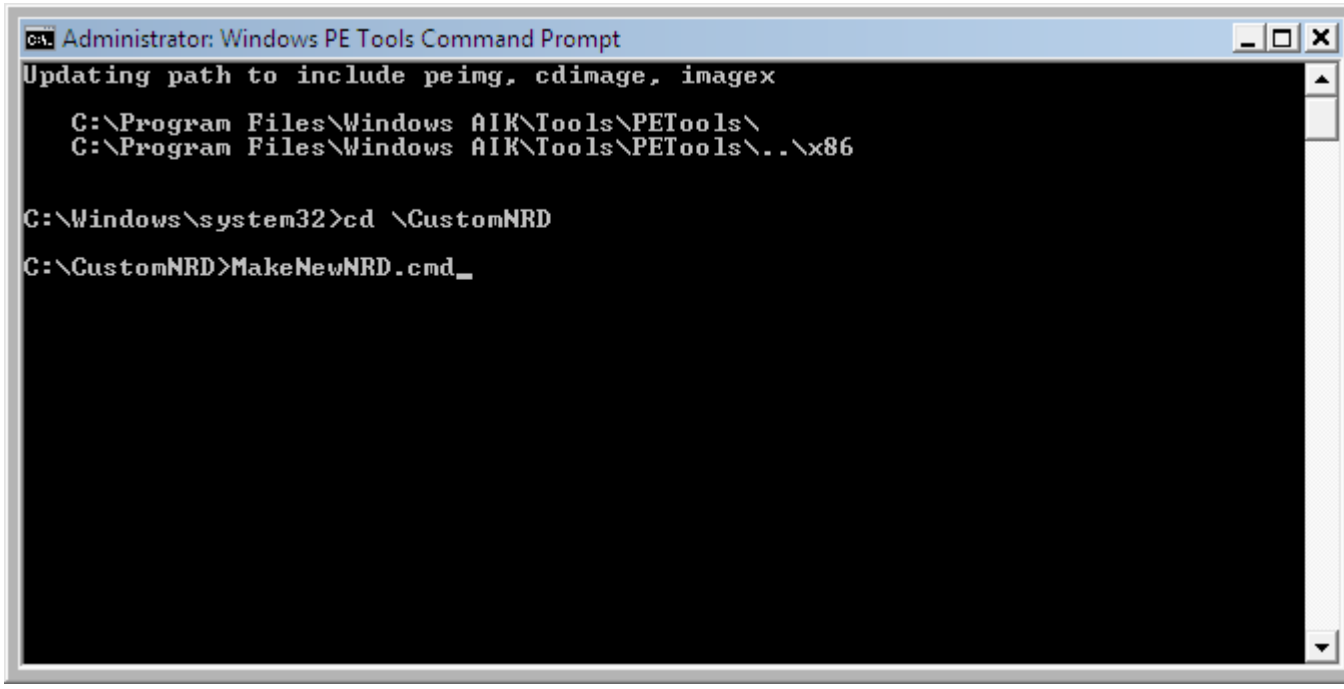
1. Save the script to the “C:\CustomNRD” folder, and name the file “MakeNewNRD.cmd”. If using a different directory, be sure to update the script to point to the correct locations.
2. Launch the “PE Tools” environment from [Start][Programs][Microsoft Windows AIK][Windows PE Tools Command Prompt].

3. On Vista this command must be executed by an elevated administrator, Right click on “Windows PE Tools Command Prompt” and select “Run as administrator”.

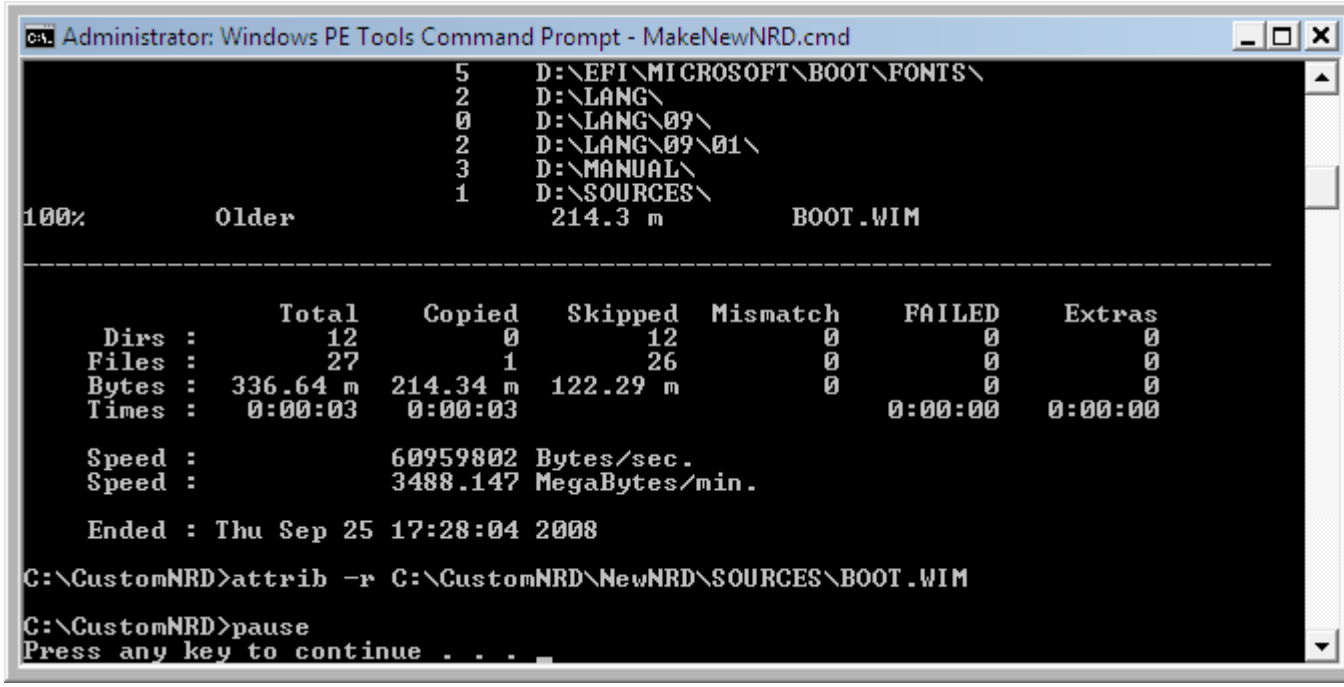


4. Navigate to “C:\CustomNRD” folder, and launch the “MakeNewNRD.cmd” script. Before running the script, remember to update any paths in the script to match the

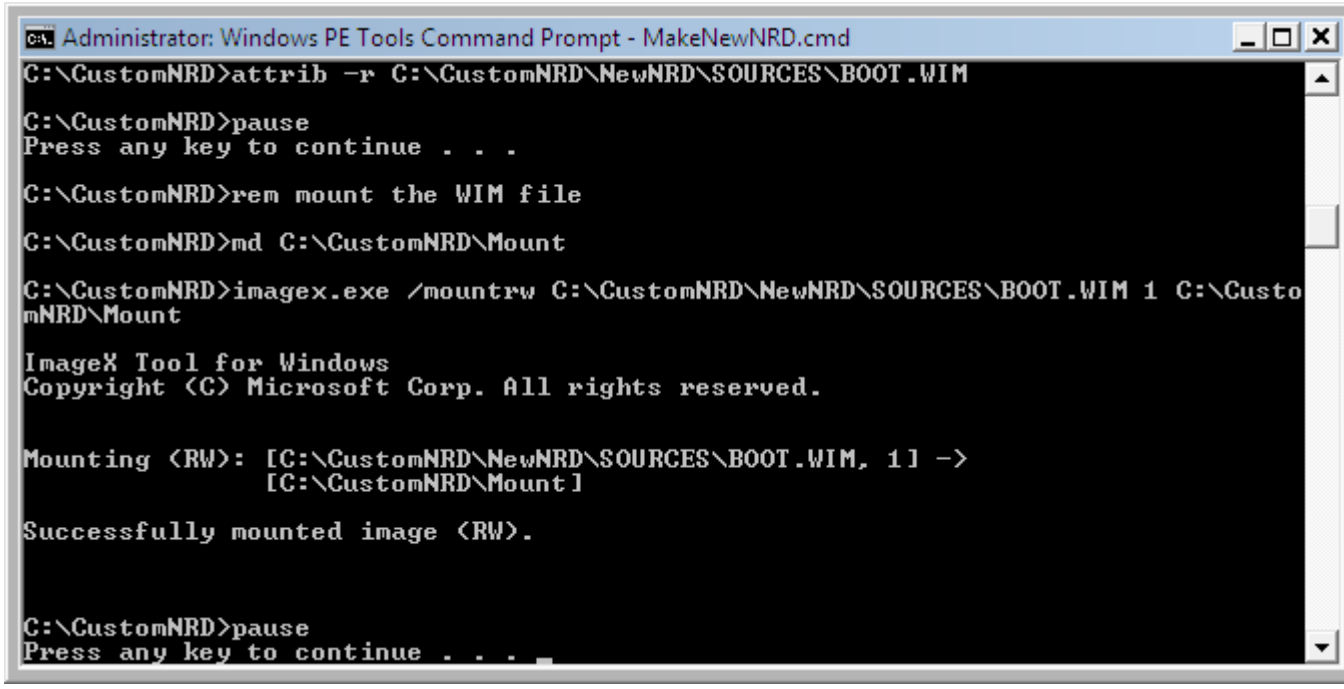
environment, i.e. original NRD disc drive letter, and path to drivers.



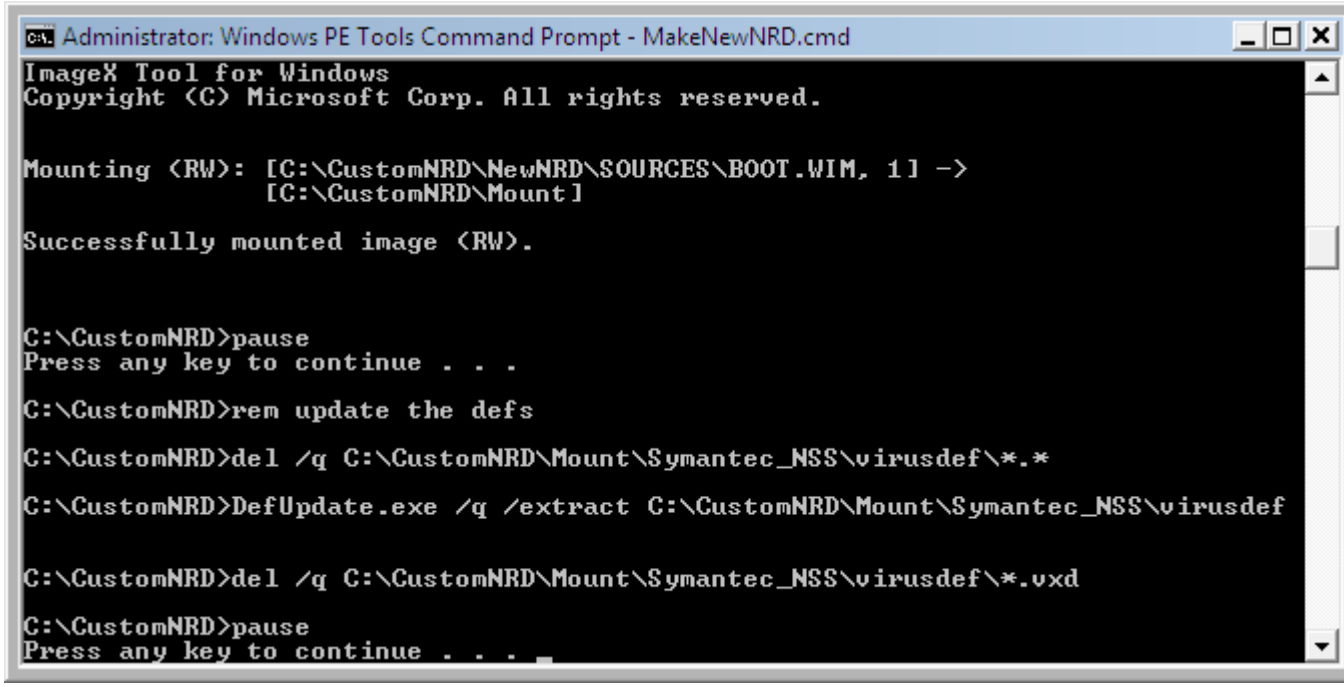
5. The script will copy the original NRD CD contents to the "C:\CustomNRD\NewNRD" folder. The default script expects the original NRD disc to be in drive "D:", if your NRD CD is in a different drive, remember to update the script before launching it.



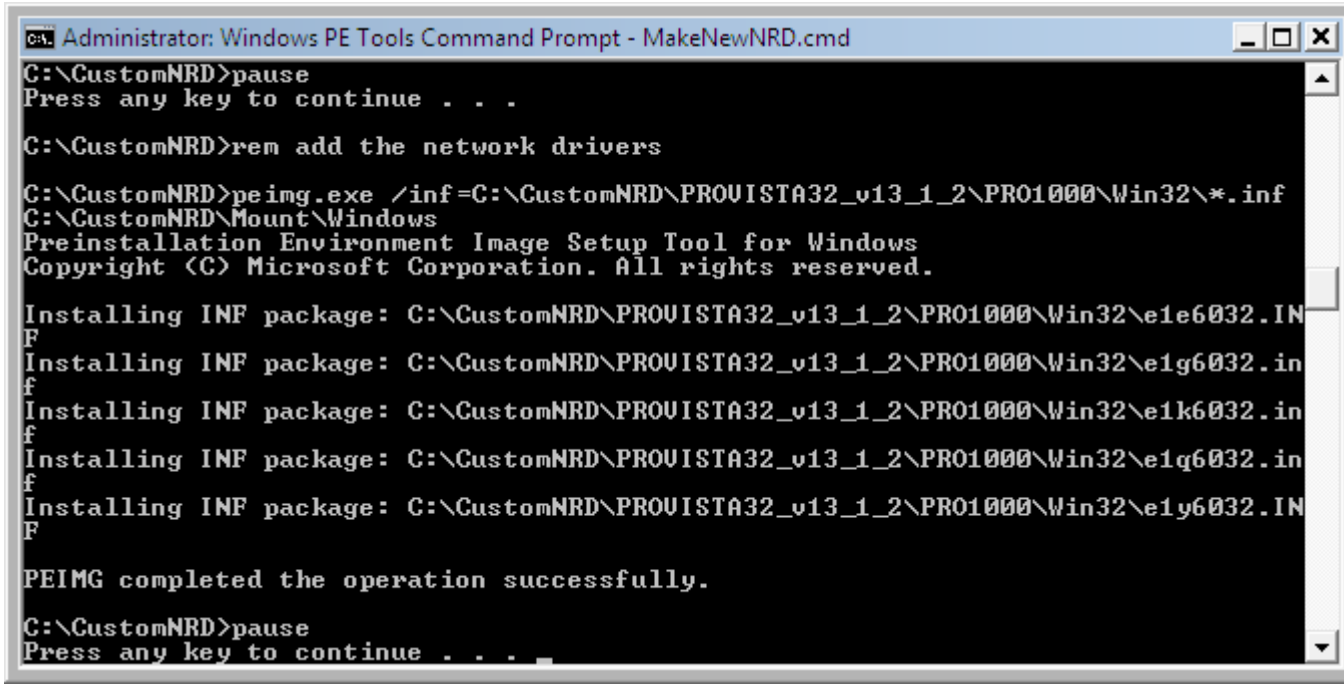
6. The script will mount the WinPE boot image WIM file to the “C:\CustomNRD\Mount” folder.
   Once mounted, the WinPE boot image can be modified.



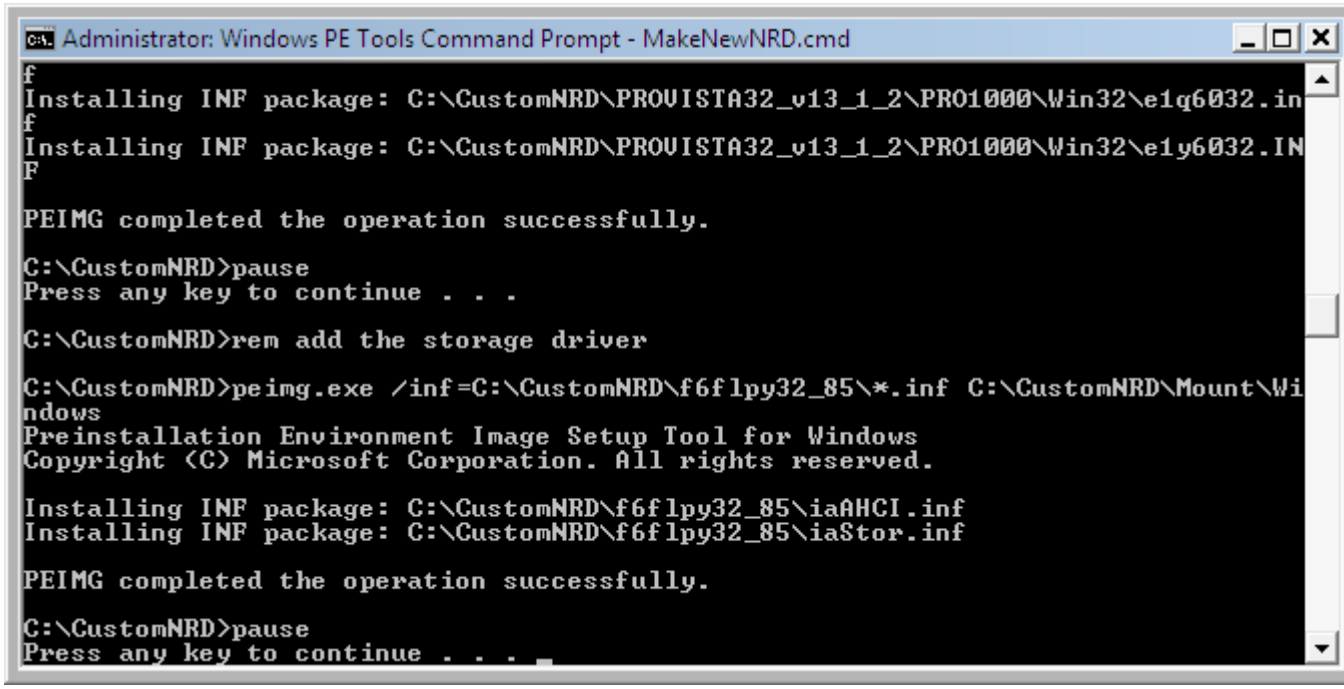
7. The script will update the virus definitions to the version you downloaded.
   Verify that the downloaded definition update file was saved as “DefUpdate.exe”.



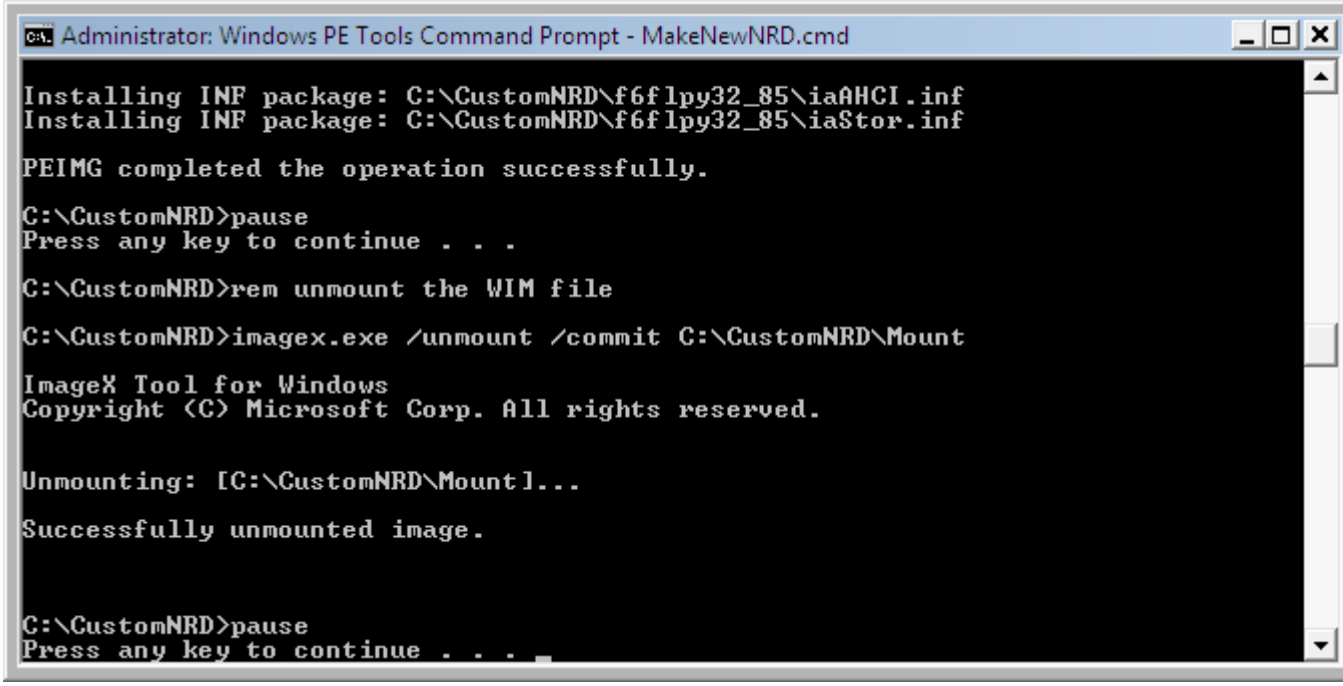
8. The script will add the network drivers.
   Remember to change the path in the script to point to the driver files.



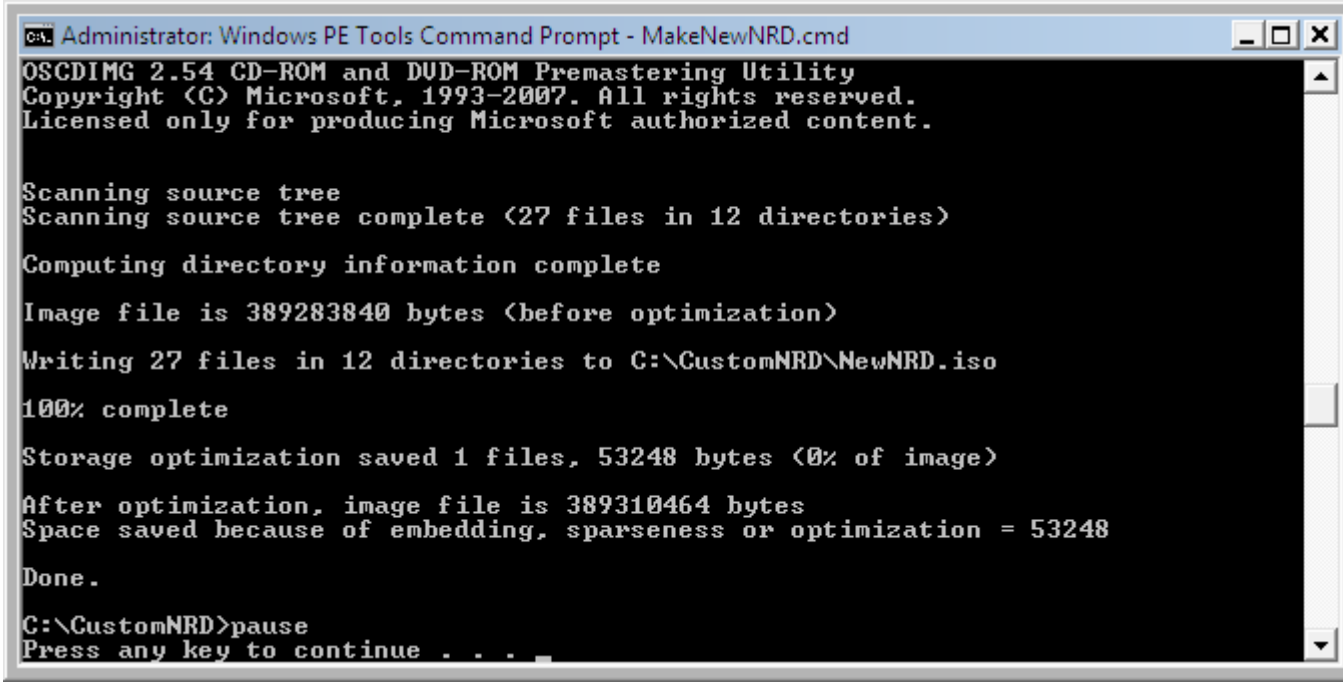
9. The script will add the storage drivers.
   Be sure to change the path in the script to point to the driver files.



10. The script will un-mount the WinPE image file.
    This will save all the changes made to the "C:\CustomNRD\Mount" directory to the WIM file.



11. The script will create a new ISO image.



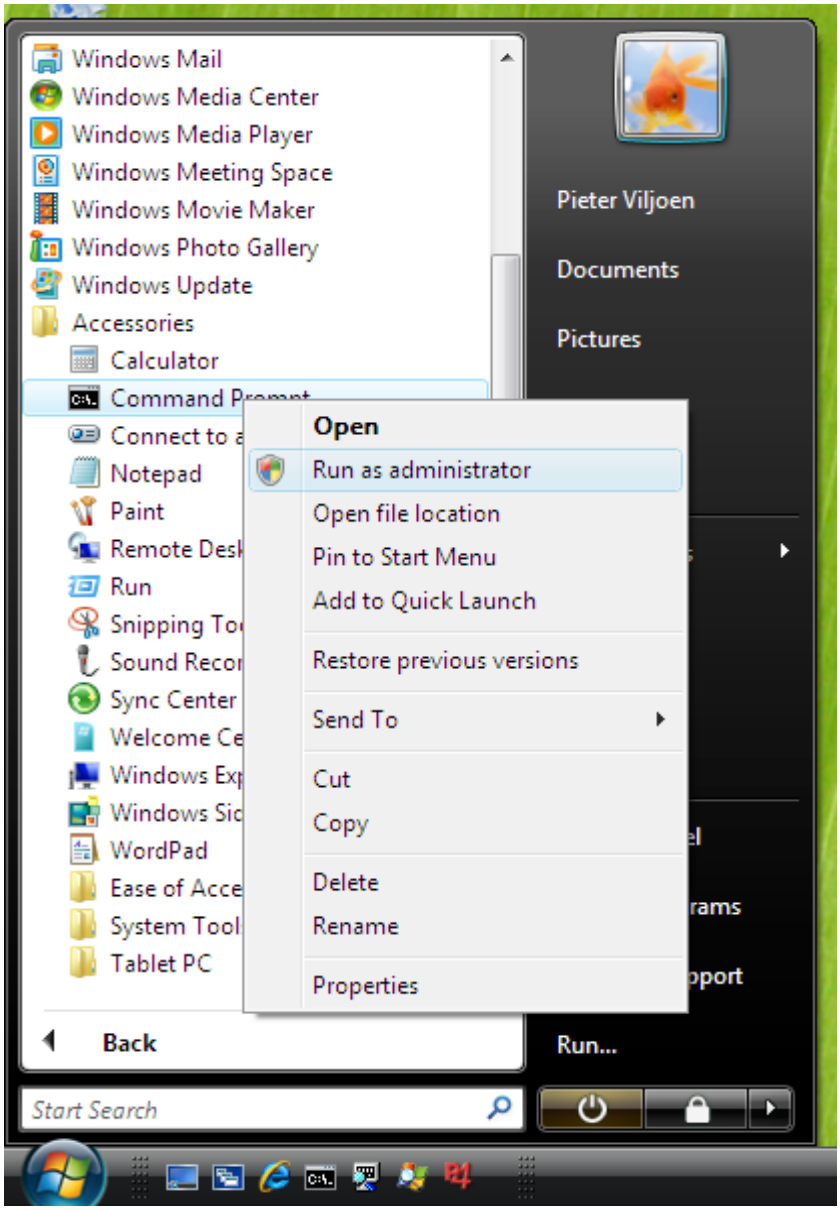
12. Burn the new "NewNRD.iso"file to a CD using a preferred CD burning software.
    Remember this is an ISO file, so the ISO file must be burned as a CD image, not as a file on the CD.

Note: There are many applications capable of burning ISO images to a CD. This site provides details on some of these applications: http://www.petri.co.il/how_to_write_iso_files_to_cd.htm

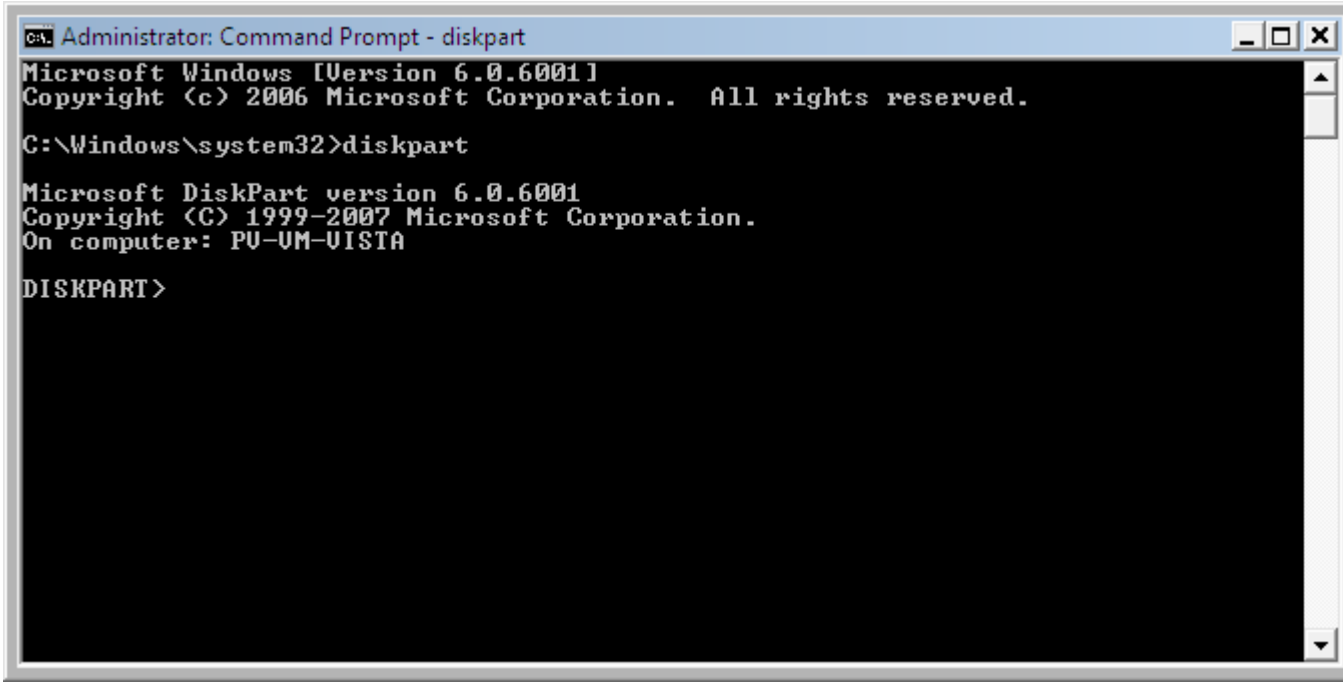
Run the NRD from a USB key

Booting from a USB key is much faster than booting from a CD, but requires hardware to support USB key booting, and requires the USB key to be specially formatted.

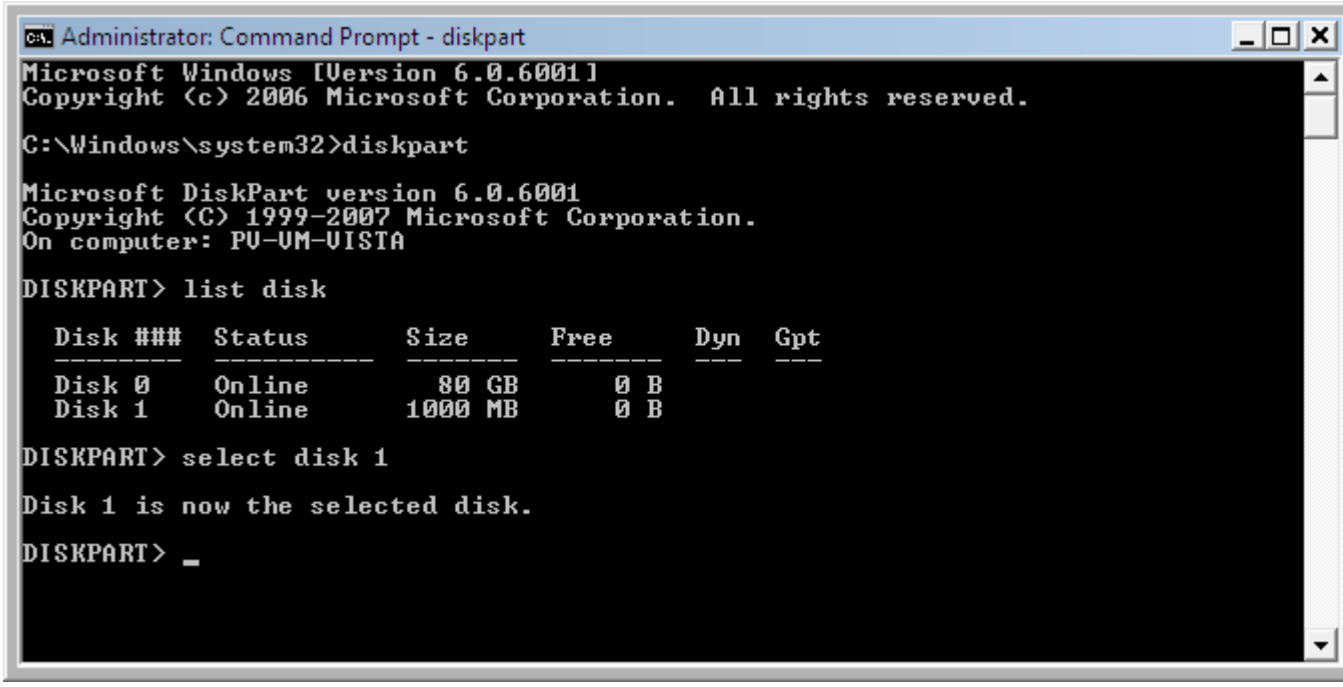
1. Connect the USB key to the system. Remember, you are formatting and deleting all data on this device.
2. Launch the “Command Prompt” from [Start][Programs][Accessories][Command Prompt].
3. On Vista this command must be executed by an elevated administrator. Right click on “Command Prompt” and select “Run as administrator”.



4. Launch the “diskpart.exe” utility.



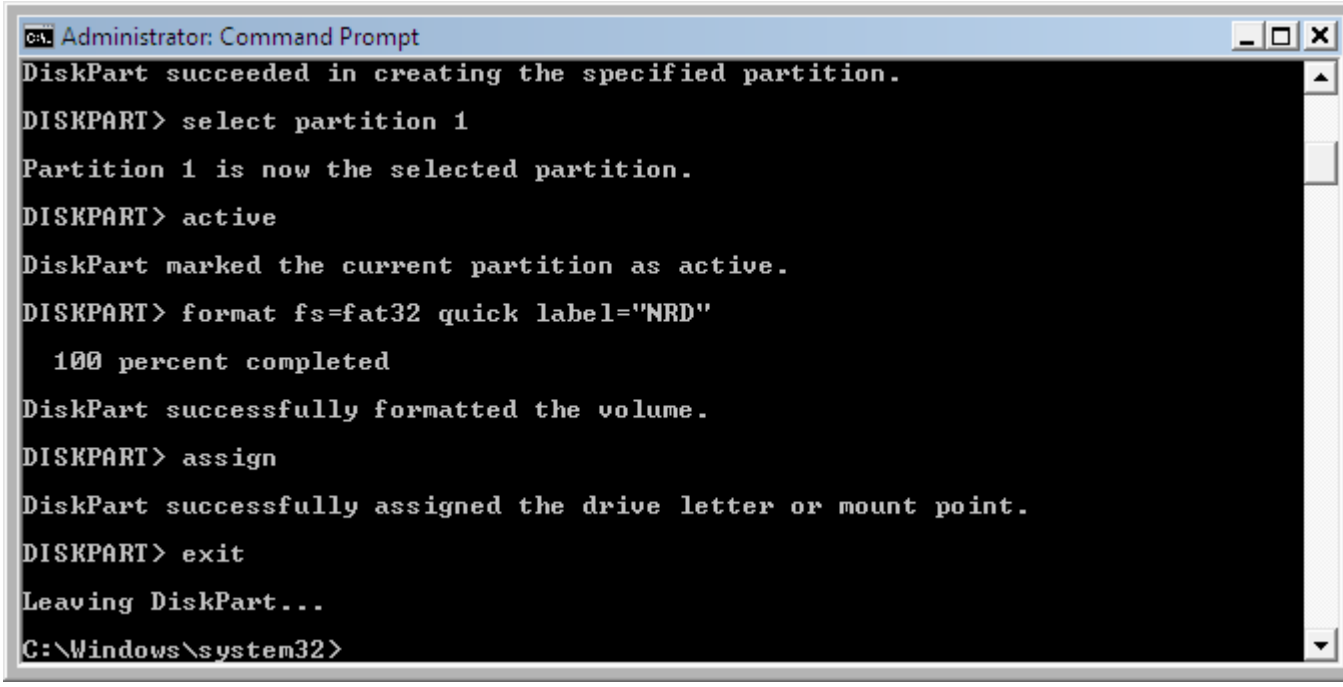
5. Select the correct disk for formatting.
   Issue the “list disk” command to display all disks, and identify the correct disk number for the USB key.
   Select that disk using the “select disk <number>” command.



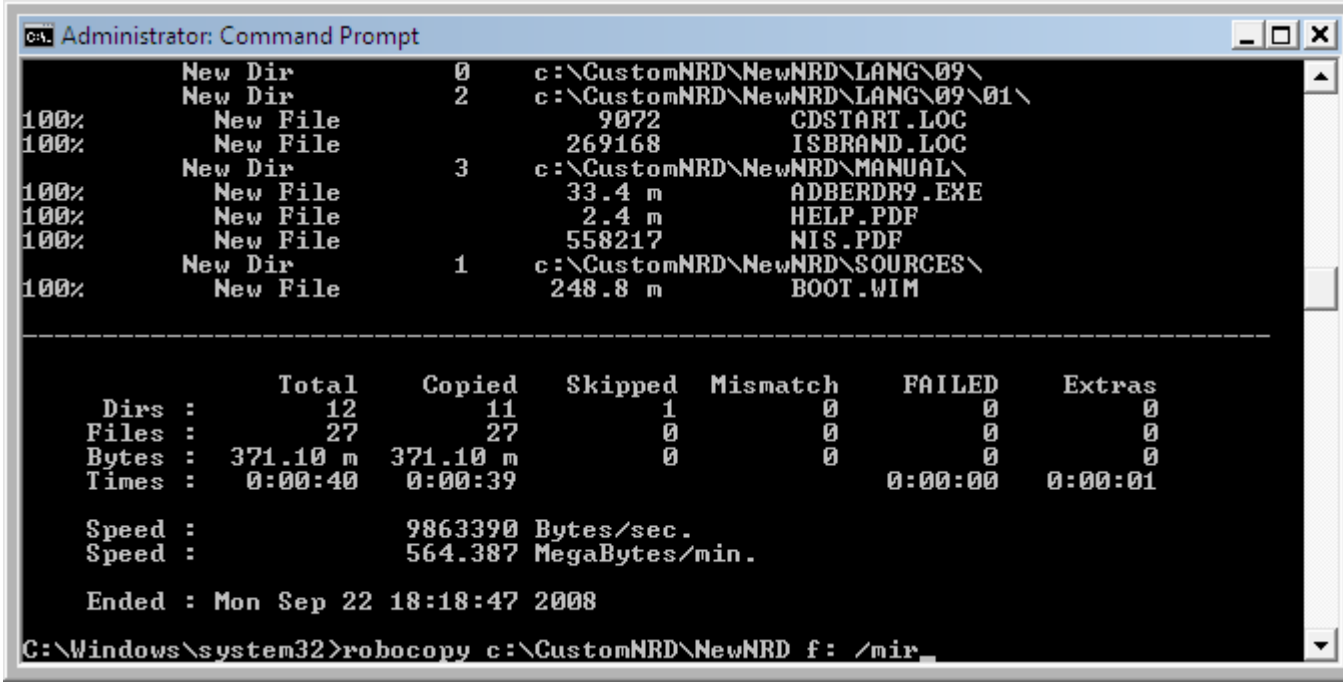
6. Format the drive using the following commands:

```
clean
create partition primary
```

```
select partition 1
active
format fs=fat32 quick label="NRD"
assign
exit
```



7. Copy the contents of the new NRD layout to the USB key.
   Remember to replace “f:” with the drive letter assigned to the USB key.
   `robocopy c:\CustomNRD\NewNRD f: /mir`



8. Boot the NRD from your USB key.

Note: Booting from an alternate device, such as a CD or a USB key, is hardware specific, but typically involves pressing a special key such as TAB or F9 or F10 or F12 during BIOS POST.

Conclusion

The Norton Recovery Disc is a version 1 product, and as such does not have any automated updating features. Future versions of the NRD will be enhanced to provide more streamlined updating and customization capabilities.