Windows Boot Process:

1. BIOS
2. OS Loader
3. Kernel Initialization
4. Session Initialization
5. Winlogon Initialization
6. Explorer Initialization
7. Post Boot Activity
8. BIOS
9. OS Loader
10. OS Initialization ( 3-7)

OS Loader:

Read drivers, read parts of registry

Kernel Initialization:

Enumerate devices, initialize and start drivers (PnP)

Session Init:

Init sessions, load win32k subsystem init, graphics, launch SCM

Winlogon Init:

Launch various services, orchestrate session logon

Explorer Init:

Init the shell, process and run auto run tasks

Post Boot Activity:

Numerous application and services consuming CPU and disk resources.

Windows booting procedure

<https://kb.acronis.com/sites/default/files/content/2006/01/1934/windows_booting_procedure.pdf>

BIOS: POST and Read MBR

POST -> Power On Self Test. Checks all hardware devices connected to a computer, like RAM, hard disk. Makes sure that the system can run smoothly with those hardware devices. If the POST is a failure the system halts with a beep sound. The BIOS checks the boot priority. MBR is read by the BIOS. MBR is Master Boot Record. First sector on the hard disk.

Boot Loader

2 stages of boot loader. Stage 1, stage 2. MBR contains the stage 1 boot loader and stage 1 boot loader is a link to the stage 2 boot loader. Stage 2 booat loader resides in the boot partition and it loads the kernel to memory.

Boot files: NTLDR, NTDETECT.COM, BOOT.INI

NTLDR -> NT Loader. Second stage bootloader. Path is C:\Windows\i386\NTLDR

Boot.ini -> contains config files of NTLDR. C:\boot.ini we cannot pass arguments to kernel, so you pass arguments using boot.ini

NTDETECT.COM -> this file detect hardware’s and passes information to NTLDR. Using the collected information the NTLDR creates a hardware key and this key is used to detect hardware’s. A new hardware key is generated after each reboot of the operating system and that’s why system asks to reboot after installation of a new hardware. The hardware keys created by NTLDR can be found in Windows registry a HKEY\_LOCAL\_MACHINE -> HARDWARES.

Kernal Loading

After executing the functions of boot files the control is passed to Kernel. Ntoskrnal.exe is the kernel file in Windows machine and its path is C:\Windows\system32\ntoskrnal.exe. Kernel acts as a layer between software and hardware. The library file hal.dll (C:\Windows\system32\hal.dll) helps Kernel to interact with hardware’s. HAL stands for Hardware Abstraction Layer and this hal.dll file is machine specific. Now the drivers for hardware’s are loaded from the file C:\Windows\system32\config\system and the Kernel is loaded to primary memory

Starting Services

When kernel is loaded in the primary memory services for each process is started and the registry entry for those services can be found at HKEY\_LOCAL\_MACHINE – System – Current control set – Services. Winlogon.exe (C:\Windows\system32\winlogon.exe) is the last service started during this process. Winlogon.exe starts the log in procedures of windows machine. It first calls the library file msgina.dll (system32\msgina.dll) MSGINA stands for Microsoft Graphics Identification and Authentication and it provides the log in window. Now msginal.dll passes the control to LSA (Local Security Authority), it verifies the username and password from the SAM file. SAM (Security Accounts Manager) contains the information about all users created in a Windows operating system.

Checking SAM by LSA