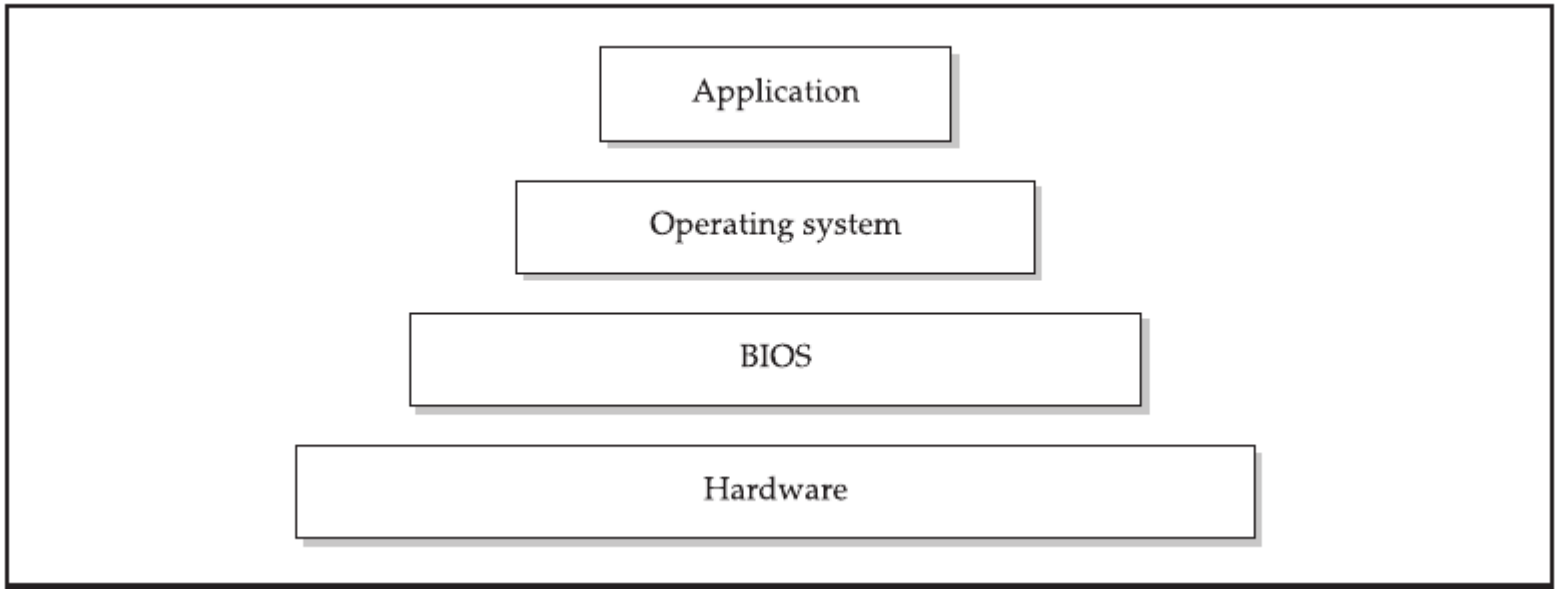
Komputer Forensik

CEH4D3

Computer Fundamentals

Introductions

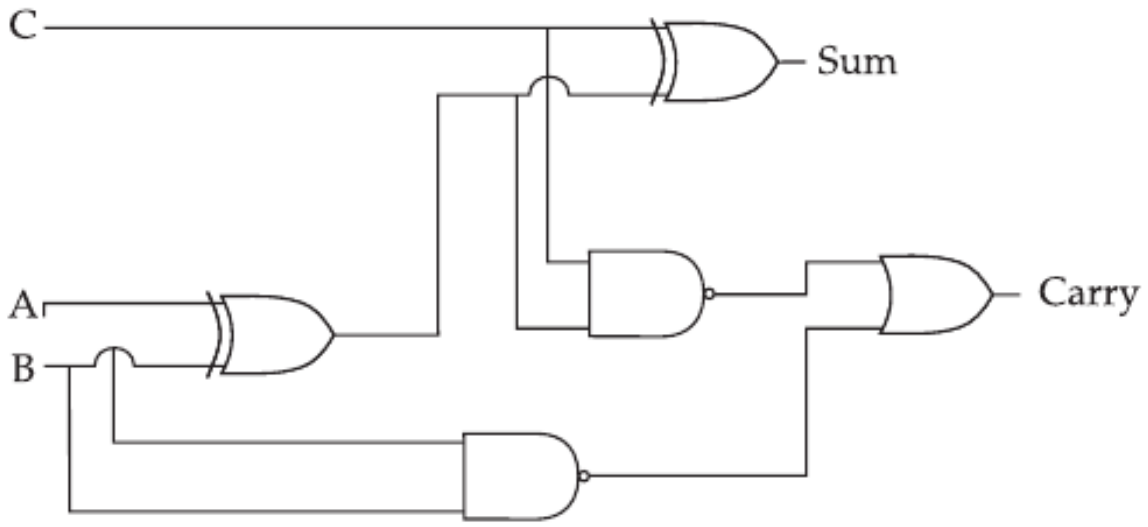
- A processor performs operations.
- A hard disk stores 1s and 0s.
- A video card converts those 1s and 0s to signals a monitor can understand.
- Put them together and you get the computer and all the possibilities that go along with it.


Application
Operating system
BIOS
Hardware

Binary System

- Every computing technology and application in existence was built by 1s or 0s.
- Known as binary number system, they are used in conjunction with transistors to create Boolean algebraic equations.
- The operations that these transistors can perform are AND, OR, NOT, and various combinations of those basic operators.
- Once these operations are defined, you can take the 1s and 0s and create a combinatorial network that performs conventional math functions (addition, subtraction, and so on).
- The Boolean operations can be combined to add two, 1-bit numbers (what is known as a 1-bit adder).

A 1-bit adder with a carry bit



- After you have built an adder, you can use it and the Boolean operations to perform addition, subtraction, multiplication, and division. You can also hook the adders together to add 8-, 16-, 32-, or 64-bit numbers, as most modern processors do.
- Computer builders have added specialized operations into computers that allow them to perform certain types of operations quickly.

Number of Transistors

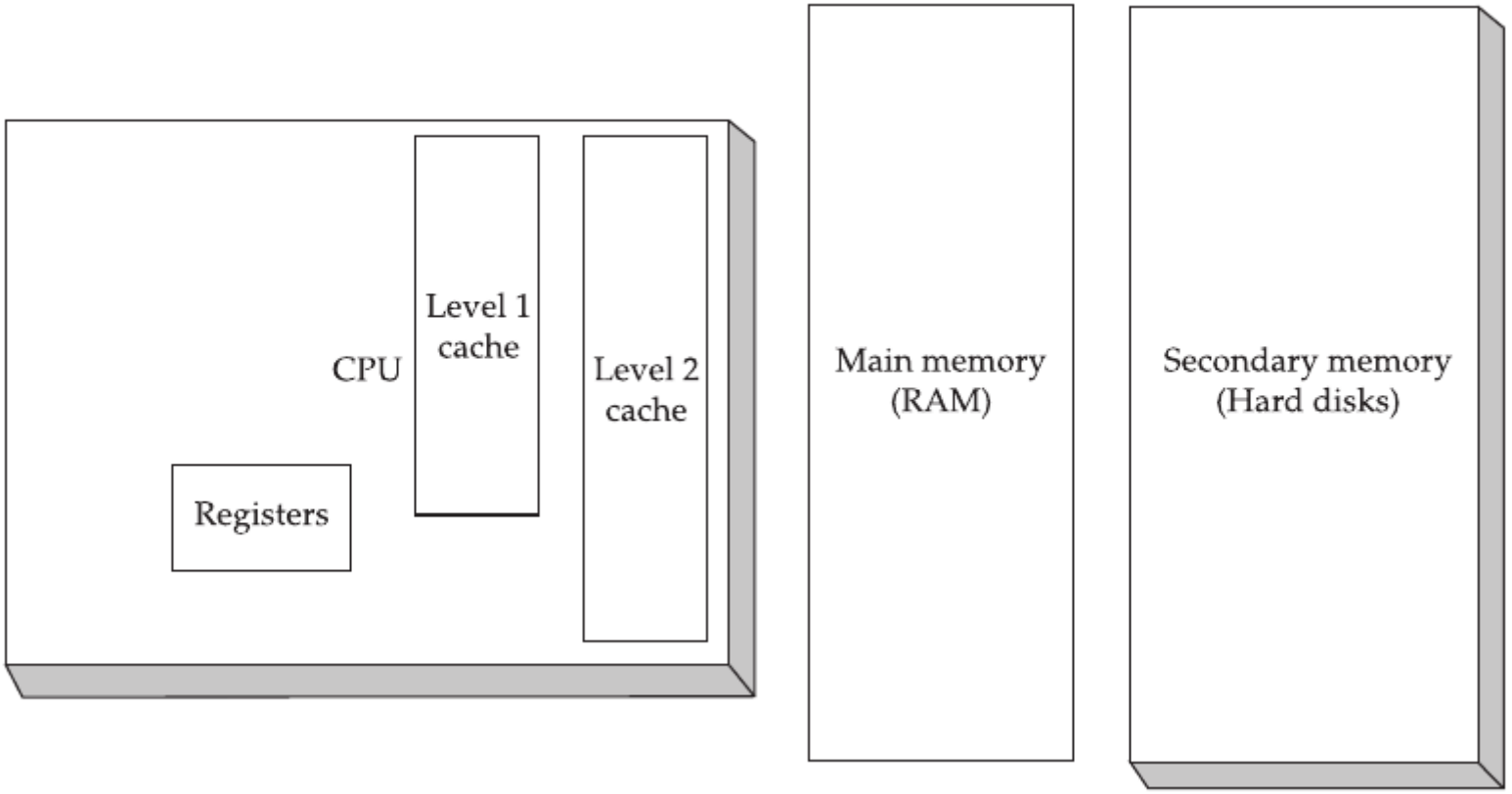
Processor	Year Created	Number of Transistors
Intel 8080	1974	6000
Intel 80486	1989	1,200,000
Intel Pentium	1993	3,100,000
Intel Pentium IV	2000	42,000,000

- The addition of multiple cores to processors.
- Dual core, 4, 8, 16, 16 cores.

Computer Memory

- Computers use two basic types of memory: volatile and nonvolatile.
- Volatile memory is difficult to retrieve when the computer is turned off.
- Examples of this type of memory are main memory (RAM, or Random Access Memory) and cache memory.
- Nonvolatile memory is not difficult to retrieve when the computer is turned off.
- This is usually the secondary memory source, such as hard disks or flash memory.

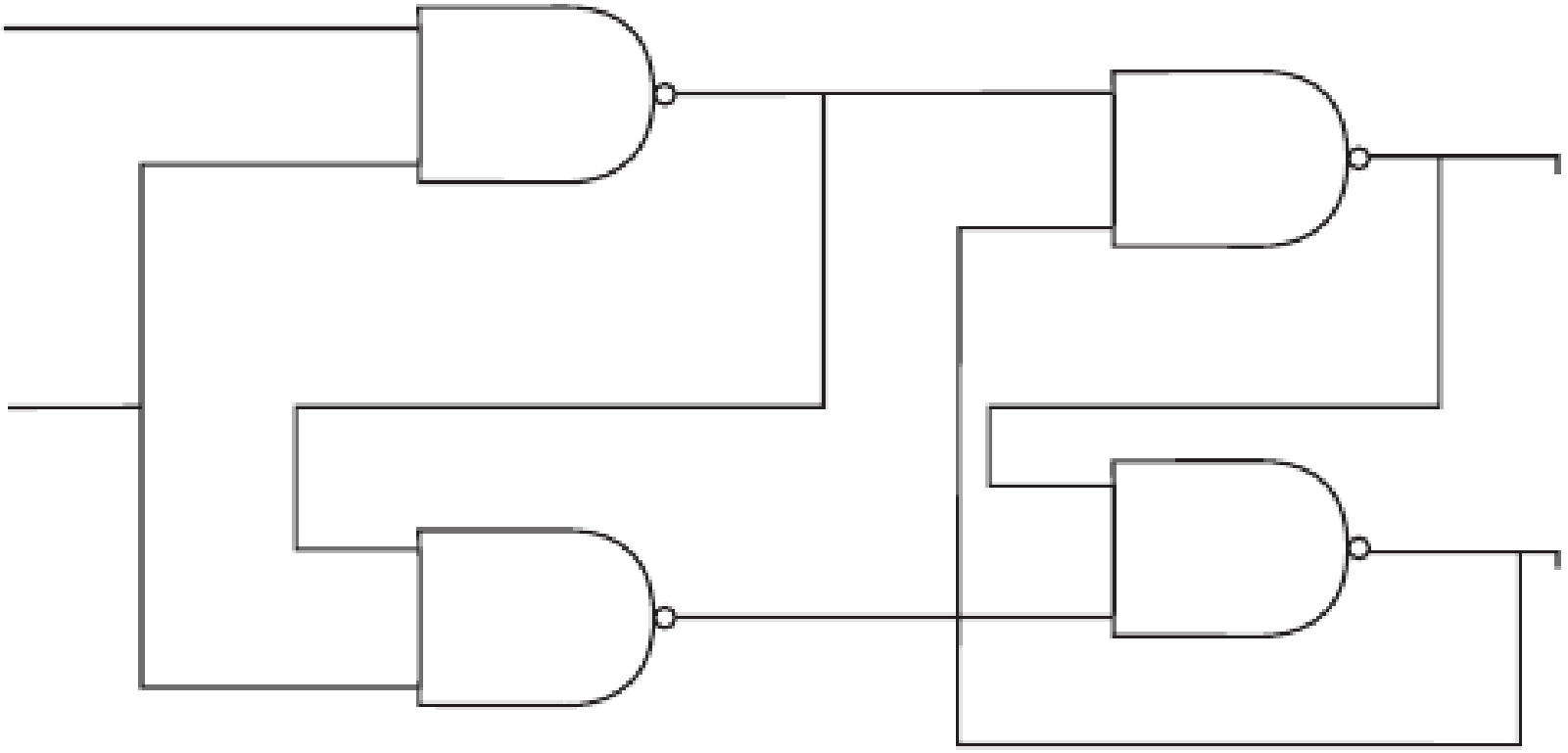
The memory hierarchy of a computer



Volatile Memory

- Think of volatile memory as a scratch pad that the computer uses when evaluating data.
- The most fundamental unit of this type of memory is the flip-flop, which can store a 1 or a 0 while the computer is on, and the computer can flip the stored value when it needs to store a different value.

Logical Diagram of a Flip-flop



Volatile Memory

- If you hook together eight flip-flops, you can store an 8-bit number.
- In the common nomenclature, a series of these flip-flops is known as a register.
- By combining this with the adder described earlier, you can add two numbers and store the result for later use.

Volatile Memory

- Registers hold a very small amount of data and are used only when the computer needs to store temporary values during multiple-step operations.
- For larger pieces of data, a second level of memory must be used, and this is where RAM comes in.
- RAM memory is outside the processor and can hold a very large amount of data while the computer is on.
- The downside to this type of memory, however, is the delay time the processor incurs when loading and storing data in RAM.
- Because of this lag time and the adverse effects on performance, most modern processors have what is known as a cache.

Nonvolatile Memory

- Used when data needs to be stored even if the computer is turned off.
- The most common type of media used in nonvolatile memory is magnetic media, such as a hard disk.
- The upside to magnetic media is that it can be purchased cheaply in comparison to volatile memory.
- The downside, however, is that it is incredibly slow in comparison.

Nonvolatile Memory

- Has moving parts: the typical hard drive has platters that spin around with a tiny magnetic head changing charges on the platter from positive to negative, which represent the binary 1s and 0s.

Nonvolatile Memory

- The other common type for media is NAND-based flash memory.
- Faster than magnetic drives.
- Has no moving parts.

Nonvolatile Memory

- Often used as swap space for the processor.
- This presents a unique opportunity for the investigator, because you can go back through the hard drive, find the swap file, and take apart the memory of the computer to locate evidence that would otherwise be destroyed or obfuscated.
- The specific way to do this varies from operating system to operating system.

- In fact, most of the time as a forensic investigator will be spent going through nonvolatile memory.
- Due to the timing of forensic investigations (you get the computers days, weeks, and sometimes months after the fact), very rarely will you have the opportunity to access the RAM in a form that is usable during an investigation.

BIOS

- Basic Input and Output System
- Provides simple methods for software to interact with hardware
- When the computer first turned on, the BIOS runs a series of self checks (called the Power On Self Test, or POST) and then turns control over to the operating system
- This transition occurs by way of what is called the Master Boot Record (MBR) on the hard drive
- BIOS manages the allocation of resources (via interrupt requests, or IRQs, and direct memory access, or DMA) to the peripherals and handles basic security measures.

Operating System

- The OS is by far the most complex piece of software on any given computer.
- Acts as the translation layer between the end-user applications and the BIOS or hardware.
- The OS manages the users, the memory, the applications, and the processor time on the computer.
- It is recommended for an investigator to spend time learning the mainstream OSs inside and out.

Applications

- Applications are the main reason to use a computer.
- From a forensics perspective, it is beneficial for you to become familiar with the ins and outs of a few select applications.
- Understanding the way that office applications create and delete documents, how e-mail programs work, and how web browsers access the Internet will help you track down evidence that you can use in your investigation.

Types of Media

Types of Media - Introduction

- Investigations will focus primarily on the secondary memory area—hard disks, CD-ROMs, tape backups, and most other types of commonly used storage.
- Each of these types of media has its own nuances and pitfalls in an investigation.
- Three most common types of media—magnetic, optical, and RAM.
- Most of the time, forensic analysis on flash memory is similar to magnetic media.

Magnetic Media

- Some kind of metal or magnetic surface holds a series of positive or negative magnetic charges.
- This series represents 1s or 0s, depending on the charge of the magnet.

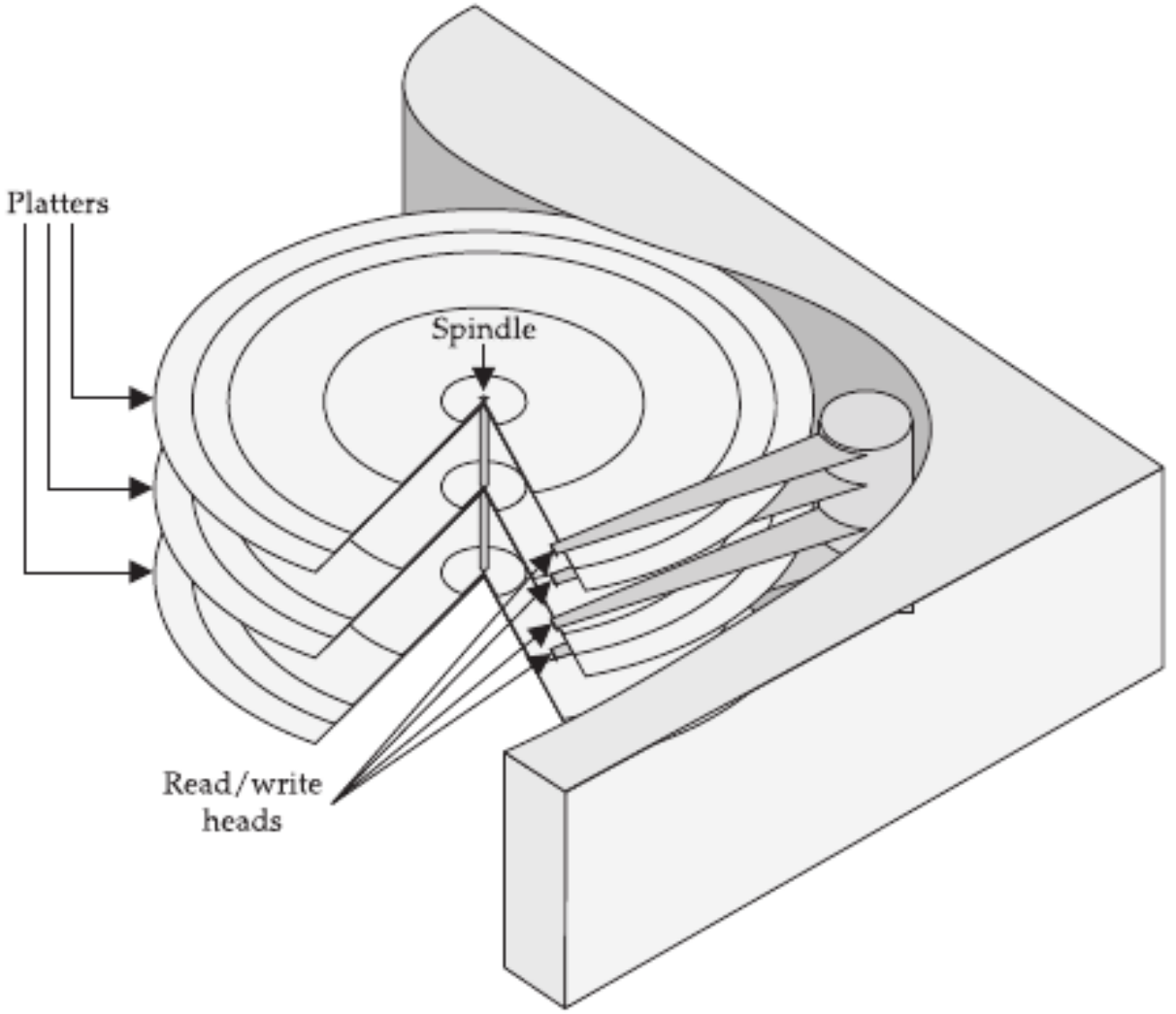
Magnetic Media

- When data is changed on the media, the magnetic charge is changed.
- This means several things:
  - First, there are moving parts, and moving parts are susceptible to breaking. Always have backups.
  - Second, the media is open to being affected by external magnets. This means that the forensic lab procedures and storage policies must consider this, and they must be able to prove that this hasn’t happened when dealing in a court of law.

Hard Disk Drives

- Ninety percent of an investigator’s time will be spent imaging, searching, or wiping hard drives.

Physical Parts of the Hard Drive



Physical Parts of the Hard Drive

Platters

- Platters are the circular discs that actually store the data.
- A single hard drive will include multiple platters often made of some aluminum alloy, but newer drives use a glass or ceramic material.
- These platters are covered with a magnetic substrate so that they can hold a magnetic charge.
- Hard drive failures rarely occur within the platters. In fact, nine times out of ten, if you send a drive off to a data recovery firm, it will take the drive apart and mount the platters in a new drive assembly to retrieve the data from them.

Physical Parts of the Hard Drive

Read and Write Heads

- Tiny magnetic read and write heads change and read the magnetic state on the platters.
- The head is a copper coil that has charges pushed through it. This creates a magnetic field that can either read or write data.
- Because there are multiple platters, multiple heads are used. Typically, to optimize the usage of the platter, both the top and bottom of the platter’s surface are used.
- For performance purposes and for better reliability, all the heads are hooked together and move in unison. This way, data can be read simultaneously from multiple platters.
- These are so compactly designed that they must be assembled in a clean room, because even a single stray particle can disrupt the head alignment.

Physical Parts of the Hard Drive

Head Actuator

- For many years, this was a major source of failure for hard drives.
- The two types of head actuators are stepper motor and voice coil.
- Stepper motor actuators were used on old hard drives (< 100 MB)
- Voice coil actuators correct themselves if they get lost on the platter using grey code. In addition, they don’t have to be parked before a hard drive is spun down.

Physical Parts of the Hard Drive

Spindle Motor

- Spins the platters.
- Engineered to very strict standards, since they have to be able to maintain precise speeds and must not vibrate.
- Rotate at a constant rate (such as 3600, 4200, 7200, 10,000, or even as high as 15,000 RPM).
- A feedback loop is set up inside the motor to ensure that it rotates at exactly the correct speed.
- On older hard drives, the motor was on the bottom of the drive, but now they are built into the hub of the platters to conserve space and allow for more platters in the drive.

Physical Parts of the Hard Drive

- The protocol used by the hard drive to communicate with a host computer or network. Following are the types of interfaces commonly used by personal computers:
  - PATA
  - SATA
  - SCSI
  - SAS

PATA

- PATA/EIDE (Parallel Advanced Technology Attachment/Enhanced Integrated Drive Electronics)
- The old standard for connecting hard drives and other devices to the motherboard using a ribbon cable and a 40-pin connector.
- These types of drives are typically hooked up externally to a computer using USB or Firewire converter.
- May occasionally encountered installed in older computers.

SATA

- SATA (Serial Advanced Technology Attachment)
- The serial interface that has come to replace PATA.
- Uses a much narrower cable and has faster data transfer speeds.
- Can be connected internally to the motherboard or externally as eSATA, USB, or Firewire converters.

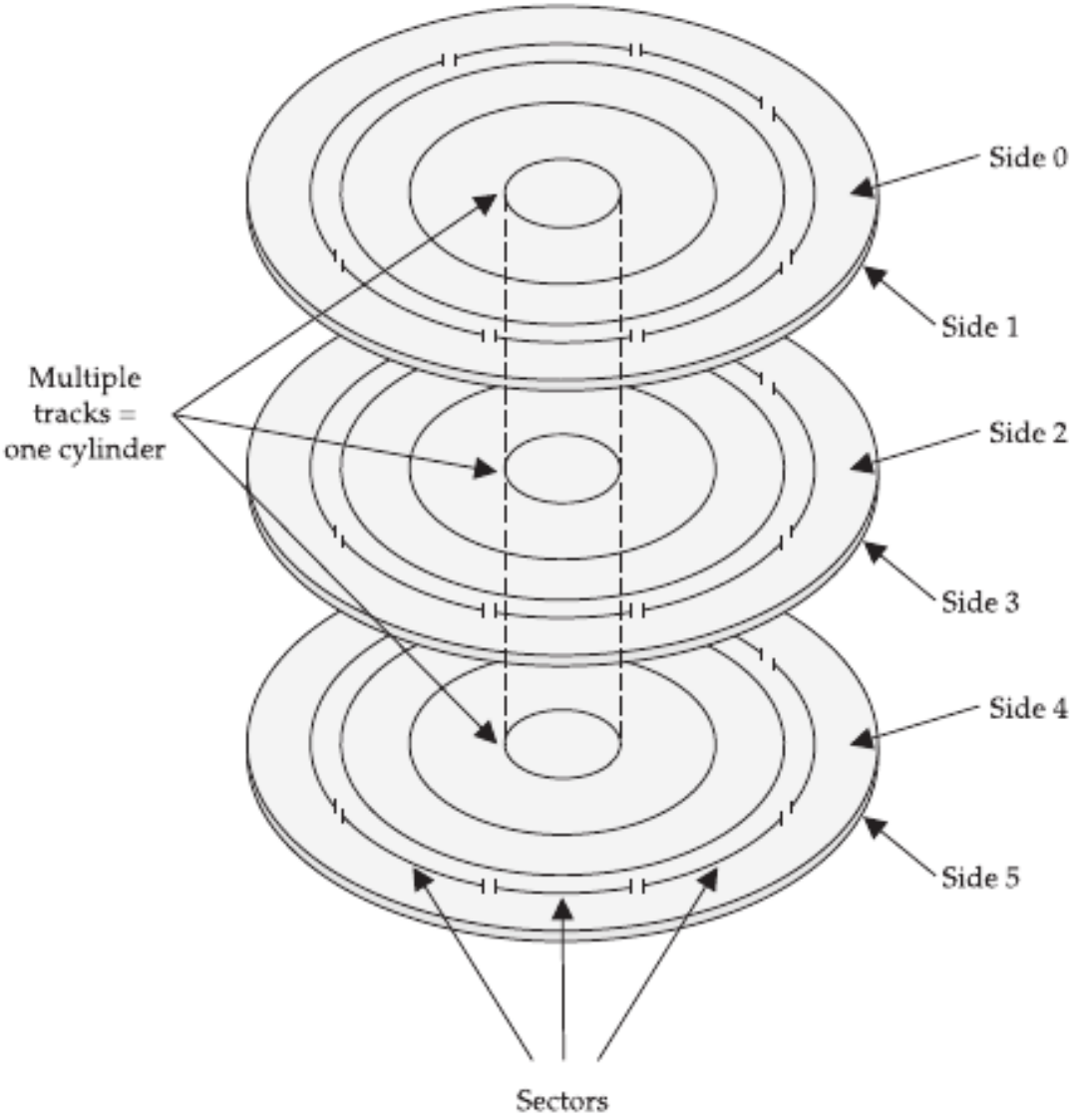
SCSI

- SCSI (small computer system interface)
- Often seen in servers and RAID controllers, but occasionally you'll find personal computers with them as well, although they are quickly being replaced by SATA.
- SCSI can be used as both an external and internal interface.

SAS

- SAS (Serial-Attached SCSI)
- The progression of SCSI drives into a point-to-point serial protocol.
- Offers faster transfer speeds over its predecessor in addition to using a narrower cable. More devices can also be supported on the SAS bus.
- It’s worth noting that SATA devices can be hooked up to SAS controllers.

Storing Data on the Hard Drive



Storing Data on the Hard Drive

- Three basic units denote position of data on a hard disk: head, sector, and cylinder.
- Head
  - Came about when multiple platters were added to the hard drive assembly.
  - The head number corresponds to the platter that holds the data.

Storing Data on the Hard Drive

- Sector
  - The name sector is derived from the mathematical term for a pie-shaped division of a circle. This term was chosen because sectors were originally broken out in pie shape on the physical disk.
  - Each sector contains 512 bytes of user data and some extra bits for error-correction and metadata. It’s the smallest unit of data that a hard disk can effectively read.
  - On older hard disks, the actuator couldn’t handle having different numbers of sectors for each track. Because of this, the shape of the sector was maintained and the density of the bits on the platter was lessened as you went to the edge of the disk.
  - This changed with zone-density recording, where a variable number of sectors could be included per track. Sectors are rolled up into units known as clusters when a file system is placed on the disk.

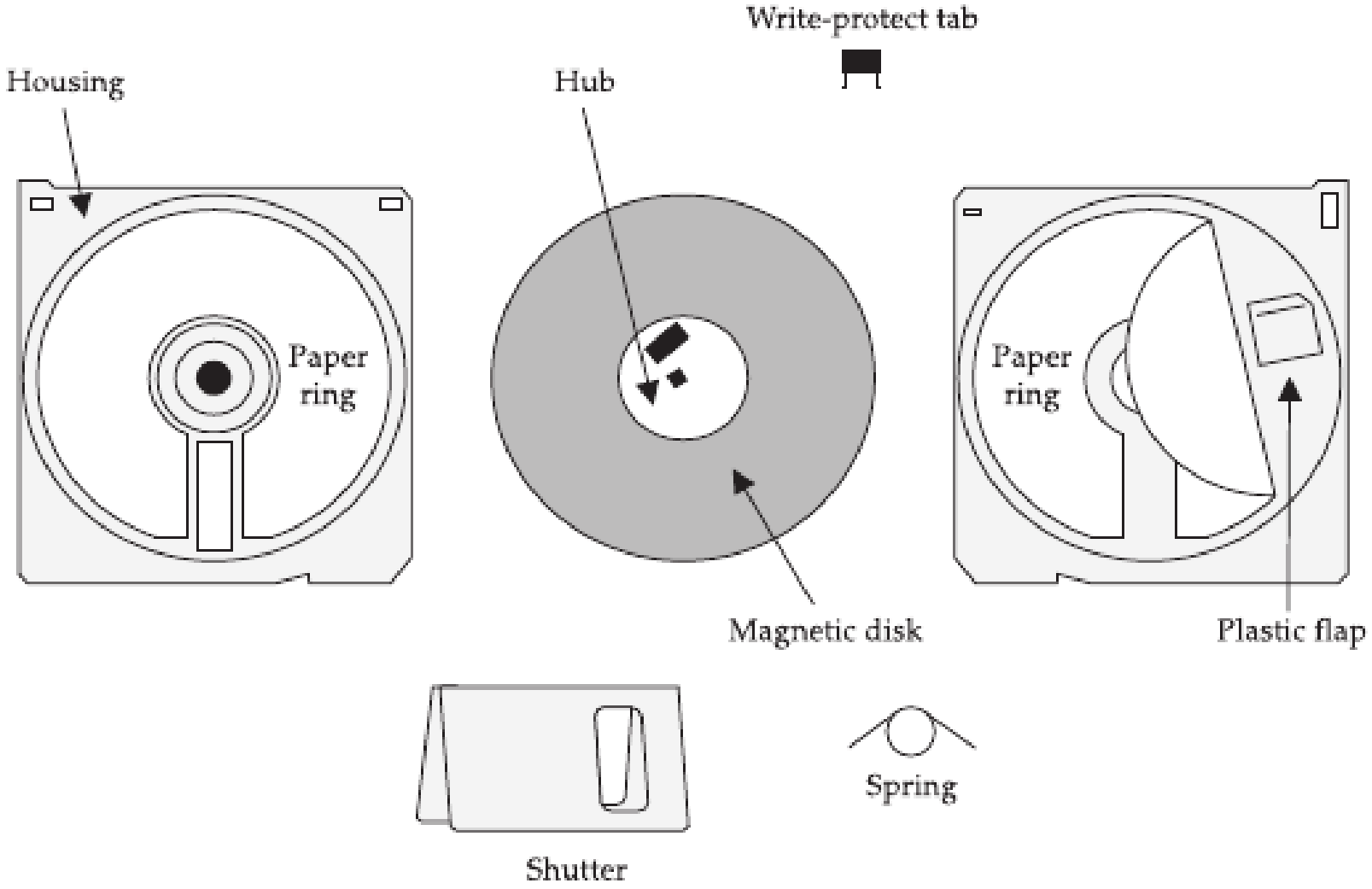
Storing Data on the Hard Drive

- Track/Cylinder
  - Think about a phonograph needle traveling around an LP. Now think about the concentric rings inside a tree. Tracks on a hard disk are laid out in the same fashion.
  - These are the actual streams of data that are written to the hard drive.
  - On multi- head hard drives, the cylinder is the combination of each track on all platters that can be accessed with the head in a certain position.

Floppy Disk

- While they aren’t used much anymore (or at all), you will still run across them if you are working on an investigation with a timeframe that goes far enough back.

Floppy Disk


Write-protect tab
Housing
Hub
Paper ring
Paper ring
Magnetic disk
Plastic flap
Spring
Shutter

Floppy Disk

- Just like the parts, the actual structure of the disk is similar to a one-platter hard disk.
- The platter is encased in either a hard or soft plastic cover that protects the storage disk inside. In the upper corner of the disk is a notch that can be set to write-protect the disk.
- The main difficulty you may have in a forensics investigation involving floppy disks is the formatting. The typical 3.5-inch disk would hold 1.44MB of data, but by using compression or extra sectors on the disk, an extra half meg of storage could be squeezed on. Woe be the investigator who has to figure out one of these cryptic methods of storing data on the disk. They are poorly documented and more than a few different ways are used to store on the disk, with no real identifying marks.

Always use forensically designed and validated tools when you deal with disks. Some tools on the market claim to pull complete disk images, but fail to do so. Other programs claim to wipe drives completely, but don’t. It is possible to derail investigation by placing bad data in end sectors and playing games with the media in general. Know the drives and layout inside and out. Use tools that you understand completely and know exactly how they work

Tape Backup Drives

- Normally used for long-term backup and data recovery purposes.
- Three of the most common drive types: DAT, DLT, and LTO.

Tape Backup Drives

- DAT (Digital Audio Tape)
  - They are more often referred to by their data recovery name, Digital Data Storage (DDS).
  - Originally created for use in high-end audio applications, but after a few tweaks for robustness, they now work well for backups.
  - They employ a helical scan technique that allows data to be tightly packed on the media, requiring less actual tape than traditional tape methods. As a tradeoff, however, they experience a lot of friction when writing to the tape. This causes the tape head to gain residue over time and can actually silently hamper the writing of data onto the tape.
  - When dealing with these drives, keep in mind the difference between a DDS and a DAT. The DAT is held to a much lower standard of quality and manufacturing than the DDS. DATs can cause problems down the line with tape breakage and loss of data.

DAT/DDS

Standard	Transfer Rate	Capacity
DDS	550 KBps	2GB
DDS-1	1.1 MBps	2GB
DDS-2	1.1 MBps	4GB
DDS-3	2.2 MBps	12GB
DDS-4	4.8 MBps	20GB

Tape Backup Drives

- DLT (Digital Linear Tape)
  - Relies on a linear recording method with either 128 or 208 total tracks.
  - The tracks are written in pairs along the entire length of the tape. The heads are then realigned, and two more tracks are written in the opposite direction. This process continues until the tape is full.
  - The design of the DLT drive is a bit different because it has only one spindle in the tape itself. The other spindle is in the drive and the tape is wound back onto the cartridge upon ejection.
  - Superior to DAT because it places less tension on the tape with less friction, and thus the drive requires less maintenance and has a lower failure rate.
  - The super DLT is essentially the same technology, but it uses a combination of optics and magnetism (laser-guided magnetic recording, or LGMR) to increase the precision of the tape..

DLT

Standard	Transfer Rate	Capacity
DLT2000	1.25 MBps	15GB
DLT4000	1.5 MBps	20GB
DLT7000	5 MBps	35GB
DLT8000	6 MBps	40GB
SDLT 220	11 MBps	110GB

Tape Backup Drives

- LTO (Linear Tape-Open)
  - LTO drives also uses a linear recording method.
  - It is an open standard that was developed jointly by Hewlett-Packard, IBM, and Seagate.
  - LTO tapes were initially designed to come in two form factors: Accelis and Ultrium.
    - The Accelis was designed for fast data access
    - The Ultrium, which is known for its high capacity.
  - The Accelis never became commercially available, while the Ultrium is now a top competitor for DLT due to its higher transfer rates and data capacity.

LTO

Standard	Transfer Rate	Capacity
LTO-1	15 MBps	100GB
LTO-2	40 MBps	200GB
LTO-3	80 MBps	400GB
LTO-4	120 MBps	800GB
SDLT 220	11 MBps	110GB

Multi-Loader

- The amount of data that needs to be backed up may exceeds the capacity of a single tape.
- In such cases, multi-tape loader mechanisms are used. These can be anything from two-tape contraptions to advanced robotic arms that sling tapes around.
- From an investigator’s standpoint, make sure you always find out not only what multi-loader was used, but also how the software stored data on the multiple tapes.

Optical Media

- CD-ROM
  - Uses a red laser as the read mechanism to extract data off the drive.
  - Like hard disks, CD-ROMs use high and low polarization to set the bits of data; however, CDs have reflective pits that represent the low bit. If the pit is nonexistent, the data is a 1; if the pit exists, it’s a 0.
  - Has their own file system that is independent of the operating system, commonly referred to Joliet file system.
  - With certain parts of the disc populated, the disc can become bootable. The standard size for a CD-ROM disc is 650MB.

Optical Media

- DVD
  - Similar to CD-ROM technology with some tweaks.
  - DVDs use a much more precise laser. Since the laser has a smaller wavelength, the data density is much greater, so the disc can hold more data. The entire DVD holds up to 4.8GB of data.
  - DVDs use a multilayer system that allows multiple discs to be overlaid onto one disc. The setup is much like the platters on a hard disk. The laser is focused on the layer holding the data being read, allowing it to pull data from only that layer.

Optical Media

- Blu-ray
  - Similar to DVD technology with some more tweaks.
  - Uses blue laser to read the data, with a much smaller wavelength.
  - Allow for as much as 50GB to be stored.

Memory Technologies

- USB Flash Drives
- SDCard
- SSD

USB Flash Drives

- Has no moving parts.
- Each bit is set by using a two-transistor cell. The memory bank then communicates with the computer using a controller and USB interface, much like a hard disk communicates over IDE or SCSI.
- An important thing to remember about these drives is that some of them have a physical switch that forces a read-only mode. Use this whenever you are extracting data for investigation.

SDCard

- Has no moving parts
- Improvement over MMC
- Typically uses NAND flash
- NAND flash is more convenient for writing (smaller pages, faster erase) but is less reliable.
- May get bad blocks after a while, with a lot of writes.

SSD

- Based on flash memory
- Not divided into the traditional 512 byte blocks, but instead is in pages of 2KiB, 4KiB, or larger, although it is still presented to the host computer in blocks
- Whilst hard drives can be written in a single pass, flash memory pages must be erased (in whole) before they can be rewritten.

SSD

- Rewriting a block at the operating system level does not necessarily rewrite the same page in the flash memory due to the controller remapping data to spread wear or avoid failing pages
- Each page can be erased and rewritten a limited number of times – typically 1000 to 10,000. (Hard drive sectors, in contrast, can be rewritten millions of times or more.)
- Flash data is often encrypted on the drive, and can be "erased" by telling the controller to forget the old key and generate a new one, as well as marking all blocks as unused.