SeoulTech

제3장 디지털 기기와 저장 매체

박 종 혁 교수

UCS Lab

Tel: 970-6702

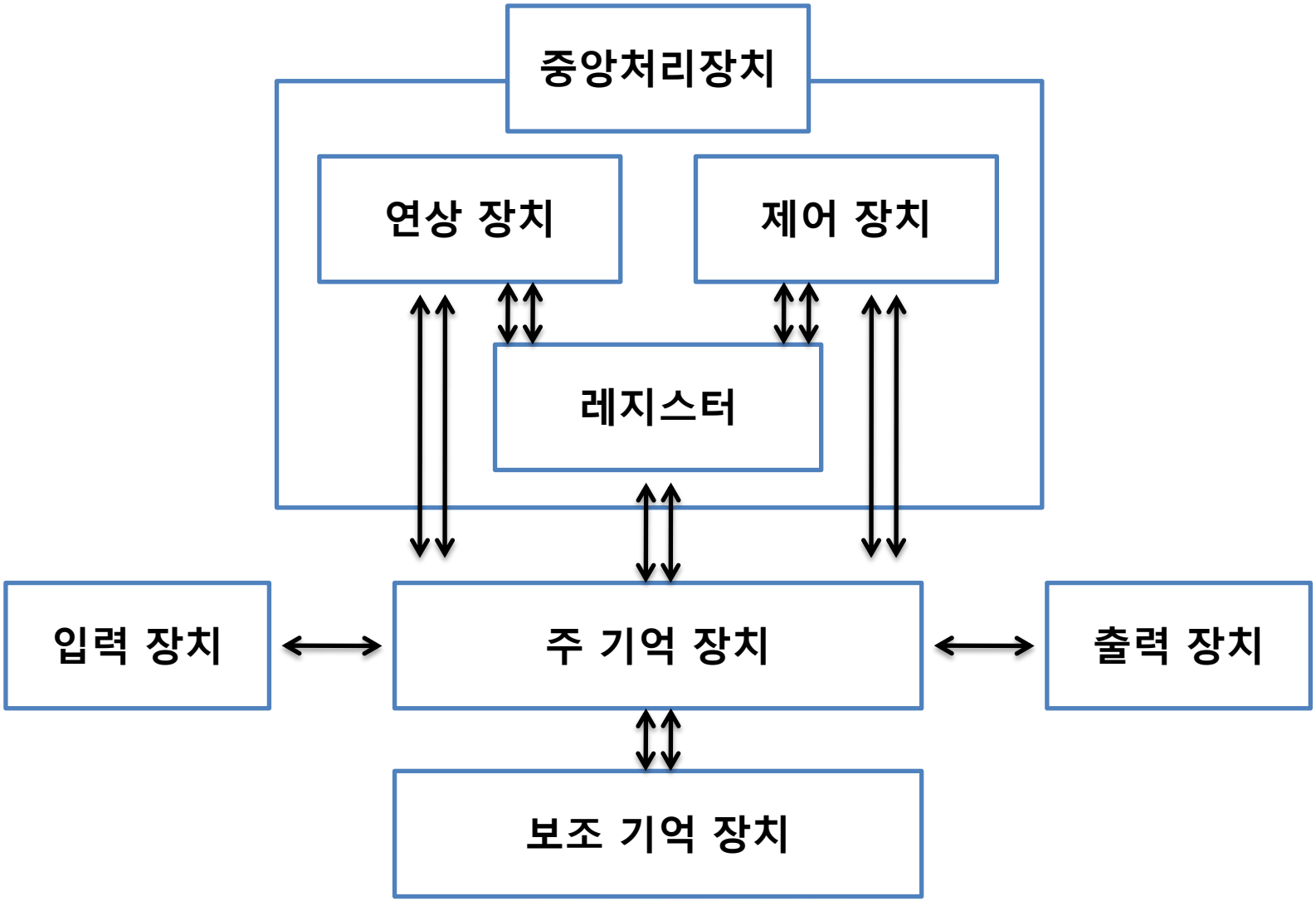
Email: jhpark1@seoultech.ac.kr

- **학습 목표**
  - 디지털 증거를 획득하기 위한 물리적 대상이 되는 것은 컴퓨터의 하드 디스크와 같이 다양한 저장 매체임
  - 따라서 디지털 증거를 수집하기 위해서는 먼저 현장에서 디지털 저장 매체를 확보해야 하며, 이를 위해서는 저장 매체의 종류와 기능을 충분히 이해하고 데이터 수집 방법을 사전에 습득해야 함

- **배울 내용**
  - 주요 컴퓨터 하드웨어의 이해
  - 휴대용 디지털 저장 매체의 종류와 특징
  - 디지털 기기의 종류와 특성 파악

목 차

2. 디지털 기기의 구성 요소



3. 디지털 저장 매체의 종류 및 특성

- **컴퓨터에서 주로 사용하는 저장 매체의 종류**
  - 플로피 디스크
  - 하드 디스크
  - 플래시메모리 기반 저장 매체
  - 광학 매체: CD-ROM, DVD-ROM 등이 존재

- **디지털 포렌식 관점에서 저장 매체**
  - 범죄 현장의 조사자는 수사 대상 컴퓨터와 여러 주변 장치 등을 파악하고 이를 확보할 수 있도록 배경 지식을 갖추어야 함
  - 대부분의 저장 매체는 메인보드에 직접 연결되어 사용되거나 USB 등과 같은 외부 연결 인터페이스를 사용하여 시스템에 연결
  - CD, DVD, 플래쉬 메모리 등과 같은 저장매체의 발달로 인해 현재 플로피 디스크 형태의 매체는 거의 사용되지 않고 있지만, 이러한 저장 매체들을 확인하고 조사해야 함

3. 디지털 저장 매체의 종류 및 특성

분류 기준		저장 매체 종류
용도	주 기억 장치	RAM, ROM
	보조 기억 장치	자기 디스크, 광학 디스크 등
물리적 저장 방식	자기	자기 테이프, 플로피 디스크, 하드 디스크, 집 드라이브, 재즈 드라이브 등
	광학	CD(Compact Disc), DVD(Digital Versatile Disc), BDA(Blu-Ray Disk)
	반도체	RAM, ROM, 플래시 메모리
전원 공급에 따른 데이터 유지 여부	휘발성	RAM, RAM 기반의 SSD(Solid State Disk)
	비휘발성	ROM, 보조 기억 장치
접근 방식	순차 접근	자기 테이프
	직접 접근	디스크, 플래시 메모리 등

반도체를 이용한 저장 매체

- ROM (Read-Only Memory)
  - ROM은 읽기만 가능한 기억장치로 전원이 공급되지 않아도 내용이 사라지지 않는 비휘발성 메모리
  - ROM은 컴퓨터를 시작할 때 필요한 설정 및 프로그램을 저장하고 있는 ROM BIOS 형태로 많이 사용
  - 초기 ROM은 제조 회사에서 미리 데이터를 기록하면 읽기만 가능했지만, 현재는 사용자가 직접 데이터를 기록하는 ROM(PROM)이나 여러 번 데이터를 재 기록할 수 있는 ROM(EPROM, EEPROM) 등이 사용되고 있음

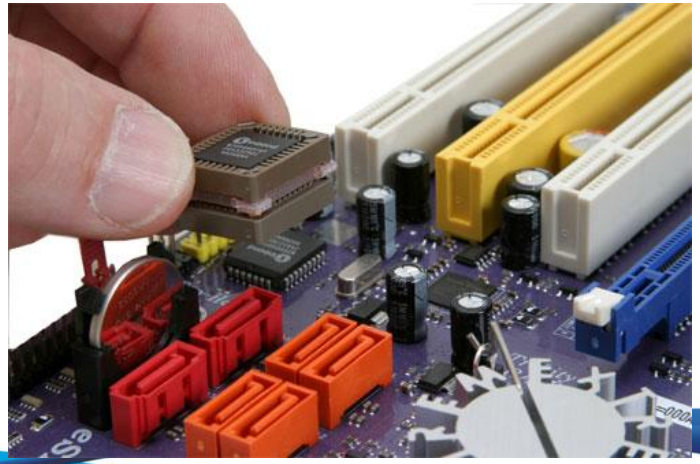
ROM 의 종류

ROM 종류	설명
Mask ROM	제조 회사에서 미리 데이터를 기록한 ROM으로 변경할 수 없음
PROM	제조된 후 사용자가 한번만 데이터를 기록할 수 있음
EPROM	자외선을 이용하여 기록된 내용을 지우고 다시 기록할 수 있음
EEPROM	전기적인 방법으로 기록된 내용을 지우고 다시 기록할 수 있음

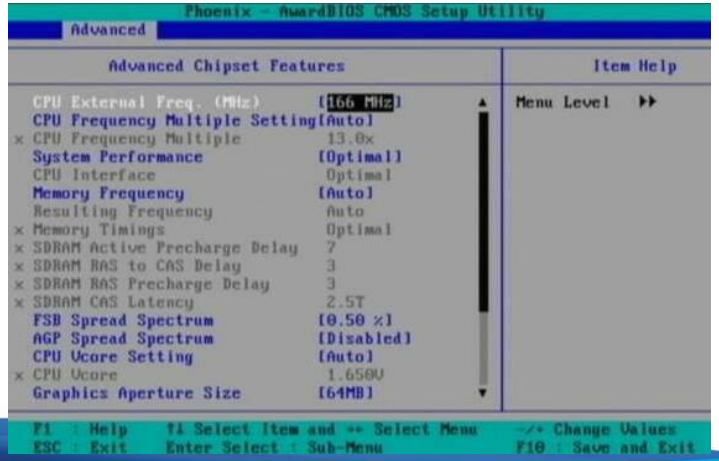
BIOS (Basic Input Output System)

- **BIOS는 운영체제와 하드웨어 사이의 입출력을 담당하는 저수준의 소프트웨어와 드라이버로 구성된 펌웨어**
  - 운영체제는 하드웨어와 통신하기 위해 중간매개체를 사용하게 되며, 이러한 역할을 하는 것이 BIOS
  - 전원이 공급되지 않아도 유지되어야 하는 정보이기 때문에 ROM으로 제작되어 하드웨어가 제조될 때 제조회사에 의해 하드웨어에 포함됨
- **ROM BIOS**
  - 흔히 컴퓨터 메인보드의 BIOS를 ROM BIOS라고 부르며, 메인보드 이외에도 SCSI, 그래픽 카드 등에 사용

메인보드의 ROM BIOS 칩셋

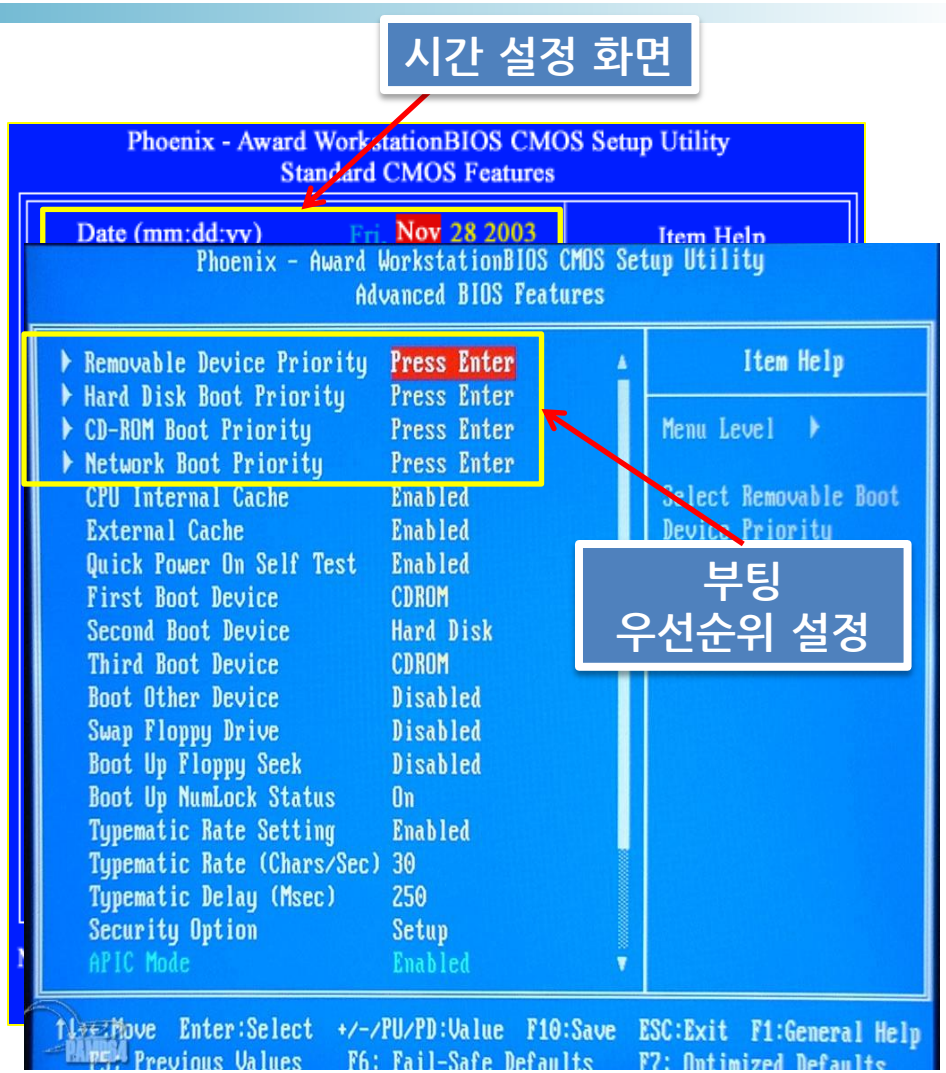


메인보드의 ROM BIOS 화면

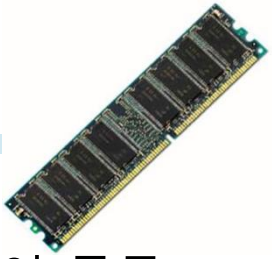


BIOS (Basic Input Output System)

- **포렌식 관점에서 ROM BIOS의 중요성**
  - ROM BIOS에 저장된 시스템의 시간은 현장에서 확보한 시스템의 시간이 정확한지, 의도적으로 변경되지 않았는지 등을 확인할 수 있는 기준이 되므로 중요함
  - 또한 하드 디스크의 구성, 종류, 용량을 확인할 수 있음
  - 시스템의 부팅 순서를 설정할 수 있으므로 데이터 수집 시 유의하여 설정해야 함
- **BIOS 셋업 모드 진입 방법**
  - 바이오스 제조사 마다 조금씩 다르지만, "DEL","F1", "F2" 를 사용
  - 일반적으로 부팅 첫 화면에서 바이오스 진입 키를 명시함



RAM (Random Access Memory)



- **RAM 이란?**
  - RAM은 자유롭게 데이터를 읽고, 쓸 수 있는 기억장치로 전원이 공급되지 않으면 기억하고 있는 데이터가 사라지므로 휘발성 메모리로도 불림
  - Random Access 라는 의미는 특정 데이터를 읽기 위해 기억장치의 처음부터 순차적으로 접근하지 않고 어떤 위치라도 곧바로 접근할 수 있다는 의미

- **RAM의 특징**
  - RAM은 ROM과 다르게 휘발성(Volatility)이라는 특징을 가짐
  - 즉 컴퓨터 전원이 공급되지 않으면 해당 데이터가 사라지지만 그렇지 않다면 계속적으로 현재 컴퓨터의 상태를 유지

- **디지털 포렌식 분야에서 RAM**
  - 수사 대상 컴퓨터에 전원이 공급되어 있다면 해당 컴퓨터의 상태를 가장 잘 알 수 있으므로 학계에서는 RAM에 있는 데이터를 수집/분석하기 위한 다양한 방법을 연구하고 있음

USB (Universal Serial Bus)

- **USB**
  - 컴퓨터와 주변기기를 연결, 통신하기 위한 표준 인터페이스로 다양한 직렬, 병렬 통신을 대체하기 위해 개발
  - 최근에는 컴퓨터를 비롯한 PDA, 임베디드 장비와 같이 다양한 디지털 기기의 주변 장치와 통신하기 위한 표준 인터페이스 역할을 하고 있음
  - 1.0, 1.1, 2.0과 같이 다양한 버전이 있으며 현재 2.0이 보편적으로 사용, 현재 3.0 개발 중

- **USB 의 다양한 버전**
  - USB 1.0 경우 1.5Mbps(Mbit/sec) ~ 12Mbps의 속도
  - USB 2.0은 최대 480Mbps 속도
  - 개발 중인 USB 3.0의 경우에는 속도가 대폭 향상된 5Gbps의 속도를 가질 예정

USB 1.0 표준 로고

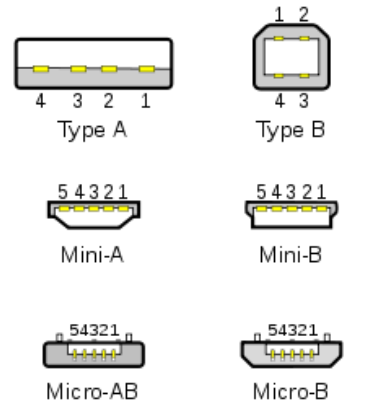
USB 2.0 표준 로고

USB 3.0 표준 로고

USB (Universal Serial Bus)

- **USB의 활용**
  - 현재 키보드, 마우스, 게임패드, 스캐너, 디지털카메라, 프린터, PDA, 저장장치 등 다양한 장치를 연결하는데 널리 사용
  - 하나의 USB 주 컨트롤러는 허브를 통해 127개 까지 확장하여 사용될 수 있고 핫 플러스 기능을 지원
  - 핫플러스 : 핫 스왑이라고도 불리며 컴퓨터의 전원이 연결된 상태에서 해당 장치의 연결/해제가 가능한 기능

다양한 USB 포트의 유형



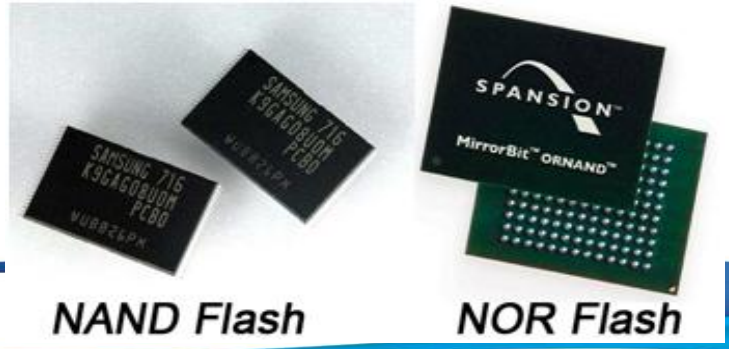
플래시 메모리 저장 매체 (Flash Memory Storage)

- **플래시 메모리**
  - 전기적으로 데이터를 지우고 재기록이 가능한 비휘발성 기억 장치
  - 전기적으로 고쳐 쓰기가 가능하다는 점에서는 ROM과 다르며, 데이터를 고쳐 쓰기 전에 소거 동작이 필요하고 데이터가 지워지지 않는다는 점에서 ROM과 RAM의 중간 성격을 띄는 메모리

- **플래시 메모리의 특성**
  - 플래시 메모리는 충격에 강하고 저 전력으로 동작이 가능하다는 장점 덕에 녹음기, MP3, 디지털 카메라, 휴대폰과 스캐너, USB 플래시 메모리로 널리 사용

플래시 메모리 종류(NAND 플래시와 NOR 플래시)

- **NOR 플래시**
  - 속도는 빠르지만 대용량으로 구성하기에는 부적합
  - MMC 카드나 Compact 플래시 메모리를 포함하여 휴대폰이나 셋탑박스 등에 주로 쓰임
- **NAND 플래시**
  - NOR 플래시에 비해 다소 속도는 느리지만 대용량으로 구성하기에 적합
  - NAND 플래시는 메모리카드 중 SD 카드나 메모리 스틱 등에서 사용되며 SSD나 디지털 카메라, MP3 등에 주로 사용
- **플래시 메모리의 저장방식**
  - SLC 방식 (Single Level Cell)은 각 셀이 1비트(0, 1)를 사용
  - MLC 방식 (Multi Level Cell)은 각 셀에 2비트(00, 01, 10, 11)를 사용하여 기억하는 방식이기 때문에 같은 크기의 셀을 사용한다고 했을 때 SLC 방식에 비해 MLC 방식이 더 많은 양의 데이터를 저장할 수 있음



NAND Flash NOR Flash

USB 메모리

- **USB 플래시 메모리**
  - 32MB부터 64GB까지 다양한 용량이 있으며, 크기가 작고 휴대가 편리하며 비교적 저렴하여 전 세계적으로 널리 쓰이고 있음
  - 크기가 작아 분실 시 정보 유출의 가능성이 존재함
  - 이러한 단점을 보완하기 위해 USB 메모리에 패스워드 입력과 같은 인증 과정을 더해 데이터를 보호하는 기술이 적용되고 있음
- **디지털 포렌식 관점에서 USB 메모리**
  - USB 메모리를 대상으로 데이터를 수집할 때에는 USB 메모리의 용량과 실제 디스크의 크기가 동일한 지를 확인하여 암호화 영역이나 숨겨진 영역이 존재하는지 점검해야 함




플래시 메모리 카드

- **다양한 플래시 메모리 카드**
  - 메모리 카드는 제조사 별로 CF, SD (Mini SD, Micro SD), SM, XD, Memory Stick, 등으로 구분되는 플래시 메모리 기기
  - 각 종류 별로 서로 다른 인터페이스를 이용하며, 일반적으로 디지털 기기의 저장 매체로서 사용

- **디지털 포렌식 관점에서 플래시 메모리**
  - 플래시 메모리는 그 특징상 크기가 매우 작기 때문에 휴대성이 좋아 범죄자가 증거물을 쉽게 은닉할 수 있음
  - 따라서 압수・수색 시 USB 메모리나 소형 메모리 카드를 숨길만한 장소까지 주의를 기울여 수색해야 하며, 수사 대상 시스템에서 메모리 카드 사용 흔적이 없는지 파악해야 함
  - 또한 하드 디스크와 같은 저장 매체와 마찬가지로 메모리 카드에 있는 데이터를 수집할 때에도 반드시 쓰기 방지 장치를 통해 데이터 무결성을 유지해야 함

플래시 메모리 카드

SD/MMC

-디지털카메라, PDA
PSP,전자사전,네비게이션 등

microSD/T-Flash

-핸드폰 메모리,네비게이션
닌텐도 DS 등

CF Card

-디지털카메라, 네비게이션,
PDA 등

XD-Picture Card

-디지털카메라

Memory Stick

-디지털카메라, PSP

SSD (Solid State Drive)

- **SSD 란?**
  - 플래쉬 메모리의 장점을 활용하여 하드 디스크 드라이브(HDD)와 동일한 형태로 개발된 대용량 플래시 메모리
  - HDD와 동일한 연결 인터페이스를 사용하지만, 자기장을 이용하는 HDD와 달리 NAND 플래시 반도체를 이용하여 정보를 저장
- **SSD의 특징**
  - 임의 접근을 하여 탐색시간 없이 고속으로 데이터를 입출력할 수 있으며, HDD에 비해 외부의 충격으로 데이터가 손상될 가능성이 적음
  - SSD는 NAND 플래시를 사용하기 때문에 읽기, 쓰기, 접근 시간이 기존 HDD에 비해 매우 빠르고 소비 전력, 소음, 발열이 낮음

플로피 디스크

- **플로피 디스크**
  - 자기 디스크 매체(Magnetic storage media)로 널리 알려진 것이 플로피 디스크로 흔히 디스켓이라 불림
  - 플로피(“floppy")라는 말은 디스켓 안에 들어가는 마그네틱 판이 딱딱하지 않고 쉽게 휘어지기 때문에 붙여진 말이며 이후 3.5인치 크기의 디스크 형태를 플로피 디스크로 일반화
  - 1987년 초기 8인치가 개발되었으며, 1.44 MB의 데이터를 저장할 수 있는 3.5인치 HD 가 널리 쓰였으며, 그 이후로 차세대 저장 매체가 꾸준히 개발되었으나 대체되지는 않았음

- **차세대 플로피 디스크 개발**
  - 대용량 휴대용 매체의 필요성이 급증하자 3.5인치 크기에 다양한 매체가 개발
  - 대표적인 것이 아이오메가의 Zip 디스크(Zip100, 100MB), 이메이션의 슈퍼디스크(LS-120, 120MB), 소니의 HIFD(150/250MB) 이 차세대 매체로 경쟁하였지만 가격, 대중화, 표준화 등에 실패
  - 특히 USB 메모리와 광학 매체의 등장으로 대부분 시장에서 사장됨

플로피 디스크 드라이브

ZIP 디스크
100MB

슈퍼디스크
120MB

플로피 디스크
1.44MB

Zip 디스크와 Jaz 디스크

- **Zip 디스크**
  - 플로피 디스크의 차세대 버전으로 아이오메가(Iomega)에서 1994년에 개발
  - 1990년대 중반부터 슈퍼 플로피 저장 매체로 가장 인기를 많이 받았으며, 100MB에서 시작하여 250MB, 750MB까지 용량 증대
  - 하지만 3.5인치 플로피 디스크를 대체하지는 못하였음

Imation Zip 드라이브

- **Jaz 디스크**
  - Zip 디스크의 차세대 기종으로 1GB, 2GB 버전으로 출시
  - Jaz 디스크는 하드 디스크 기술을 기반으로 하여 Zip 디스크에 비해 저장 용량이 훨씬 크고 속도도 빠르지만 높은 가격과 안정성 부족으로 인기를 끌지는 못함
  - Zip 디스크와는 달리 현재 단종된 상태

Imation Jaz 드라이브

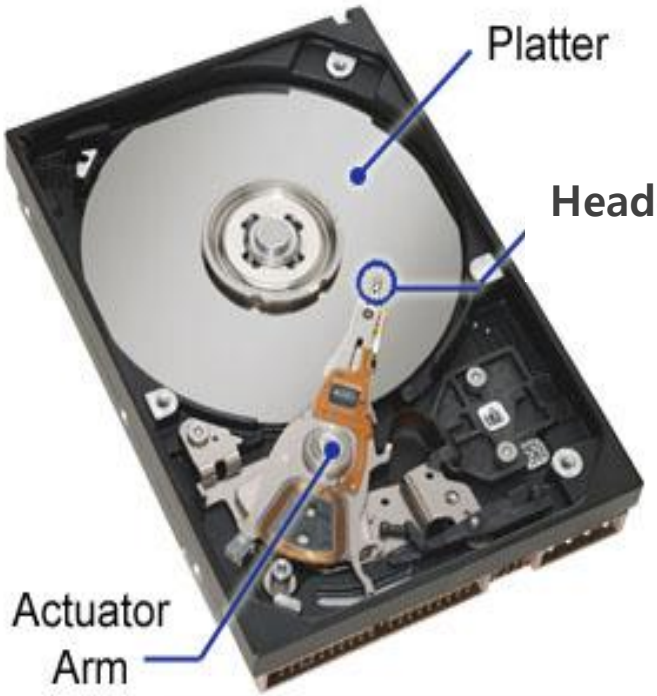
기타 플로피 형태의 저장 매체

- **광자기 디스크 (MO Disk: Magento Optical Disk)**
  - 3.5인치 크기의 광자기 저장 매체
  - 광자기 디스크의 경우 레이저를 이용해 데이터를 쓰고 지우므로 자성에 의해 데이터가 지워질 우려가 없어 보관성이 뛰어남
  - 여러 나라에 널리 보급되기 보다는 전문가를 위한 고가의 매체로 사용
  - 종류는 130 mm (5.25 인치) 와 90 mm (3.5 인치)로 나뉘며, 용량은 650 MB부터 9.2 GB까지 다양

- **미니 디스크 (Mini Disk)**
  - 1990년대 초반에 휴대용 음악 재생 미디어로 개발되어 2000년초까지 CD의 대체 미디어로 인기를 누린 음악 녹음 매체
  - 최근 소니는 2004년 1GB까지 데이터 저장이 가능한 디지털 기반의 Hi-MD를 내놓았지만, MP3 플레이어의 등장으로 최근 시장에서 거의 사라지고 있는 추세

하드 디스크 드라이브(Hard Disk Drive)

- **하드 디스크**
  - 현재 컴퓨터에서 가장 널리 쓰이며, 중요한 역할을 하는 비휘발성 저장장치
  - 하드 디스크의 동작원리
    - 하드 디스크는 자기장을 이용해 플래터(platter)라고 부르는 금속판 위에 데이터를 기록
    - 플래터가 회전하면 헤드(head)에 의해 데이터가 기록되며 플래터의 회전 속도는 현재 4,800 ~ 15,000 RPM을 유지
    - 플래터는 양면에 데이터를 모두 기록할 수 있으며, 하드디스크의 용량에 따라 양면을 모두 사용하거나 여러 장의 플래터를 사용



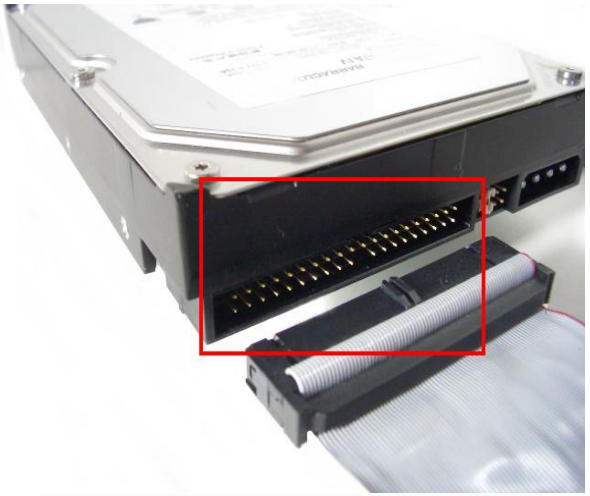
HDD의 내부 구성

- **하드디스크 인터페이스**
  - ATA(IDE), SATA, SCSI와 같이 다양한 인터페이스를 가지므로, 디지털 증거 획득을 위한 디스크 이미징은 다양한 인터페이스를 지원할 수 있어야 함

ATA (Advanced Technology Attachment)

- **ATA 인터페이스**
  - 하드디스크, CD-ROM 등 저장 장치의 표준 인터페이스
  - ATA는 흔히 IDE (Integrated Drive Electronics)라는 용어와 혼재되어 사용
  - ATA 방식은 ATA-1 표준부터 현재 ATA/ATAPI-8 까지 발전
  - 기존 병렬 전송 방식을 사용하는 Parallel ATA(PATA)에서 직렬 전송 방식을 사용하는 Serial ATA(SATA) 인터페이스로 발전

- **EIDE 인터페이스**
  - 기존의 컨트롤러가 두 개의 장치만 연결할 수 있는 점을 보완한 것으로 하나의 IDE에서 Primary, Secondary라는 개념을 통해 더 많은 장치들을 연결할 수 있도록 설계
  - ATA는 최대 4개의 장치만 연결 가능하며, 2개의 채널을 위해 2개의 ATA 커넥터를 이용
  - 각각의 채널은 다시 2개의 장치 연결을 위해 MS(Master)/SL(Slave)라는 방식을 사용
  - MS/SL의 구분은 각 장치에서 지원하는 점퍼 설정이나 시스템이 자동으로 구분하는 CS(Cable Select) 방식을 사용



ATA HDD의 Interface

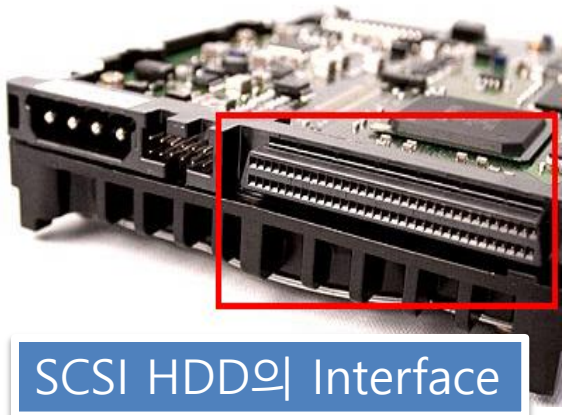
SATA (Serial ATA)

- SATA 인터페이스
  - 병렬 전송 방식의 ATA를 직렬 전송 방식으로 변환한 드라이브 표준 인터페이스
  - SATA 방식은 기존 ATA가 4개만 연결 가능했던 것에 반해 컨트롤러에 따라 5~8개까지 가능
  - 그리고 각 장치와 커넥터는 1:1 연결을 하므로 ATA와 같은 점퍼 설정이 필요하지 않음
  - ATA가 최대 133 MBps(MByte/sec)의 속도인 것에 비해 SATA1은 150 MBps, SATA2에서는 300MBps까지 지원하며, SATA3에서는 600MBps까지 지원

SATA HDD의 Interface

SCSI (Small Computer Systems Interface)

- SCSI
  - ATA가 ANSI에 의해 처음 표준으로 제정되던 1986년에 함께 제정된 표준 인터페이스 형식으로 주로 서버 시스템에 많이 사용
  - SCSI의 가장 큰 특징은 ATA에 비해 하나의 컨트롤러가 최대 16개의 장치가 연결 가능하다는 점
  - 각 장치는 서로 독립적으로 동작이 가능



SCSI HDD의 Interface

인터페이스	SCSI		ATA		
	SCSI1	Ultra 320 SCSI	PATA-133	SATA-150 (SATA I)	SATA-300 (SATA II)
전송 속도	5 Mbps	320 Mbps	133 Mbps	150 Mbps	300 Mbps

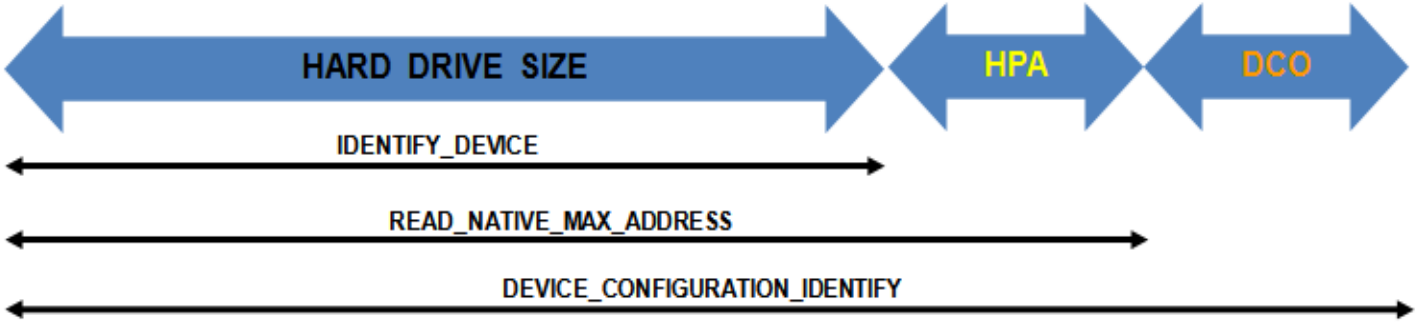
HPA, DCO

- **HPA (Host Protected Area)**
  - HPA는 ATA(Advanced Technology Attachment)-4 표준에서 추가된 기능으로 해당 영역은 HDD에 의해 미리 예약된 영역으로 BIOS를 통해 접근이 불가능함
  - 즉, OS에서는 보이지 않는 영역으로 일반 사용자에 의해 수정되지 않는 HDD의 영역
  - HPA 영역을 사용하는 경우
    - 시스템 부팅이나 진단 유틸리티 저장
    - CD, DVD와 같은 별도의 매체 없이 시스템 복구
    - 노트북 보안 유틸리티 저장
    - 루트킷을 통한 악의적인 용도 및 데이터 은닉

- **DCO (Device Configuration Overlay)**
  - ATA-6부터 추가된 기능으로 이 기능을 사용하여 60GB, 100GB, 200GB, 500GB, 1TB 등 여러 사이즈로 제조한 HDD를 같은 섹터 개수를 가지는 고정된 크기의 HDD로 구성이 가능
  - DCO도 BIOS를 통해 확인되지 않으며, HDD 제조사에 따라 정의된 특별한 ATA 명령을 통해 접근이 가능

HPA, DCO

- **HPA 영역과 DCO 영역**
  - 두 영역 모두 동일한 HDD 내에 존재할 수 있으며, 동일한 HDD에 HPA와 DCO를 동시에 구성하기 위해서는 먼저 DEVICE CONFIGURATION SET 명령을 통해 DCO를 설정한 후 SET MAX ADDRESS 명령을 통해 HPA를 구성해야 함.
  - HAP와 DCO가 모두 설정된 HDD에서 해당 영역들을 확인하는 방법



- **디지털 포렌식 관점에서 HPA, DCO**
  - 두 영역 모두 BIOS에 의해 확인되지 않기 때문에 증거를 은닉할 목적으로 사용될 수 있음
  - 따라서 하드디스크를 조사할 때는 HPA와 DCO 영역이 있는 지 확인해야 하며, 디스크 이미징의 경우 OS 상에서 BIOS를 통해 수집할 경우 HPA와 DCO 영역이 제외된 상태로 수집될 수 있음
  - 따라서 디스크 이미징 도구에서는 HPA와 DCO 영역을 고려하여, 해당 HDD의 모델이 가지는 정해진 용량을 확인해야 함

광학 저장 매체 (Optical Disc)

- **CD-ROM (Compact Disc - Read Only Memory)**
  - CD-ROM은 기존의 음성 정보 저장을 위해 개발된 CD(Compact Disc)의 발전된 형태로 모든 형태의 디지털 정보를 기록
  - 디지털 정보를 기록할 수 있는 기층(shyny underlayer)을 가진 폴리카보네이트(bulletproof polycarbonate)로 이루어진 12cm(120mm)의 단면만 기록할 수 있는 원형 판
  - 8cm의 소형 CD-ROM도 존재하지만 12cm가 주로 사용
  - 초기에는 용량이 540MB(Mega Bytes) 였으나 현재에는 650~700MB이고 포맷은 ISO 9660을 사용

- **DVD-ROM (Digital Versatile Disc, Digital Video Disc)**
  - DVD는 12cm(또는 8cm)의 알루미늄 원형 판에 플라스틱 막이 코딩되어 데이터가 기록되는 저장매체
  - 크기는 CD-ROM과 같지만 용량은 CD-ROM의 7배가 넘는 데이터 저장
  - DVD는 크게 싱글레이어와 듀얼레이어가 존재하는데 싱글레이어는 4.7 GB(Giga Bytes), 듀얼레이어는 8.5 GB의 데이터를 저장
  - DVD-R, DVD+R, DVD-RW 등의 다양한 포맷이 존재

차세대 광학 저장 매체 (Blu-Ray Disc)

- **차세대 광학 저장 매체**
  - 기존 DVD 를 대체하고, 고화질 비디오(HD: High Definition) 및 대용량 데이터를 지원하기 위한 광학 저장 매체
  - 2000년 초부터 개발되기 시작하여, Sony를 대표하는 Blu-Ray 진영과 Microsoft를 대표하는 HD-DVD 진영 간의 경쟁이 치열해짐
  - 2008년 HD-DVD 진영의 기업들이 컨소시엄을 포기함으로써 블루레이 디스크가 사실상의 표준으로 정립

- **블루레이 디스크(Blu-Ray Disc)**
  - DVD 디스크에 비해 훨씬 짧은 파장을 갖는 청색 레이저를 사용함으로써 DVD와 같은 크기인데도 더 많은 데이터를 담는 것이 가능
  - 저장 용량: 일반 DVD 크기(직경 12cm)의 싱글레이어 블루레이 디스크는 25 GB, 듀얼레이어 디스크는 50 GB를 저장
  - 종류: 블루레이 디스크(BD-ROM), 사용자가 블루레이 드라이브를 이용하여 데이터를 기록 가능한 BD-R(Recordable), 재기록 가능한 블루레이 디스크 BD-RE(Rewritable)

3. 디지털 기기의 종류

- **범용 시스템**
  - 개인용 컴퓨터(PC, Personal Computer)
  - 서버 컴퓨터
  - 메인 프레임(Main Frame)
  - 슈퍼 컴퓨터
- **임베디드 시스템**
  - 정보가전
  - 정보기기
  - 사무기기
  - 네트워크 기기
  - 기타

디지털 기기의 종류 – 범용 시스템

- **개인용 컴퓨터(PC, Personal Computer)**
  - 워크 스테이션 : 전문적인 용도
  - 데스크톱 컴퓨터 : 일반적으로 사무실 또는 가정에서 사용
  - 랩톱 컴퓨터 : 노트북, 무릎에 올려놓고 사용할 수 있다는 의미, 이동성
  - 넷북 컴퓨터 : 랩톱의 종류, 휴대성 강화, 적은 연산 작업에 사용
  - 태블릿 컴퓨터 : 랩톱에 태블릿 기능 추가, (ex : 아이 패드)
- **서버 컴퓨터**
  - 네트워크를 통해 클라이언트의 요청을 처리하는 컴퓨터
  - 예 : 웹 서버, 파일 서버, 프린트 서버, 네트워크 모니터링 서버, DNS 서버, DB 서버
- **메인 프레임(Main Frame)**
  - 단말기를 통해 다수의 사용자가 작업할 수 있는 범용 목적의 대형 컴퓨터
  - RAS(Reliability, Availability and Serviceability)
  - 금융기관, 정부 기관 등에서 사용
- **슈퍼 컴퓨터**
  - 연구 목적으로 사용되는 초고속 컴퓨터, 단일 기계로는 가장 빠름
  - 핵실험, 지진 데이터 분석, 기상 예층 등에 사용

디지털 기기의 종류 – 범용 시스템

- **디지털 포렌식에서 다양한 컴퓨터 조사**
  - 대부분의 조사 대상은 데스크탑 컴퓨터와 다수의 사용자가 접속해서 사용하는 서버 컴퓨터로 구분
  - 두 종류의 컴퓨터 모두 다수의 하드디스크가 내장될 수 있으며, 주로 하드디스크가 압수 수색에서 가장 중요한 대상
- **컴퓨터 조사 시 유의 사항**
  - 일반적으로 컴퓨터 본체를 압수하거나 하드디스크를 분리하여 디스크만 압수해야 하지만, 레이드(Raid) 시스템을 운영하는 환경의 컴퓨터나 서버의 경우 그 환경이 특수하므로 전체를 압수하지 못하고 사건에 연관된 일부 데이터만을 압수

    ※ RAID(Redundant Array of Independent Disks)

    여러 개의 하드 디스크에 일부 중복된 데이터를 나눠서 저장하는 기술

    레벨에 따라 저장장치의 신뢰성 향상, 전체적인 성능을 향상 등
  - 하드디스크를 분리할 때, 그 내용을 읽지 못하게 하는 시스템 또는 자동으로 파괴시키는 구조의 컴퓨터도 고려해야 하기 때문에 가능한 컴퓨터 안의 하드디스크는 컴퓨터 그 자체를 압수하는 것이 바람직
  - ODD 내부에 CD나 DVD가 들어있을 수 있으므로 이를 주의해야 함. 컴퓨터와 이동식 저장 매체는 각각 다른 증거물로 관리되기 때문

디지털 기기의 종류–임베디드 시스템

- **휴대폰**
  - 내부에는 플래시 메모리가 내장되어 있으며, 평소 휴대폰을 사용하여 저장하는 정보는 대부분 이 저장매체 안에 기록
  - 따라서 휴대폰을 조사할 때에는 기기 자체를 압수해야 하며, SIM(Subscriber Identity Module Card) 혹은 USIM(Universal Subscriber Identity Module Card) 메모리 카드를 장착하고 있으므로, 기기와 메모리 카드 각각을 분류해서 압수

- **개인 휴대용 정보 단말기 (PDA, Smart Phone)**
  - 내부 저장 장치로 플래시 메모리를 장착하고 있는 작은 컴퓨터
  - 또한 내장된 플래시 메모리 외에 소형 메모리 카드를 삽입해서 사용할 수 있으므로 이를 확인 후 각각을 압수
  - 스마트 폰의 경우에는 휴대폰과 같은 속성을 가지기 때문에 반드시 전자파를 차단해야 함

디지털 기기의 종류–임베디드 시스템

- **사무기기**
  - 복사기, 팩시밀리, 스캐너, 프린터, 복합기
  - 복합기 : 작업한 데이터가 저장되는 공간이 존재
    -> 디지털 포렌식 조사 대상
- **네트워크 기기**
  - NIC(Network Interface Card) : 데이터 링크 계층, MAC 주소
  - 허브(Hub) : 물리 계층, 전기적 충돌 발생 가능
  - 스위치(Switch) : 데이터 링크 계층, 전기적 충돌 없음
  - 라우터(Router) : 네트워크 계층, 동일한 프로토콜을 사용하는 다른 네트워크 연결
  - 게이트웨이(Gateway) : 서로 다른 네트워크를 연결

디지털 기기의 종류–임베디드 시스템

- **기타 임베디드 시스템 - 디지털 캠코더 및 카메라**
  - 영상 및 사진 정보를 담는 기기로서 포렌식 수사 관점에서 볼 때 컴퓨터의 하드디스크만큼이나 중요한 증거대상
  - 이 기기들은 내부적으로 플래시 메모리를 장착하고 있으나, 실제 영상이나 사진 데이터는 소형 메모리 카드를 통해 저장하므로 기기 안에 삽입되어 있는 메모리 카드는 반드시 분리하여 따로 확보
- **기타 임베디드 시스템**
  - 최근 MP3, PMP, 휴대용 게임기, 네비게이션, 비디오 게임기 등 다양한 디지털 기기에 대한 사용이 증가하고 있음
  - 이러한 기기들은 내부/외부에 플래시 메모리나 하드 디스크 같은 저장 매체를 이용하므로 포렌식 조사의 대상으로 인식하고, 데이터를 수집할 수 있도록 이를 확보해야 함

Q & A