Hard Drives

They're drives, and they're not soft

NMAAHC Workshop,
Caroline Gil and Eddy Colloton
2021

As we've done already with floppy disks and optical media, we're going to spend a bit of time talking about hard drives. Our conversation will be on both hard disk drives, sometimes called spinning disk drives, as well as solid state drives, also called flash drives. We're going to start with a short video clip that will illustrate the different components of a hard disk drive.

HDD

Nick Parlante - How A Hard Drive Works
http://www-cs-faculty.stanford.edu/~nick/
released as CC Attribution-ShareAlike 3.0   5/2012

Nick Parlante from Stanford

HDD

Platter | Spindle | Head
Actuator Arm
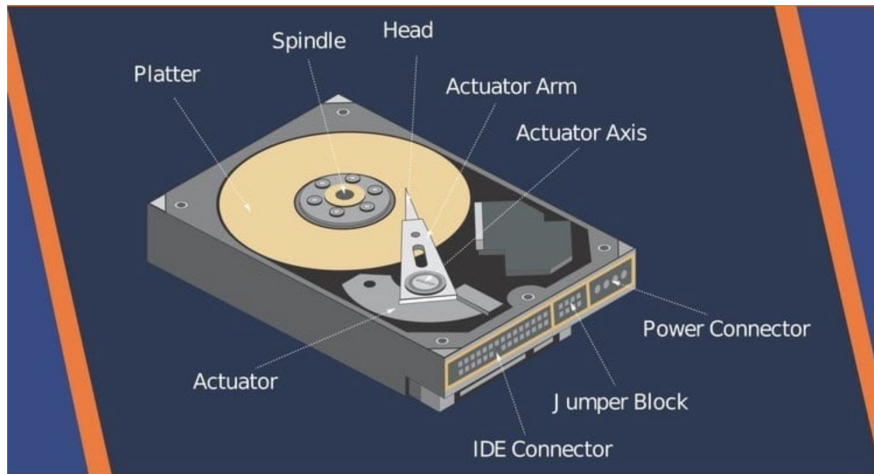Actuator Axis
Power Connector
Actuator
Jumper Block
IDE Connector

Image source: Understanding How A Hard Drive Works: A Useful Guide for Users
by TTR Data Recovery

NMAAHC Workshop,
Caroline Gil and Eddy Colloton
2021

I'm going to review the different components once more just for clarity since Nick goes through them pretty quickly:
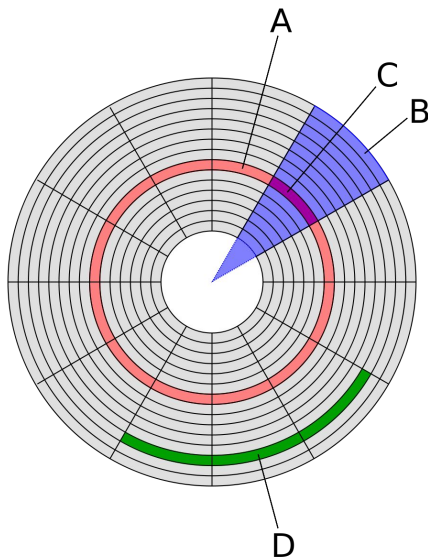
- platters
- actuator
- arm
- head
- spindle

It's important to remember that most hard drive have multiple platters, and they use multiple arms to access the different platters.

Fun Fact: In most modern hard drives, voice coils are used to control the actuator arm. As their name suggests, these are the simple electromagnets often used in audio technology, such as the moving coils used in subwoofers

HDD

Data is structured on platters in a similar way to the other formats, tracks form a ring around the disk and are subdivided into sectors. Sectors are traditionally 512 bytes. Remember, a series of adjacent sectors can grouped as a "block", which is set by the file system, and not by the hardware. Sometimes this differentiation is also referred to as a "physical sector" versus a "logical sector," with a logical sector being dictated by the file system.

The same file systems are used across spinning disks and solid state drives, so sector size, and the hierarchical structure of the file system is consistent across both. Solid state drives *physical* layout is somewhat different, however.

SSD

Programming via hot electron injection

12 V

0 V

floating
gate

200 Å

SOURCE

DRAIN

12 V
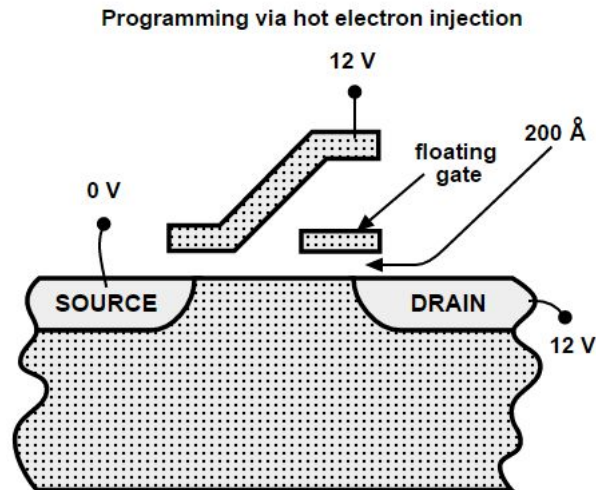
This is an image of a flash memory cell, the most granular element of an ssd. Each cell contains a floating-gate transistor, which stores individual electronic charge (actual electrons) in memory cells. Counter-intuitively, if there is no charge a binary reading of 1 is recorded, if there is a charge, it reads as a 0. In this was, solid-state drives don't rely on moving parts or spinning disks, hence their name.

SSD
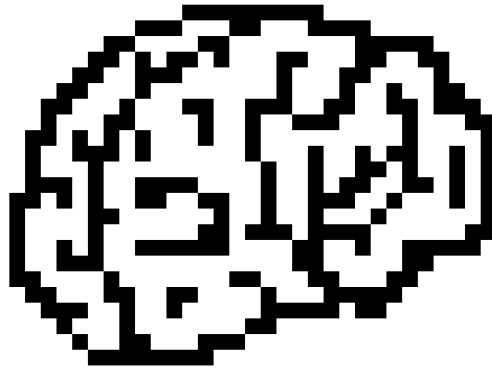
Created by emilegraphics
from Noun Project

Flash's complex organizational system is governed by firmware. The flash disk's firmware will record data to new cell locations when possible, and attempt to distribute writes to cell locations evenly to promote even wear on the memory cells and thus improve the memory cell life.

SSD

- Wear and Tear
  - Data is read/written using electrical pulses
  - Limited Number of Read/Writes
 - Read disturb
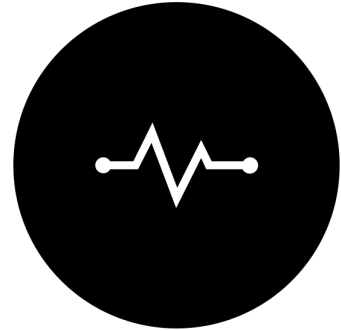
Created by Guilhem
from Noun Project

Flash data is written and read via an electronic pulse sent to the control gate of the memory cell. These electronic pulses take their toll over time, so solid state drives are said to have a limited number of read/writes. However, simply leaving a solid state drive on the shelf exposes it to risk as well. The permanent storage of electrical charge is impossible. The regular use of a drive, involves the active oversight of the drive's firmware, and maintenance of the cells' charges.

The complexity of storing an electrical charge should not be underestimated. Electronic pulses intended to read from one cell can actually accidentally charge neighboring flash cells, causing 1s to read as 0s. This is called "read disturb." Just as with other physical media however, redundancies are in place to ensure that read errors are mitigated.

SSD
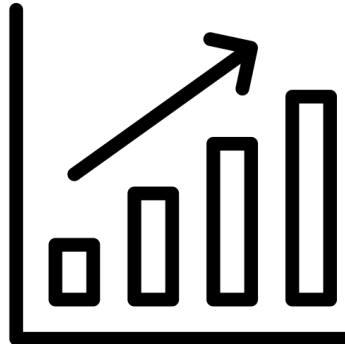
Created by Vectorstall
from Noun Project

Solid State Storage is growing in adoption and implementation almost across the board. Cameras, mobile phones, laptops all use solid state storage, so we're likely to see more collections material coming in on the drives. It still remains less popular for long term storage, as flash drives perform better when they're used regularly. That risk, coupled with the slightly higher cost of solid state, still leaves spinning disk as the preference for large-scale storage providers.

Hard Drives

- Connections

Going to transition now to talking about connection types.

Obviously when imaging external hard drives, the most straightforward approach is going to be to connect them using USB forensic bridges, which we've already discussed.

It's worth mentioning, though, that many larger external drives (not the thumb drive style external drive pictured here, but the tabletop style), inside their enclosure, have the same connection types as internal hard drives.

Hard Drives

SCSI   **IDE**   **SATA**

So either by taking an external drive out of its enclosure, or taking an internal drive out of a computer, you'll have access to these connectors. Unless you're working with a relatively old hard drive, you're far more likely to encounter the second two listed on the screen, an IDE connector type, or a SATA connector. On IDE hard drives, the four pin connector on the left in this image is the power connector to the drive, and the data connects to the multi-pin connector on the right. Be careful with these tiny pins, as they're very easy to bend. They'll still work if they bend, but it's best to try to avoid that if you can.

There are two SATA drives in this picture, a 3.5 inch, and, stacked on top of it, a 2.5 inch. The 2.5" size are more commonly used in laptops. On SATA drives the wider part is for the power and the smaller part is for the data.

Hard Drives

SCSI

IDE

SATA

Here are the corresponding cables for those connection types. As you can see front
he IDE and SATA connectors, sometimes the power is attached to the cable, but more
commonly, they're two separate cables, one for data and one for power.

Hard Drives

- Removing the Hard Drive
  - Plan ahead - Research
  - Apple Only - Target Disk Mode (hold "T" on startup)
  - Document position and connections
    - Multi-pin connectors are delicate!
  - Turn computer on beforehand?

- ESD
  - Wrist Straps
  - Anti-static Bags for storage

Image source: *Preventing Static Damage to Your Hard Drive*, Rocket Yard

It's important to be familiar with these types of connections if you're going to remove a hard drive from a computer. In the event that you need to remove an internal drive, do some research ahead of time to learn where and how the hard drive is connected in that specific computer model. It's quite likely there is already a youtube video of someone removing the hard drive front he computer you're working with.

Regardless, it's often straightforward to open the computer's case and physically extract the hard drive. However, certain Apple computers, especially early mac minis, don't make it so easy. Luckily, Macs have a feature called Target Disk Mode which allows for forensically-sound disk imaging without physically removing the hard drive from the computer's case.

If you are going to remove the hard drive from a computer, be sure to get lots of pictures of the drive before hand, so you'll have reference photos of how the drive was connected before it was removed. It *may* also be a good idea to power on the computer before removing the drive to ensure that everything is working correctly. However, depending on the state fo the computer, this may be to great a risk. That's best considered on a case-by-case basis.

Another risk to be aware of when considering removing a drive from a computer is electrostatic discharge or ESD. ESD occurs when static electricity suddenly flows from one charged object to another. This can occur, for example, when a person charged with static electricity touches exposed components, such as a hard drive or a RAM chip. ESD exposure may permanently damage the component, but this risk is

relatively low.

An ESD wrist strap is a common tool used for mitigating the risk of ESD damage. The wearer should attach the cable connected to the strap to something grounded, such as a large piece of metal touching the floor, an ESD mat, or the metal frame of the computer's case (Lowe 2017). Some ESD wrist straps are designed to plug into wall outlets, but these are not recommended. ESD straps are electrically conductive, and if there is a ground fault in the electrical wiring of the building, the wearer could be electrocuted (Lowe 2017).

When stored outside of the computer's case, hard drives can be placed on ESD safe mats and stored in ESD safe storage bags. These mats and bags contain conductive material that prevents static electricity from building up around the electronic component.

Hard Drives

- Technical Specifications of Target Computer
    - macos - System Information
        - Located in Utilities
        - Makes a new file on the hard drive
    - Linux - Hardinfo
        - In Applications under "System Profiler and Benchmark"
        - Makes a new file on the hard drive
    - Windows - MSINFO
        - Run the command "msinfo32"
        - Makes a new file on the hard drive

If you are working with internal hard drives from computers, an important bit of documentation to be aware of are system profile reports.

A computer's operating system can quickly generate a technical report of the hardware it is currently running on. This report will consolidate the technical aspects of a computer, including model number, serial number, ports, RAM, etc. The process is a bit different depending on the operating system. In the macos, you run an application called "System Information," in Linux it is called "Hard Info, and in Windows, MSINFO. Regardless, each application will crawl the computer's file system and create a new file. Keep this in mind when thinking about disk imaging. Creating a System Profile account will add a file to the drive, and therefore change the disk images checksum.