Windows 시스템의 부팅 프로세스

Microsoft MVP
Windows Development
신승운

1. Booting

Boot Manager 가 메모리 상에 로드되고 실행되면서 시작된다.

1-1. BIOS(Basic Input/Output System)의 경우

1-1-1. POST (Power On Self Test)

펌웨어가 BIOS 일 경우, 가장 먼저 POST 동작을 수행한다. POST 는 현재 장착된 하드웨어를 점검하며 전반적인 Device 들의 상태를 확인한다.

1-1-2. MBR boot code

다음으로 BIOS 는 부팅 섹터를 찾기 위해 부팅 가능한 디바이스 목록을 검색한다. 부팅 가능한 장치가 하드디스크라면 이 장치의 부트 섹터를 MBR(Master Boot Record) 라고 부른다. (만약, 부팅 가능한 장치가 CD, Floppy 디스켓 등과 같이 하드 디스크가 아니라면 BIOS 는 장치의 VBR 메모리에 로드하여 실행시킨다.)

MBR 은 기본적으로 MBR Boot code 와 파티션 테이블을 가지고 있다. MBR Boot code 가 실행되면서 파티션 테이블 중 활성화 파티션(= *active partition*, *bootable partition*, *system volume*) 즉, 부팅 가능한 파티션을 찾아 메모리에 로드한다. 이 부팅 가능한 파티션을 VBR(Volume Boot Record) 이라고 한다.

1-1-3. VBR boot code, Boot Manager

VBR 에도 VBR boot code 가 존재하며, VBR boot code 는 자신의 파티션에서 16bit 의 boot manager program(*%SystemDrive%₩bootmgr* 에 존재)을 찾는다. 이 16bit 의 bootmgr 은 32bit bootmgr 코드 앞에 붙어 있어, 사실상 두개의 실행파일이 연결되어 있다. 64bit Windows 의 경우, bootmgr 에 64bit 명령어가 포함된다.

16bit 의 boot manager 는 Real Mode 에서 동작하며 데이터 구조체 초기화, Protected Mode 로의 전환을 수행한 뒤 Protected mode 에서 동작하는 boot manager program(32bit)을 메모리에 로드 시킨다.

- BIOS 부팅, 동작 흐름

펌웨어가 BIOS 일 경우 수행하는 동작 흐름은 아래와 같다.

1-2. EFI(Extensible Firmware Interface)의 경우

1-2-1. POST (Power On Self Test)

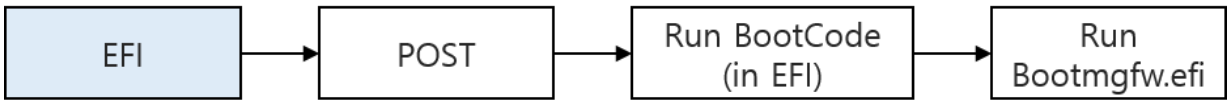
펌웨어가 EFI 일 경우 역시 가장 먼저 POST 동작을 수행한다.

1-2-2. Boot code, Boot Manager(bootmgfw.efi)

EFI 방식에서의 Boot code 는 MBR 이나 VBR 에 존재하지 않고, 펌웨어 안에 존재한다. 펌웨어 안에 존재하는 Boot code 는 %SystemDrive%₩EFI₩Microsoft₩Boot₩Bootmgfw.eif 에 존재하는 EFI 실행 프로그램을 구동 시킨다.

- EFI 부팅, 동작 흐름

펌웨어가 EFI 일 경우 수행하는 동작 흐름은 아래와 같다.



2. Boot Manager (부팅 관리자)

EFI 방식이나 BIOS 방식 둘다 최종적으로 Boot Manager(bootmgr)를 메모리에 로드하여 실행시킨다. Boot Manager 는 BCD(Boot Configuration Data) 설정 데이터를 사용하여 시스템을 시작한다(BCD 는 레지스트리 하이브 파일로 존재). 최종적으로 Windows Boot Loader 인 winload.exe 를 로드하고 실행한다.

- BCD(Boot Configuration Data)

BCD 하이브 데이터는 "HKLM₩BCD00000000" 레지스트리 경로에 존재한다. 일반적으로 BCD 파일을 조작하기 위해 bcdeidt.exe 를 사용한다. 또한 BCD 는 다음과 같은 최소한 2 개 이상의 요소를 포함하고 있다.

- 하나의 Windows Boot Manager Object
- 하나 이상의 Windows Boot Loader Object

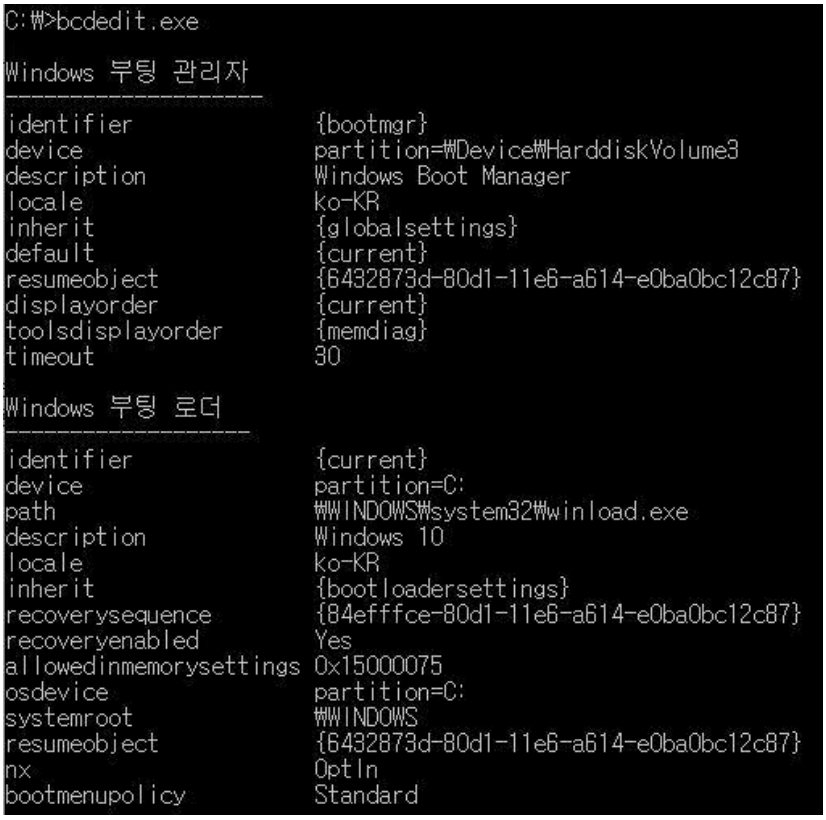
- Boot Manager Object

BCD 가 포함하고 있는 Boot Manager Object 는 문자 셋 기반의 BOOT MANAGER 화면의 모든 설정 값을 가진다. 예를 들면, OS 의 개수, 부팅 도구 메뉴, 기본 타입 아웃 값 등이 이에 해당한다.

Boot Manager Object 는 {9DEA862C-5CDD-4E70-ACC1-F32B344D4795} 레지스트리에 정의되어 있으며, bcdedit.exe 실행 시 {bootmgr} 이라는 이름으로 볼 수 있다.

- Boot Loader Object

Boot Loader Object 는 OS 별로 가지고 있는 부팅 설정 값을 나타낸다.
만약, 현재 PC 가 한개의 Boot Loader Object 를 가지고 있다면, Boot Manager 화면은 표시되지 않는다.



<bcdedit.exe 실행 시 보여지는 Boot Manager Object 와 Boot Loader Object 값>

3. Windows Boot Loader (윈도우즈 부트 로더)

구동 시킬 운영체제가 선택된 후 Boot Manager 는 선택된 운영체제의 Boot Loader Object 가 가리키고 있는 위치의 Windows Boot Loader 를 로드하고 실행시킨다.
(winload.exe 를 말하며 일반적으로 %SystemRoot%₩System32 경로에 존재)

- Winload.exe

이전 버전의 Windows 에서는 NTLDR(NT Loader) 이 winload.exe 와 같은 역할을 수행했다.
아래에서 winload.exe 가 로드 되고 난 뒤 수행하는 동작들에 대해 알아본다.

3-1. SYSTEM 레지스트리 로딩

HKLM₩SYSTEM 레지스트리를 로딩 한다.
SYSTEM 레지스트리 하이브 파일은 %SystemRoot%₩System32₩config 경로에 존재한다.

3-2. Self 무결성 검사

winload.exe 는 현재 로드 되어 있는 자신의 이미지에 대한 무결성 검증을 수행한다.
현재 로딩 되어 있는 winload.exe 의 서명과 카테고리 파일 nt5.cat 에 존재하는 서명을 비교하여 무결성 검증을 수행한다.

이 무결성 검사에 실패하면, winload.exe 는 종료(HALT) 된다. 예외적으로, kernel-mode 디버깅 중일 때는 경고 메시지만 출력한다.

3-3. ntoskrnl.exe, hal.dll 로드

무결성 검사가 끝난 winload.exe 는 ntoskrnl.exe 와 hal.dll 을 메모리에 로드 한다.
이때, 커널 디버깅 기능이 활성화되어 있다면 아래와 같은 kernel-mode 드라이버도 같이 로드 한다.

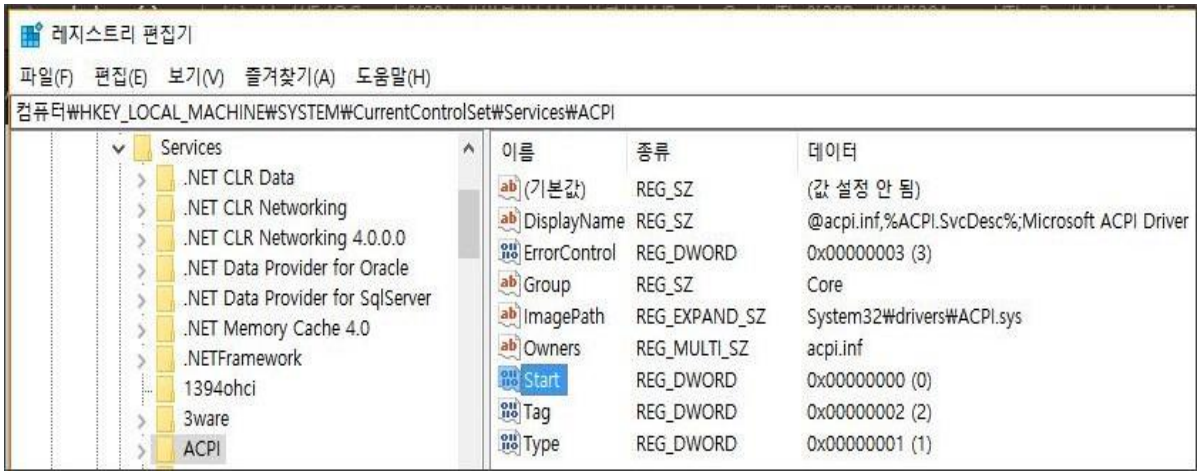
- kdcom.dll (null modem cable)
- kd1374.dll (IEEE1394 cable)
- kdusb.dll (USB 2.0 Debug cable)

ntoskrnl.exe 는 자신이 import 하고 있는 DLL 에 대해 무결성 검사(nt5.cat 과 비교)를 마친 뒤 문제가 없다면, 아래의 순서와 같이 DLL 을 로드 한다.

1. pshed.dll
2. bootvid.dll
3. clfs.sys
4. ci.dll

3-4. Boot Class Service 로드

winload.exe 는 HKLM₩SYSTEM₩CurrentControlSet₩Services 에 존재하는 모든 값을 조회하여 boot class 카테고리에 해당하는 서비스 드라이버를 로드 한다.
레지스트리 하위 키 중 Start 값이 0x00000000(SERVICES_BOOT_START) 인지 참조하여 boot class 드라이버인지 확인할 수 있다.



만약 무결성 검사 옵션이 활성화되어 있다면, winload.exe 는 nt5.cat 파일과 로드 되는 드라이버들의 서명을 비교한다. 도중에 무결성 검사가 실패하면, winload.exe 는 종료(HALT) 된다. 예외적으로, kernel-mode 디버깅 중일 때는 경고 메시지만 출력하지만, 아래의 목록에 존재하는 파일에 대한 무결성 검증이 실패하면 kernel-mode 디버깅 중일 때에도 winload.exe 는 종료된다.

- bootvid.dll
- ci.dll
- clfs.sys
- hal.dll
- kdcom.dll
- kd1394.sys

- kdusb.dll
- ntoskrnel.exe
- pshed.dll
- winload.exe
- ksecdd.sys
- spldr.sys
- tpm.sys

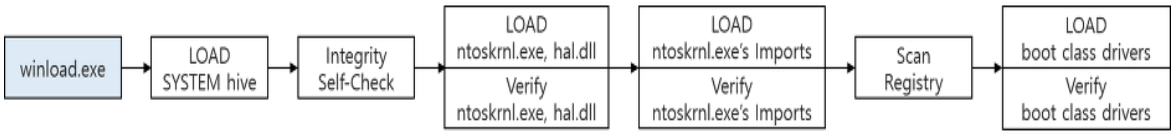
3-5. Protected Mode 전환 준비 및 ntoskrnl.exe 실행

최종적으로 winload.exe 는 protected mode 의 페이징을 활성화하고,
boot log 를 저장한 뒤, ntoskrnl.exe 로 실행을 넘겨준다.

("bcdedit.exe /set BOOTLOG TRUE" 옵션을 설정하여 생성되는 Ntbtlog.txt 를 통해 로드 되는 이미지들에 대한 자세한 로그를 확인할 수도 있다.)

- winload.exe 동작 흐름 정리

winload.exe 에서 수행하는 동작 흐름을 간략하게 도식화하면 다음과 같다.



4. ntoskrnl.exe 실행 (Executive 동작)

ntoskrnl.exe 는 실제로 광범위한 동작을 수행하며, 각종 초기화와 설정을 시작한다. 예를 들어, 메모리 관리자가 페이지 테이블을 생성하고, 인터럽트 컨트롤러를 설정하며, SSDT 가 생성되는 등의 동작이 수행된다. 아래에서는 ntoskrnl.exe 가 수행하는 몇 가지 동작에 대해서만 기술한다.

- System Class Service 로드

winload.exe 에서 수행한 것과 같이 HKLM₩SYSTEM₩CurrentControlSet₩Services 에서 Start 키 값이 0x00000001(SERVICE_SYSTEM_START) 인 것과 Type 키 값이 0x00000001(SERVICE_KERNEL_DRIVER) 또는 0x00000002(SERVICE_FILE_SYSTEM_DRIVER) 인 것에 대해서 서비스를 로드 한다. 로드하는 드라이버에 대해서 무결성 검증이 실패하면, 드라이버는 로드 되지 않는다.

- smss.exe 로드 및 실행

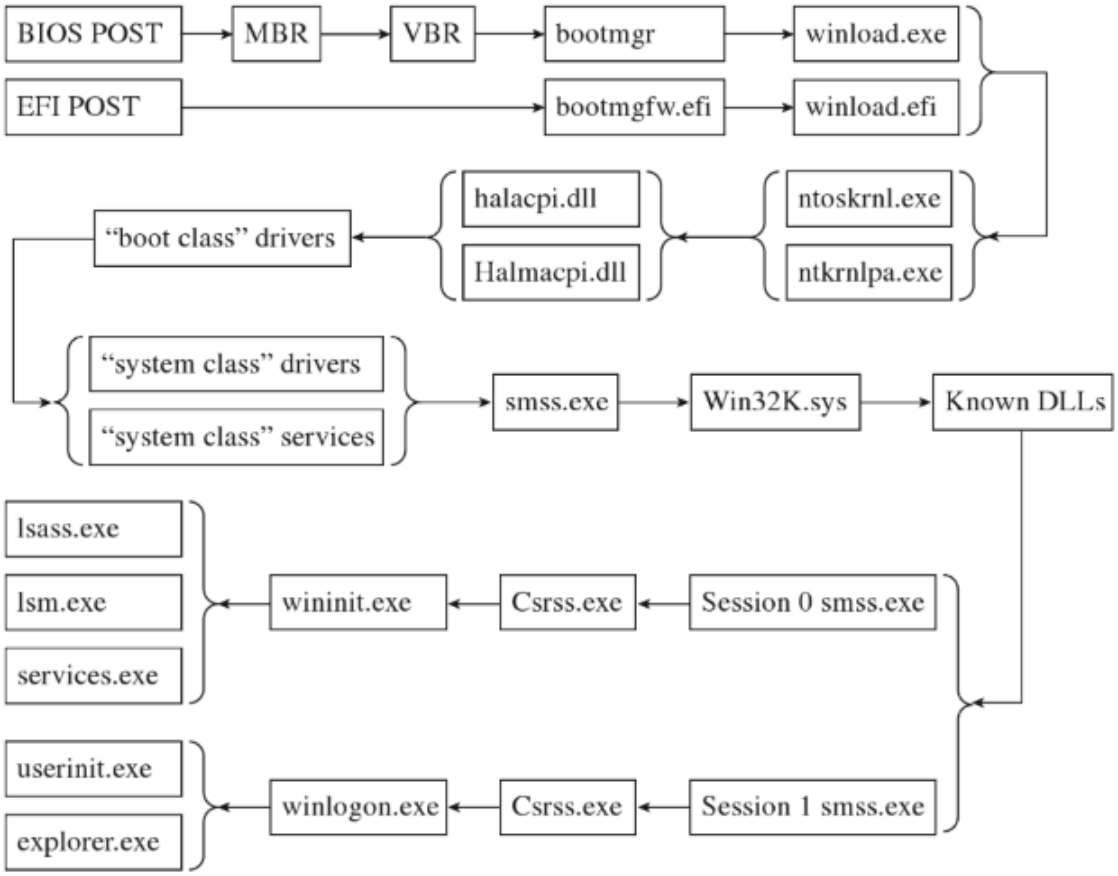
smss.exe 를 초기화 하고 실행한다.

5. smss.exe 실행

6-1. wininit.exe 실행

6-2. winlogon.exe 실행

출처: https://elfmfl.tistory.com/25



1. Run BootManager

① BIOS Firmware

- POST: 부팅 시 가장 먼저 동작. 하드웨어를 점검합니다.

- Load Boot Manager: 디스크의 첫번째 섹터인 MBR(Master Boot Record)로부터 파티션 테이블을 검색하여 부팅가능한 파티션의 VBR(Volume Boot Record)를 읽습니다.

VBR은 16bit Boot Manager(%System-Drive%bootmgr) 프로그램을 읽습니다. 16bit 코드는

(32bit/64bit) 코드 앞에 붙어서 존재합니다.

② EFI Firmware

- POST: BIOS과정과 동일합니다.

- Load BootCode: Boot Code가 펌웨어 내부에 내장되어 있어 MBR 과 VBR로드과정이 없습니다.

EFI Firmware는 Protected Mode로 전환하여 32bit/64bit bootmgr.efi 프로그램이 실행되도록 합니다.

2. Windows Boot Manager

Read BCD(Boot Configuration Data): 부팅구성에 필요한 Data를 읽어옵니다.

- BCD(Boot Configuration Data)

하나의 Windows Boot Manager Object, 하나 이상의 Windows Boot Loader Object로 구성

- 레지스트리: HKLM/BCD000000
- 파일 BISO /EFI: %SystemDrive%₩Boot₩와 %SystemDrive%EFI₩Microsoft₩Boot₩

① Windows Boot Manager Object

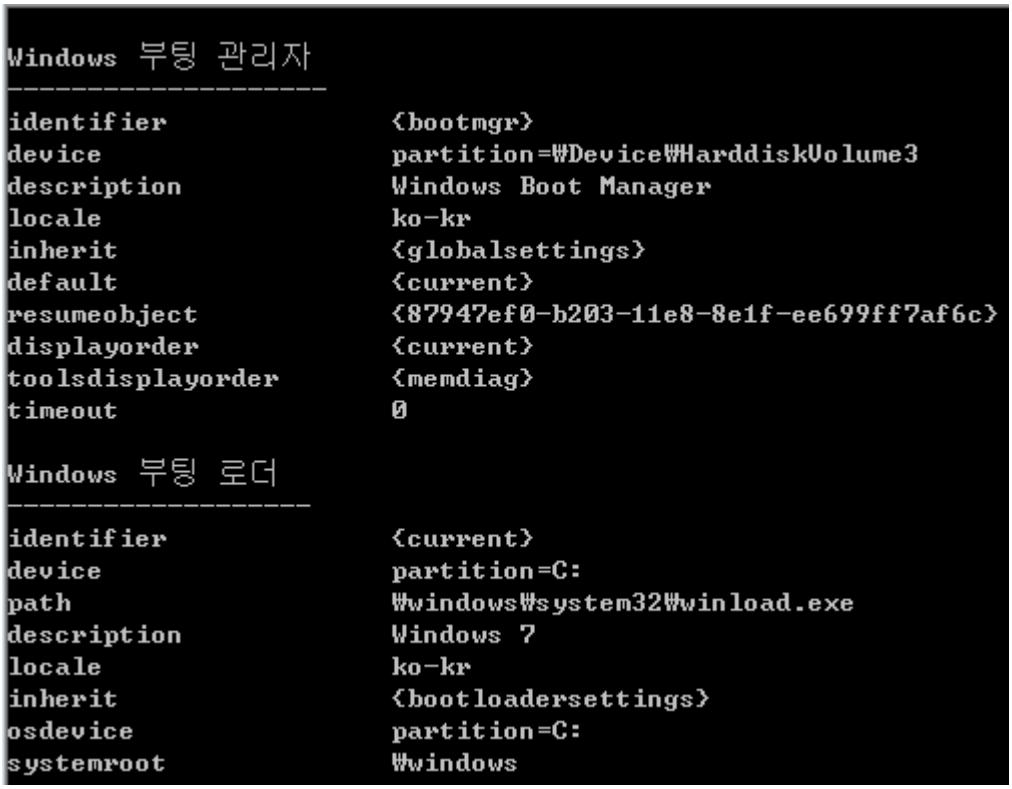
Boot Manager 화면의 설정값들(OS개수, 부팅도구메뉴 등)을 의미한다.

- 레지스트리 sub-key: {9dea862c-5cdd-4e70-acc1-f32b344d4795}

- BCDEdit.exe: 실행 시 Identifier Bootmgr에서 보여줍니다.

② Windows Boot Loader Object

설치된 OS가 가지는 구성을 나타냅니다.



3. Windows Boot Loader (winload.exe, NTLDR, Winload.efi)

① Load SYSTEM registry: HKLM/SYSTEM하위의 레지스트리를 로드

② winload의 무결성검사 로드된 이미지의 시그니쳐와 nt5.cat

(%SystemRoot%₩System32₩CatRoot₩{F750E6C3-38EE-11D1-85E5-00C04FC295EE}₩)과 비교가 진행됩니다. 일치하지 않으면 종료, 디버깅 활성화 중이라면 경고메시지만을 보여줍니다.)

③ ntoskrnl.exe와 hal.dll을 로드. 커널 디버깅 활성화시, 다음의 kernel-mode driver를 로드합니다.

- Kdcom.dll (null modem cable)
- Kd1394.dll (IEEE1394 cable)
- Kdbus.dll (USB2.0 Debug cable)

무결성검사 이후 다음의 dll들을 로드합니다.

- pshed.dll
- bootvid.dll
- clfs.sys
- ci.dll

로드 이후 HKEY_LOCAL_MACHINE₩SYSTEM₩CurrentControlSet₩services₩하위의 sub key들을 스캔하여 Start Value가 0x00000000(SERVICE_BOOT_START)를 가지는 디바이스 드라이버를 찾습니다.

④ Load Device Driver

무결성 체크가 활성화되어 있다면 nt5.cat과 검색된 드라이버의 디지털서명을 비교한다. 실패한다면 Boot Loader를 종료하고 디버깅 활성화 중이라면 경고 메시지만을 보여줍니다.

⑤ 실행에 필요한 프로그램 및 구성요소 초기화
ntoskrnl.exe에서 KiSystem-Startup()실행 시, ntoskrnl.exe의 주소공간에서 subsystem 및 구성하는 데이터들을 초기화를 시킵니다. (SSDT구성, NTDLL.DLL로드 등)
레지스트리(HKEY_LOCAL_MACHINE₩SYSTEM₩CurrentControlSet₩services₩ 의 Start == SERVICE_SYSTEM_START,Type)시스템 클래스드라이버 및 서비스에 대한 검사를 진행합니다.
드라이버 무결성 체크가 활성화되어 있다면 ci.dll에있는 무결성 루틴을 수행하여 디지털 서명을 체크한다. 실패하면 로드되지 않습니다.

4. Session Manager

Session Manager 초기화

① "HKLM₩SYSTEM₩CurrentControlSet₩Control₩Session Manager₩"에 등록된 프로그램 실행

② 환경변수 세팅 및 윈도우즈 SubSystem실행

※ Smss.exe로드

-> Win32k.sys 초기화 및 로드(VGA모드로 전환)

->"HKLM₩SYSTEM₩CurrentControlSet₩Control₩Session Manager₩KnownDlls₩" Dll을 로컬 시스템 계정 하위에 로드

-> Csrss.exe로드(Windows API를 사용 가능하게 함)

-> 세션 0(wininit.exe)과 1(winlogon.exe)을 실행

※Wininit.exe 실행 시

- lsass.exe 실행: local security authority subsystem
- services.exe: Service Control Manager(레지스트리: SERVICE_AUTO_START값을 가지는 모든 드라이버 로드)
- lsm.exe: local session manager(원격 연결을 관리)

※Winlogon.exe 실행 시

- logonui.exe 실행: ctrl+alt+delete
- "HKLM₩SOFTWARE₩Microsoft₩Windows NT₩CurrentVersion₩Winlogon₩"하위 "Shell"(explorer.exe),"UserInit"(userinit.exe)값들을 실행
- UserInit.exe는 다음의 레지스트리 값을 가지는 프로그램을 실행한다.

```
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce\
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\
HKCU\Software\Microsoft\Windows\CurrentVersion\Run\
HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce\

%SystemDrive%\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup\
%SystemDrive%\Users\%USERNAME%\AppData\Roaming\Microsoft\Windows\Start Menu\
```

출처: https://jeep-shoes.tistory.com/35

끝.