2. MBR이란?

앞에서 MBR을 분석하기 위해 필요한 사전지식(?)을 조금 공부하였다, 생판 컴퓨터가 처음인 사람이라면 물론 조금 어렵겠지만 언젠가는 자연스럽게 이해가 될 수 있는 내용이기도 하며 이 글을 보고 있을 대부분의 컴퓨터 전공자들은 시시한 내용이 될 수 있다. 하지만 개인적인 의견으로는 정말 컴퓨터를 좋아한다면 이러한 과정조차도 즐겨야 한다고 생각한다. 그럼 새로운 마음가짐으로 MBR이 무엇인지 본격적으로 알아 보도록 하자.

2.1 부트 프로세스 (Boot Process)

서론부터 MBR을 알아보자 라는 말로 벅찬 마음을 가지고 MBR 분석을 기대한 독자에게 미안하지만 아직 우린 알아야 할 것이 조금은 남았다! 바로 부트 프로세스 (Boot Process), 즉 우리의 컴퓨터가 어떠한 방식을 통해서 지금 사용중인 운영체제를 화면에 띄우는 것인가에 대해서 알 필요가 있다. 이건 또 무슨 상관이냐 하는 독자도 있을 수 있지만 윈도우에 대해서 조금이라도 공부를 해봤거나 MBR과 관련된 오류를 경험해본 독자는 알 것이다. 핵심만 말하겠다. MBR은 부팅과정에서 등장하며 필수적이다! (MBR 디스크 한정)

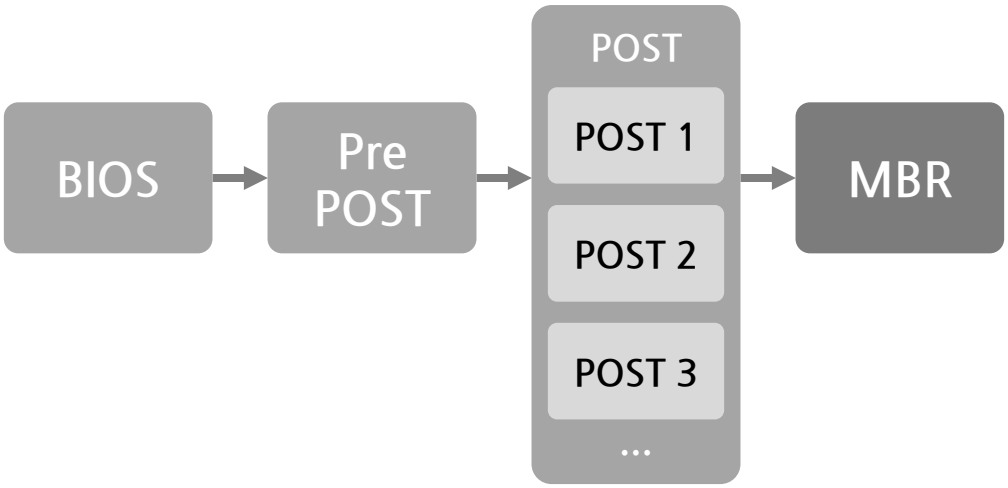

그림 2-1 MBR까지의 공통적인 부팅 과정

그림 2-1은 컴퓨터의 MBR까지의 공통적인 부팅과정이다. 사실은 이 뒤에도 운영체제 별로 무궁무진하게 다양한 부팅 절차가 존재하지만, 우리의 목표는 MBR 분석이기 때문에 MBR까지의 부팅과정만을 간단하게 살펴 볼 것이며 새로운 지식에 대하여 크게 부담을 가지지 않아도 된다! (필자는 새로운 것을 배우는 일을 좋아한다, 독자들도 그렇게 되도록 노력해보자.)

✓ **롬 바이오스 (ROM BIOS) 부트 프로그램 로드** : 전원 버튼을 누른 뒤 일련의 과정을 거쳐 CPU가 메인보드의 ROM BIOS를 메모리에 로드 한 뒤, ROM BIOS를 실행한다. 그림 2-3이 아마 독자들이 많이 봐왔던 화면으로 무엇을 의미하는지 이해가 더 쉽게 될 것이다.

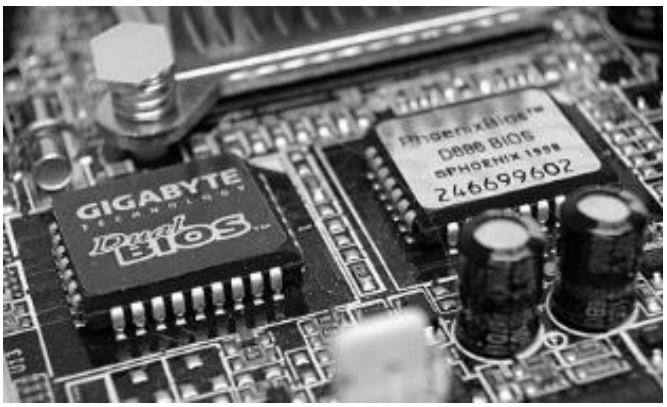

그림 2-2 메인보드의 ROM BIOS

그림 2-3 출력되기 시작하는 BIOS

BIOS & CMOS

CMOS와 BIOS 둘은 상당히 비슷해 보인다. 컴퓨터를 부팅하면서 접근 할 수 있는 설정 중 하나 이기도 하며 블루 스크린을 제외하고 보통 쉽게 접할 수 있는 검거나 파란 화면에 흰 글 씨들이 가득한 화면은 CMOS나 BIOS 뿐이기 때문이다. 공부를 하는 입장으로써 이 둘의 차이를 알아두자. (필자도 혼동하는 용어 중 하나다.)

CMOS는 Complementary Metal-Oxide Semiconductor의 약자로 상보성 금속 산화 막 반도체라는 (…) 듣기만해도 어려워지는 **하나의 기술**이다! 컴퓨터에는 RTC/NVRAM이라는 CMOS 칩이 존재하는데 이 칩이 바로 CMOS 방식으로 만들어져 그렇게 불리게 되었다. 이 RTC(Real-Time Clock)은 시스템의 날짜와 시간을 저장하며 NVRAM(Non-Volatile RAM)은 메모리 크기, 드라이브 타입, 부팅 순서 및 구성 정보의 CMOS Data를 저장하고 있으며 이 둘은 중요한 내용이 저장되어 있는 만큼 시스템이 꺼진 경우에도 내용이 보존이 된다!

BIOS는 Basic Input Output System의 약자로 운영체제와 하드웨어 사이의 입출력을 담당하기 위한 **펌웨어**를 의미한다, 운영체제가 하드웨어와 통신하기 위해서는 BIOS와 같은 중간 매개체와 통신해야 한다. 하드웨어 안에 포함 되어 있어 전원이 없는 상태에서도 유지하기 위해 ROM을 사용, ROM BIOS라고 칭한다.

둘은 엄연히 다르지만 CMOS와 BIOS가 혼동되는 이유는 부팅 설정을 위한 내용들은 CMOS(RTC/VRAM)에 저장되어 있는 반면에 설정이 가능하도록 화면을 출력하는 유틸리티는 ROM BIOS에 존재한다. 그래서 보통 부팅 설정을 하게 되면 BIOS의 설정 유틸리티가 CMOS의 내용을 읽어와 화면에 출력하게 된다.

그림 2-4 BIOS Setup

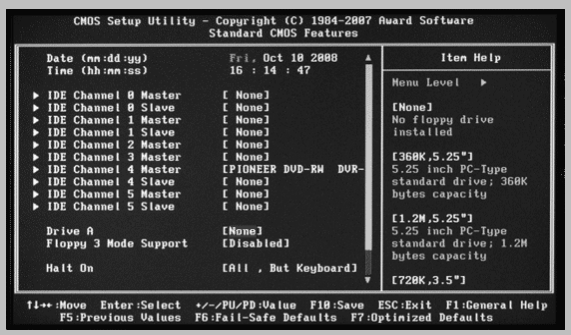

그림 2-5 CMOS Setup

ROM BIOS를 실행시킨 우리의 컴퓨터는 이제 컴퓨터에 큰 문제가 없는지, 하드웨어가 잘 연결되어 있는지의 약간의 "자가진단"을 시작한다. 이러한 과정을 "POST (Power On Self-Test)"라고 하며 이 POST 과정을 시작하기 전에도 약간의 진단을 한다. 그것이 바로 "Pre-POST"라고 한다.

✓ **Pre - POST** : ROM BIOS 내부의 부트 프로그램을 실행하며, POST 작업 수행을 위한 여러 가지 기본 테스트를 거친다. 테스트 결과가 ROM BIOS에 저장된 올바른 값과 일치한다면 다음 단계인 POST 작업을 수행한다.

✓ **POST (Power On Self-Test)** : 앞서 POST는 대략8~9개의 단계로 나뉘어진다. 각 단계 마다 무엇을 점검하는지 살펴보도록 하자.

● **POST 1단계 (시스템 버스 테스트)**

시스템 버스에 특정한 신호를 보내어 이상 유무를 확인한다.

- 시스템 버스 : CPU및 여러 장치들을 상호 연결해주는 중심 통로

● **POST 2단계 (RTC/VRAM 테스트)**

전에 언급한 RTC/VRAM이 정상 작동되는지 확인한다. (14쪽 참조)

● **POST 3단계 (비디오 구성 요소 테스트)**

화면 출력에 필요한 여러 요소들의 작동을 확인한다. 이 과정부터는 우리가 눈으로 직접 부팅 과정을 볼 수 있게 된다.

그림 2-6 확인 가능한 부팅 과정

● **POST 4단계 (RAM 테스트)**

RAM이 정상적으로 작동하는지 테스트한다.

● **POST 5단계 (키보드 연결 테스트)**

키보드가 정상적으로 연결이 되었는지 테스트한다.

● **POST 6단계 (드라이브 테스트)**

시스템에 연결된 모든 드라이브 테스트

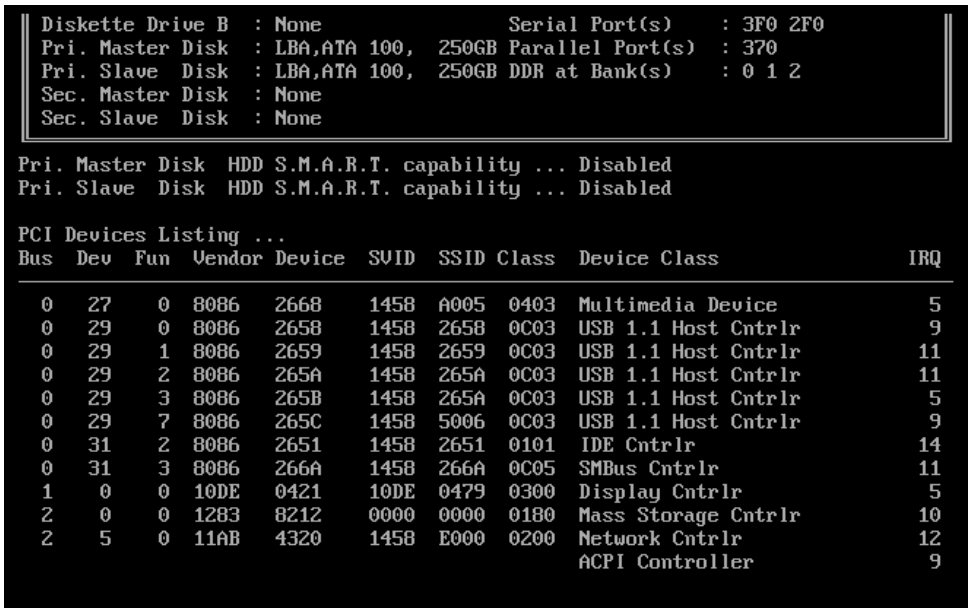

그림 2-7 연결 드라이브 확인

● **POST 7단계 (값 일치 검사)**

POST 결과가 RTC/NVRAM에 저장된 값과 일치하는지 확인

● **POST 8단계 (추가 바이오스 로드)**

추가적인 BIOS가 있다면 불러온다.

이러한 과정이 모두 끝났다면 이제 대망의 MBR에 접근할 준비는 모두 끝난 것이다. MBR을 공부하기 위한 기초지식이기에는 조금 방대했을 수도 있거나 시시했을 수도 있지만, 늘 말하지만 항상 기초가 튼튼해야 한다. 그래야지만 후에 좀 더 심화된 공부를 하게 되어도 이해하기 어렵지 않고 지칠 가능성이 낮아지기 때문이다.

2.2 Hello MBR!

우리는 지금까지 우리의 하드디스크가 어떻게 이루어져있는지, 디스크가 어떤 체계로 우리의 데이터를 관리하고 있는지, MBR까지 도달하는 부팅 과정 등 여러 기본지식에 대해 공부 했다. 그럼 아래의 그림을 한 번 보자. 앞의 내용에 대해서 충분히 숙지했다면 익숙하기도 어렵지 않은 그림일 것이다.

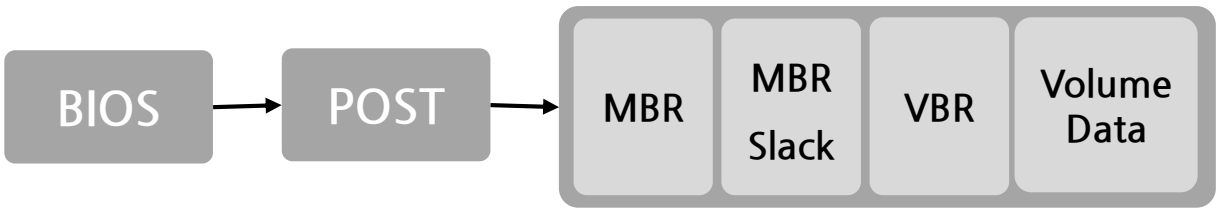

그림 2-8 부팅과정과 디스크의 추상적 구조

POST 단계를 통하여 나의 컴퓨터가 온전하게 작동할 준비가 되었다는 걸 확인한 뒤 컴퓨터는 디스크의 MBR을 불러오게 된다. 그럼 MBR이 무엇인지 지금부터 정확히 알아보자.

- ✓ **MBR(Master Boot Record)** : 저장장치의 첫 번째 섹터에 존재하는 MBR은 파티션 테이블에서 부팅 가능한 파티션을 검색해준다. 부팅 가능한 디스크가 있을 경우에는 VBR로 뛰어넘게 되고, 없을 경우에는 오류 메시지를 출력하게 된다. 우리가 분석하게 될 이 MBR은 부팅 코드와 파티션 테이블로 나뉘어 이를 분석함으로써 여러 정보를 습득할 수 있다. 최근에는 이 MBR의 단점을 보완한 GPT, UEFI 방식을 사용하여 부팅한다.
- ✓ **MBR Slack** : MBR과 VBR 사이에 존재하는 낭비되는 공간이다. 보통 악성코드에게 악용되거나, 보안 솔루션으로 선용 되는 경우로 나뉜다. 운영체제마다 차지하는 섹터 수가 조금씩 다르니 참고하자.
- ✓ **VBR(Volume Boot Record)** : 볼륨의 시작 위치에 존재하며 볼륨의 클러스터 크기만큼 할당되어있다. 볼륨의 부트로더를 로딩함으로써 운영체제를 부팅시키는 역할을 한다.

MBR은 저장장치의 첫 번째 섹터(0번) 에 위치하는 512 Byte 크기의 영역으로 크게 2부분으로 분류된다 (시그니처 제외) 아래의 그림을 참조하자.

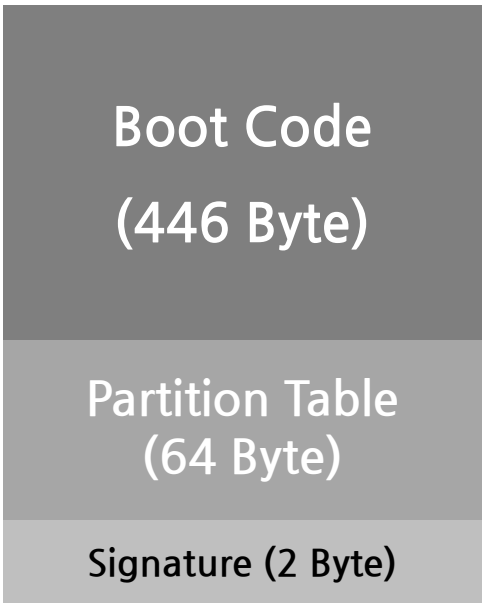

그림 2-9 MBR 구조

조금 있으면 분석하게 될 MBR의 기본적인 구조다. 사실 이렇게만 봐서는 감이 잘 안 오겠지만 여러 도구들을 사용해서 MBR을 한 번 보게 된다면 어떻게 나누어서 봐야 할지 감이 조금씩 잡힐 것이다. 익숙해지면 눈에 보이겠지만 아래의 표와 후에 설명할 여러 세부적인 구조를 학습함으로써 조금 더 상세히 MBR을 볼 수 있다.

범위		정보	크기
DEC	HEX		
0 - 445	0x0000	부트 코드	446 Bytes
446 - 461	0x01BE	파티션 테이블 엔트리 #1	16 Bytes
462 - 477	0x01CE	…	16 Bytes
478 - 493	0x01DE	…	16 Bytes
494 - 509	0x01EE	파티션 테이블 엔트리 #4	16 Bytes
510 - 511	0x01FE	시그니처 (0x55AA)	2 Bytes

그림 2-10 MBR 데이터 구조