

## Windows Boot Process and Simple Troubleshooting

This is the (simplified) boot sequence for Windows NT, 2000, XP and 2003:

**BIOS:** performs Power On Self Test (POST)

**BIOS:** loads MBR from the boot device specified/selected by the BIOS

**MBR:** contains a small amount of code that reads the partition table, the first partition marked as active is determined to be the system volume

**MBR:** loads the boot sector from the system volume

**BOOT SECTOR:** reads the root directory of the system volume at loads NTLDR

**NTLDR:** reads BOOT.INI from the system volume to determine the boot drive (presenting a menu if more than 1 entry is defined)

**NTLDR:** loads and executes NTDETECT.COM from the system volume to perform BIOS hardware detection

**NTLDR:** loads NTOSKRNL.EXE, HAL.DLL, BOOTVID.DLL (and KDCOM.DLL for XP upwards) from the boot (Windows) volume

**NTLDR:** loads \WINDOWS\SYSTEM32\CONFIG\SYSTEM which becomes the system hive HKEY\_LOCAL\_MACHINE\System

**NTLDR:** loads drivers flagged as "boot" defined in the system hive, then passes control to NTOSKRNL.EXE

**NTOSKRNL.EXE:** brings up the loading splash screen and initializes the kernel subsystem

**NTOSKRNL.EXE:** starts the boot-start drivers and then loads & starts the system-start drivers

**NTOSKRNL.EXE:** creates the Session Manager process (SMSS.EXE)

**SMSS.EXE:** runs any programs specified in BootExecute (e.g. AUTOCHK, the native API version of CHKDSK)

**SMSS.EXE:** processes any delayed move/rename operations from hotfixes/service packs replacing in-use system files

**SMSS.EXE:** initializes the paging file(s) and the remaining registry hives

*\*\* before this step completes, bugchecks will not result in a memory dump as we need a working page file on the boot (Windows) volume \*\**

**SMSS.EXE:** starts the kernel-mode portion of the Win32 subsystem (WIN32K.SYS)

**SMSS.EXE:** starts the user-mode portion of the Win32 subsystem (CSRSS.EXE)

**SMSS.EXE:** starts WINLOGON.EXE

**WINLOGON.EXE:** starts the Local Security Authority (LSASS.EXE)

**WINLOGON.EXE:** loads the Graphical User Identification and Authentication DLL (MSGINA.DLL by default)

# Windows Boot Process and Simple Troubleshooting

**WINLOGON.EXE:** displays the logon window

**WINLOGON.EXE:** starts the services controller (SERVICES.EXE)

*\*\* at this point users can logon \*\**

**SERVICES.EXE:** starts all services marks as automatic

## NOTES:

The *SYSTEM* volume is the partition from which the boot process starts, containing the MBR, boot sector, NTLDR, NTDETECT.COM & BOOT.INI

The *BOOT* volume is the partition which contains the Windows folder - this can be a logical partition

## Example 1:

2 hard disks, 0 and 1

Disk 0, partition 0 is the SYSTEM volume

Windows is installed to "D:" which is disk 1, partition 0 [even if disk 0 has an extended & logical partitions] - this is the BOOT volume

- if either disk fails or is removed, Windows cannot boot

## Example 2:

1 hard disk, 2 partitions

Disk 0, partition 0 is the SYSTEM volume

Disk 0, partition 1 is the BOOT volume [D:]

- add another disk to the system and create a partition on it, this becomes D: and Windows will not boot [disk 0, partition 1 now becomes E:]

## Boot Problems And Their Possible Causes & Resolutions:

### Symptoms:

*Black screen*

*"Invalid Partition Table"*

*"Error loading operating system"*

*"Missing operating system"*

### Cause:

*Corrupt Master Boot Record (MBR)*

### Resolution:

*Boot into Recovery Console and run "fixmbr" to repair the MBR*

### Symptoms:

*"A disk read error occurred"*

*"NTLDR is missing"*

*"NTLDR is compressed"*

### Cause:

*Corrupt boot sector*

## Windows Boot Process and Simple Troubleshooting

### **Resolution:**

*Boot into Recovery Console and run "fixboot" to repair the boot sector*

### **Symptoms:**

*"BOOT.INI is missing or corrupt"*

*"Boot device inaccessible"*

*"Windows could not start because the following file is missing or corrupt:*

*<Windows root>\system32\hal.dll"*

### **Cause:**

*BOOT.INI missing, corrupt or out of date as a partition has been inserted*

### **Resolution:**

*Boot into Recovery Console and run "bootcfg /rebuild" to repair the BOOT.INI*

### **Symptoms:**

*"Windows could not start not start because the following file is missing or corrupt:*

*\\WINDOWS\\SYSTEM32\\CONFIG\\SYSTEM"*

### **Cause:**

*Corrupt/missing system hive*

### **Resolution:**

*1. Boot into Recovery Console and run "chkdsk C: /f" to check the system disk for errors and fix them, then reboot.*

*2. If the error continues and System Restore is enabled, copy the system hive from the last restore point into \\WINDOWS\\SYSTEM32\\CONFIG*

*3. If the error continues, copy the system hive from \\WINDOWS\\REPAIR into \\WINDOWS\\SYSTEM32\\CONFIG*

*4. If the error continues, perform a repair installation by booting from the Windows installation media*

### **Symptoms:**

*"Windows could not start because of a computer disk hardware configuration problem.*

*Could not read from the selected boot disk, Check boot path and disk hardware."*

### **Cause:**

*Boot volume (with Windows folder) is not accessible as defined in BOOT.INI*

### **Resolution:**

*Check the boot volume is accessible*

### **Symptoms:**

*Dual-boot 32-bit Windows and 64-bit Windows system reports "NTOSKRNL.EXE is corrupt" trying to boot into 64-bit Windows*

### **Cause:**

## Windows Boot Process and Simple Troubleshooting

*System volume contains an older boot loader than the boot volume requires - e.g. XP SP2 installed after XP x64*

### **Resolution:**

*Copy NTDETECT.COM and NTLDR from XP x64 installation media to the root of the system volume*

### **Notes:**

Not all of the above applies to Windows Vista/Longhorn, there are a few differences:

the boot loader is different, and if the machine has a TPM 1.2 chip then BitLocker might be involved right at the start to decrypt & validate the boot code

the boot drive will become "C:" regardless of which partition it might be (so any bootable Vista volume will refer to itself as C: even in a multi-boot environment)

WINLOGON.EXE no longer launches SERVICES.EXE, this is handled by a separate process WININIT.EXE, as session 0 is now solely the system area and not combined with the console desktop (the first interactive logon session becomes session 1)

the recovery options are more automated via wizards by booting from the installation DVD, common faults can be checked for automatically