1. MBR 분석 기초 지식

Windows MBR을 분석하기에 앞서 여러 기본적인 용어나 지식을 쌓아둘 필요가 있다. 우리가 분석하게 될 MBR이 존재하는 저장 장치의 구조, MBR을 분석함으로써 얻는 정보가 무엇인지, 우리의 컴퓨터는 어떤 과정을 통해서 MBR을 불러오게 되는지 등 분석에 앞서 필요한 기본 지식을 이번 장에서 설명하고자 한다. 용어가 생소할 수도 있으나 컴퓨터에 관심이 있다면 대부분 한 번쯤은 들어 봤을 법한 내용들이니 부담은 갖지 말도록 하자.

1.1 하드 디스크 드라이브(HDD) 구조

MBR을 분석하는데 하드 디스크의 구조를 왜 알아야 할까? 반드시 필요한 개념이 아닐 수도 있지만 필자의 생각으로는 이러하다, 앞으로 디지털 포렌식을 공부하는데 있어 수 많은 저장장치를 접하게 될 것이고, 우리가 분석할 MBR 또한 하드 디스크와 같은 저장장치에 상주해 있으며 구조에 대해 공부하면서 앞으로 자주 사용하게 될 용어나 지식에 대해서 간단한 선행을 할 수 있기 때문에 하드 디스크의 구조 정도는 공부할 필요가 있다고 생각한다.

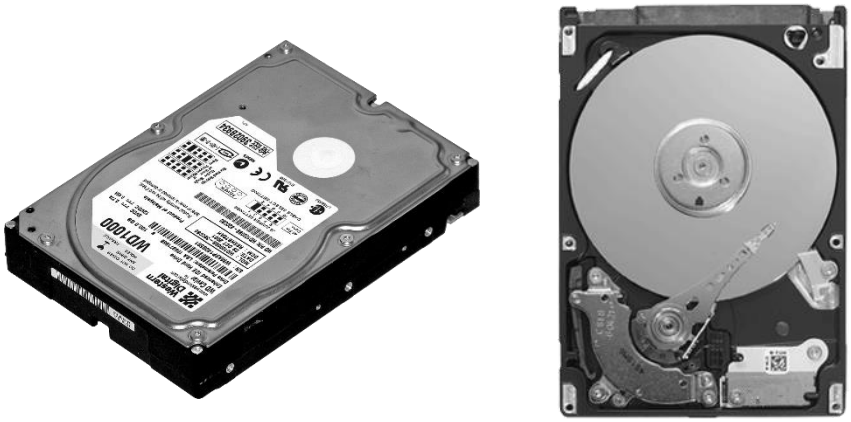

그림 1-1 HDD 외관 및 내부

위의 그림이 우리가 기본적으로 알고 있거나, 컴퓨터 안에 내장되어있는 HDD의 모습이다. 우리의 목표가 HDD의 구조에 대한 공부인 만큼 HDD를 좀 더 자세히 들여다 보도록 하자.

그림 1-2 HDD 내부 구조

위의 그림은 HDD의 커버를 제거하면 볼 수 있는 내부의 모습이다. 내부에 중요한 여러 요소들이 존재하지만 대표적으로 4가지 정도만 알아보자.

- ✓ **플래터 (Platter)** : 알루미늄 원판 표면에 자성체 산화금속 막을 양면 코팅한 부분으로, 우리의 데이터는 이 플래터에 저장되어 있다고 보면 된다. 추후 설명할 헤드(Head)를 이용하여 산화금속 막을 나누고(Partitioning) 위치를 지정(Formatting)하는 방식으로 사용된다. 또한 하드 디스크(Hard Disk)는 이 플래터를 구성하는 산화금속의 단단함(Hard)에서 유래 되었다.
- ✓ **스핀들 모터 (Spindle Motor)** : 플래터를 일정한 속도로 회전시키는 장치로 모델에 따라서 회전하는 속도(RPM) 가 차이가 난다. 일반적으로 회전하는 속도가 높을 수록 더 빠르게 데이터를 찾아서 전송할 수 있다. 그러나 회전 속도가 높을 수록 발열이나 소음이 심해지는 단점이 존재한다.

✓ **헤더 (Head)** : 플래터 표면에 코팅된 자성체를 자성화/소거하여 정보를 저장 및 삭제하거나 읽는 역할을 한다. 헤드의 수는 보통 플래터의 두 배로 플래터와 미세한 간격을 유지한 채로 읽기/쓰기를 시행한다. 오래된 하드 디스크의 경우에는 헤드가 플래터나 긁거나 열로 인해 붙게 된다.

✓ **헤드 구동 장치 (Actuator Arm)** : 헤드를 움직이는 장치로써 컨트롤러로부터 제어 신호를 받아 헤드가 부착된 암을 원하는 위치로 이동시켜준다. 기본적으로 헤드의 수가 많을 수록 헤드 구동 장치의 수도 늘어난다.

이제 하드 디스크가 어떠한 구조를 가지고 있는지 간단하게 나마 이해가 되었을 것이다. 그러나 우리의 데이터들을 플래터란 금속 덩어리에 단순히 기록하기보다는 효율적으로 저장하고 관리하기 위해서는 어떤 체계 필요하다. 그래서 효율적인 데이터 관리를 위해 디스크를 논리적으로 구분해놓게 된다. 그 구조는 아래와 같다.

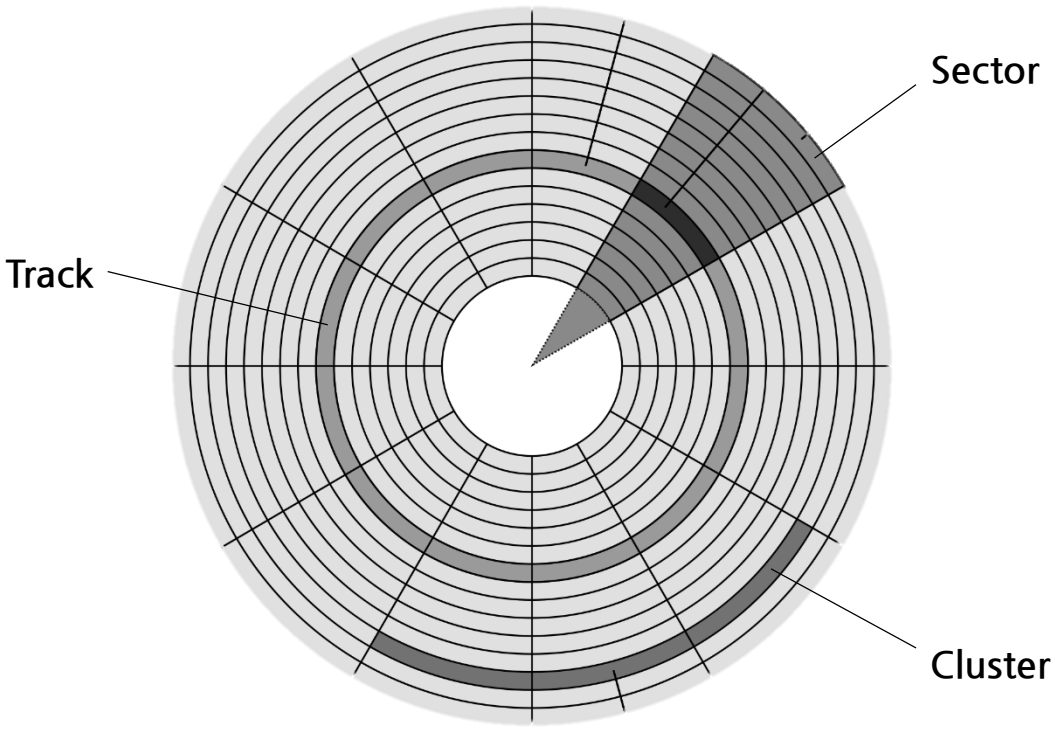

그림 1-3 HDD 논리적 구조

✓ **트랙 (Track)** : 디스크 상에 데이터를 기록할 수 있는 고리 모양의 영역으로 각 트랙은 여러 개의 섹터로 나뉘어진다. 보통 운영체제와 디스크 드라이브는 트랙과 섹터 번호를 통해 데이터의 저장 위치를 파악한다.

✓ **섹터 (Sector)** : 디스크에서 사용하는 최소의 저장단위 이다. 섹터 하나 당 크기는 512 Byte를 가졌지만, 최근에는 크기를 변경이 가능하다. 0번 섹터에는 파일 할당표(FAT)이라는 특수한 파일이 저장되어 있다.

그림 1-4 디스크 포맷을 통한 섹터 크기 변경

✓ **클러스터 (Cluster)** : 16 Bit 시스템의 한계로 등장한 개념으로, 섹터 여러 개를 하나로 묶은 뒤 운영체제의 최소 단위로 사용한다. 파일을 읽고 찾는 속도는 빨라졌지만 섹터와 클러스터의 차이로 사용되지 않고 버려지는 용량이 존재하게 된다.

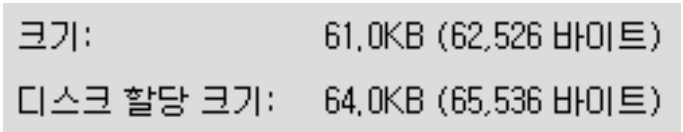

그림 1-5 파일 속성을 통한 실제 크기 확인

1.2 디스크 관련 용어

앞서 하드 디스크가 가지고 있는 구조, 데이터를 기록하는 방식 등에 관해서 간략하게나마 알아 보았다. 그렇다면 이제 우리가 사용하는 시스템에서 사용되는 디스크와 관련된 용어들을 알아보도록 하자. 그러나 들어가기 전 하나만 짚고 넘어가보자. 다음과 같은 질문에 대답해보자. "CD나 DVD는 디스크인가?" 대부분은 "네" 라고 대답하겠지만 사실은 질문이 조금 잘못되었다. 질문이 틀린 이유에 대해서는 아래를 참조하자.

동명이인의 디스크

위의 질문이 모호한 이유는 HDD와 CD/DVD 둘 다 디스크라고 부르기 때문이며, 질문자가 요구하는 디스크를 정확히 알 수 없기 때문이다. 자세한 설명은 아래를 보자.

디스크 (Disk, Magnetic Disk) : 앞서 설명한 하드 디스크와 같이 표면에 자력을 이용하여 데이터를 기록하고 자기장의 변화를 통해 데이터를 읽는 방식의 자기 기록 매체를 의미한다. 대표적인 플로피 디스크 드라이브, 하드 디스크 드라이브 (HDD) 등이 있다.

디스크 (Disc, Optical Disc) : 하드 디스크와는 다른 광 디스크로 둥근 원반에 얇은 반사체를 입힌 후 레이저를 이용하여 홈을 파서 데이터를 기록하고 레이저 반사의 변화를 통해 데이터를 읽는 방식의 광학 기록 매체를 의미한다. 대표적으로 흔히 볼 수 있는 CD, DVD, Blue - Ray 등이 있다.

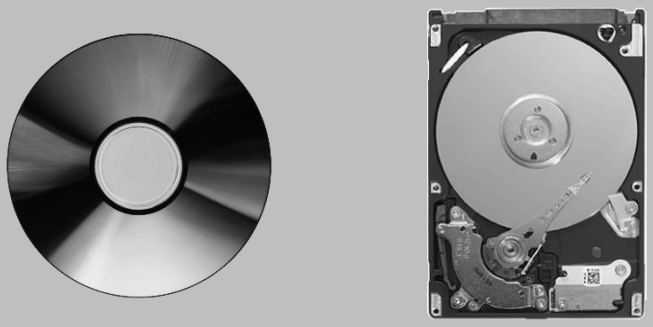

그림 1-6 광 디스크와 하드 디스크

이제 우리가 어떤 디스크를 공부하는지 알 수 있을 것이다. 우린 디스크(Disc)가 아닌 디스크(Disk)에 대해 공부하는 것이다! 이런 이상한 점을 지닌 디스크를 윈도우에서는 대략 세가지 종류로 나누어서 구분한다.

- ✓ **고정 디스크 (Fixed Disk)** : 시스템에 장착되어 이동할 수 없는 형식의 디스크를 일컫는 말로 메인보드와 연결되어 있는 HDD나 유사한 방식의 드라이브 (SSD 등), RAM에 생성된 램 디스크, 가상 디스크가 이에 속한다.
- ✓ **이동식 디스크 (Removable Disk)** : 흔히 잘아는 시스템에서 탈,부착 가능하여 이동 가능한 USB 저장장치나 외장 하드 디스크가 이에 속한다.
- ✓ **가상 디스크 (Virtual Disk)** : 윈도우 7부터 지원되는 디스크 형식으로 가상 하드 디스크(VHD, Virtual Hard Disk)이다. 다른 저장 매체에 파일의 형태로 존재하며 언제든지 시스템에 연결 및 분리가 가능하다.

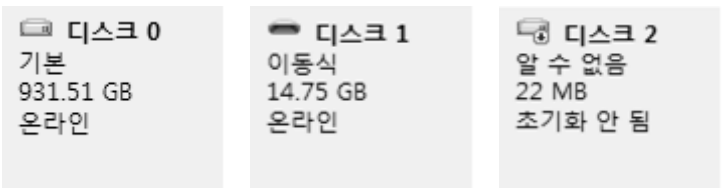

그림 1-7 디스크 관리에서의 표현 방식

사실 일반적으로 디스크 관리를 통해 접할 수 있는 디스크는 고정 디스크와 이동식 디스크일 것이다. 가상 디스크는 특별한 경우가 아니면 사용할 일이 잘 없기 때문이다. 그러나 가상 디스크의 존재나 어떤 용도를 가지는지 정도는 알아 두도록 하자.

다음은 "파티션"에 대한 내용이다. 사실 파티션이라는 용어는 대부분 컴퓨터 포맷을 할 때 한 번 쯤은 들어 봤을 법한데 대부분은 어떤 역할을 하며 어떻게 설정을 해주어야 할지 잘 모르는 경우가 많은데 MBR 분석을 함으로써 이 파티션에 대한 정보도 얻을 수 있으니 지금까지 몰랐더라도 알아가면 된다!

파티션이란 “디스크 공간을 논리적으로 별개의 데이터 영역으로 분할한 공간”을 지칭한다. 간단하게 파티션을 통해 하나의 디스크를 여러 부분으로 분리시켜 여러 개의 디스크 처럼 쓸 수 있는 것이다. 예를 들어 아래처럼 우리가 흔히 사용하는 C: 드라이브와 D:드라이브 형식으로 파티션을 나눌 수 있다.

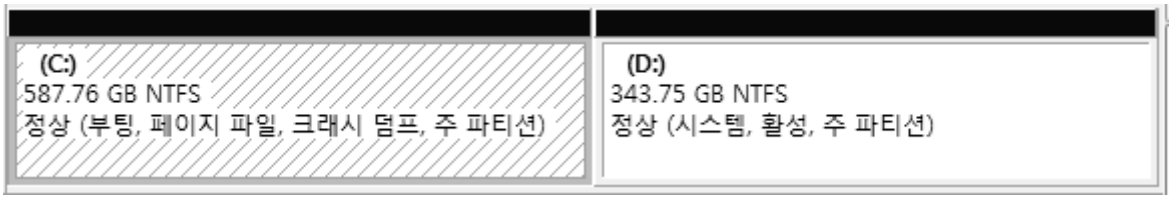

그림 1-8 파티션 분할의 예시

파티션을 생성하는 것은 데이터를 기록하기 위한 필수적인 과정이다. 그러나 디스크에서 파티션을 생성 하지 않은 공간을 “할당되지 않은 빈 공간”이라 칭하고 이 빈 공간은 포맷과 데이터 기록이 불가한, 준비되지 않은 공간이라고 생각하면 된다. 이러한 파티션도 디스크와 마찬가지로 3가지 종류가 있다. (MBR과 GPT의 경우에 따라 파티션의 종류도 달라지지만, 이번 문서에서는 MBR 디스크 중점으로 설명을 한다고 이해하자)

- ✓ **주 파티션 (Primary Partition)** : 기본 디스크에서 만들 수 있는 파티션으로 주 파티션은 분리된 디스크처럼 작동하며 운영체제(Operation System)를 설치하여 부팅하거나 데이터를 저장할 수 있다. MBR 디스크의 경우 최대 4개까지 지정이 가능하다.
- ✓ **확장 파티션 (Extended Partition)** : 기존의 파티션 제한(4개) 을 극복하기 위해 개발된 특별한 유형의 주 파티션으로 확장 파티션은 내부에 논리적 파티션을 생성할 수 있다. 이 확장 파티션은 데이터를 포함할 수 없고 드라이브 문자가 할당되지 않지만 확장 파티션 내부의 논리적 파티션은 응용 프로그램과 데이터를 포함할 수 있다.

✓ **논리 드라이브(Logical Drive)** : 위의 확장 파티션에서 언급되었듯이 기본 디스크의 확장 파티션 내에서 만들 수 있는 파티션의 한 종류이다. 논리 드라이브에 운영체제를 설치할 수는 있지만 논리 드라이브 자체로는 부팅할 수 없으나 데이터 저장이 가능하고 주 파티션과는 달리 최대로 생성할 수 있는 논리 드라이브의 개수에는 제한이 없다는 점이 장점이다.

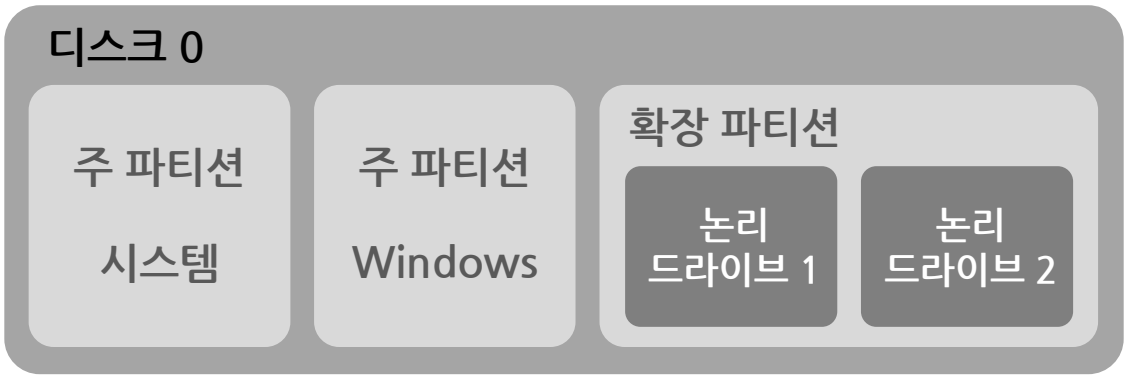

그림 1-9 디스크 파티션 구조 예시

사실 논리 드라이브나 확장 파티션에 대해서는 이해가 어려울 수도 있다. 쉽게 생각해보자! 확장 파티션은 논리 드라이브라는 물건들을 생성해 보관하는 컨테이너라고 생각하고 위의 그림을 보면 좀 더 이해하기가 쉬울 것이다. (이전에 언급한 내용대로 위 예시와 설명은 MBR 기준이며 GPT를 기준으로 할 시에는 다를 수 있다는 점을 유의하자!)

마지막으로 **드라이브(Drive)**라는 용어를 알아보자! 간단하다, **"드라이브 문자가 지정된 저장 영역"**을 말한다. 예를 들어 C:, D:, E:, … 말이다. 이 때 저장 영역은 디스크를 포함하여 CD-ROM 장치들, 플로피 디스크 모두를 포함한다. 즉 드라이브 문자를 지정할 수 있는 모든 장치 및 저장 공간들도 문자를 할당 받으면 드라이브가 되는 것 이다. 하나의 저장 영역은 반드시 하나의 드라이브 문자만을 할당 받을 수 있으며 하나의 드라이브 문자는 하나의 저장 공간에만 할당될 수 있게 된다. 어렵지 않은 개념이며 드라이브를 계속 언급하였지만 사실 그 정의를 정확히 모르는 경우가 많았지만 지금부터라도 숙지하면서 본격적으로 MBR이 어떤 것인지 파악해보자.