PART 1,2,3

Wednesday, March 29, 2023 2:29 PM

Converting the characters or other objects into binary is done by using ASCII(before since it has 127 values out of 256 values) and now UTF-8((can store in more than one byte where ascii stores in one byte)we can use this to form a variable number of bytes(emoji's into binary))

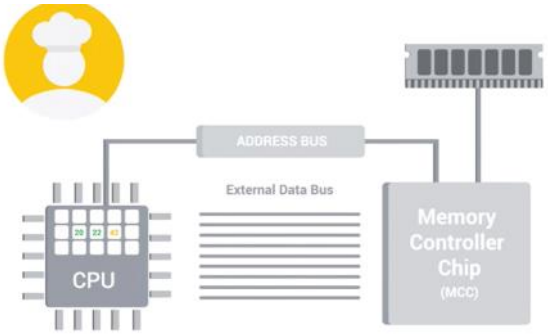
For colors the three RGB is used and a set of characters are used to shuffle in order to determine the color and put it into each pixel we see

Transistors helps us in determining and sending electrical signals as 1,0

It uses logic gates in order to determine where to send this electrical signals depending on logical conditions and to do complex tasks

The external Data Bus(EDB) connects the data movement across the computer

The registers are the storage that computers use for calculation like A+b=c(a=register a,b=register b,c=registerc)



3 ghz means 3.4 billion cycle per second (there is a bus known as clock bus which sends a signal indicating the cpu that it can start its one set of processing like that in cycles)
Overclocking means doing more than this will heat the cpu because it can do only these average amount of cycles

A CPU cache is normally stored inside each core of the CPU. Older computers might store CPU cache in a transistor chip that is attached to the motherboard, along with a high-speed bus connecting the chip to the CPU

Level 3 cache: L3 cache is the largest and slowest of CPU cache. However, it is often twice as fast as RAM. L3 is the first CPU cache location to store data after it is transferred from RAM. L3 cache is often shared by all of the cores in a single CPU.

Level 2 cache: L2 cache holds less data than L3 cache, but it has faster access speeds. L2 holds a copy of the most recently accessed data that is not currently in use by the CPU. Each CPU core normally has its own L2 cache.

Level 1 cache: L1 cache is the fastest and smallest of the three CPU cache levels. L1 holds the data currently in use by the CPU. Each CPU core usually has its own L1 cache.
Achieving a higher CPU clock frequency rate means the CPU can process a higher volume of instructions per nanosecond, resulting in faster performance

Overclocking a CPU's frequency involves three variables:

> The base CPU clock frequency, often measured in GHz.
>
> The core frequency, which is calculated by multiplying the base frequency by the CPU core multipliers.
>
> The core voltage, which needs to be increased in small increments to meet the increasing power demand of the CPU during the overclocking process.

1. **Check if overclocking is supported:** First, make sure the CPU is a model that is unlocked for overclocking. Not all CPUs can support overclocking, including most laptop CPUs. Check the CPU manufacturer's documentation to determine if overclocking is possible for the CPU model. Both Intel and AMD provide overclocking guides and tools for supported CPU models (see below for links to these guides). Additionally, check the documentation for the computer's motherboard model to ensure that it can support an overclocked CPU.
2. **Clean the inside of the computer:** Turn off and unplug the computer. While wearing an anti-static wristband, open the computer and use compressed air to remove any dust build-up that has accumulated. It is especially important to remove any dust from around the CPU, fans, and intake vents.
3. **Ensure an appropriate CPU cooler is installed (critical):** If the computer has a stock CPU cooler, it is most likely insufficient for cooling an overclocked CPU. Replace the stock CPU cooler with an advanced cooling system, like a liquid cooling system.
4. **Follow the manufacturer's instructions for overclocking the CPU:** Using the detailed instructions from the manufacturer (see below for links to Intel and AMD's guides):
    1. Use benchmarking software to establish a baseline for the normal performance of the computer.
    2. Set each CPU core multiplier to the value of the lowest multiplier using either the manufacturer's overclocking software (recommended) or the BIOS. Then reboot the computer.
    3. Increase each CPU core multiplier by 1 to increase the CPU frequency.
    4. Test each increase for stability using the testing utility provided by the manufacturer.
    - Fix any problems flagged by the testing tools, especially temperature alerts. If the system becomes too unstable, roll back to the last frequency that produced a stable performance and stop overclocking the CPU.

- If the voltage appears to become insufficient to support the new frequency, increase the voltage by 0.05V. Do not increase the voltage above 1.4V without specialized cooling hardware.
- If the computer freezes or crashes, it has either become completely unstable or the CPU is not getting enough voltage to support the overclocked frequency. Use the BIOS to return to the last stable frequency or increase the voltage in 0.01V increments until stable.

5. If stable, reboot the computer before attempting the next increase.

CPU:

Land Grid Array and Pin Grid Array. LGA – Land, i.e., Flat CPU with no pins, motherboard sockets with pins. PGA – Pins, i.e., Not Flat – CPUs with pins, Motherboard sockets without pins

There are also different types of memory sticks that **DRAM** chips can be put on. The more modern **DIMM** sticks, which usuallystands for **Dual Inline Memory Module**, have different sizes of pins on them.

In today's system, we use another type of RAM, called **double data rate SDRAM** or **DDR SDRAM** for short.

MOTHERBOARD:

Northbridge- interconnects RAM and video cards
Southbridge - maintains i/o controllers

Peripherals are extenral devices that are connected the the computer

Serial ATA(SATA) cable is used for hard drive,ssd data transfer(can plug without turning off the power)(one way)

NVMe technology utilizes the PCIe bus, instead of the SATA bus, to unlock enormous bandwidth potential for storage devices. PCIe 4.0 (the current version) offers up to 32 lanes and can, in theory, transfer data up to 64,000MB/s compared to the 600MB/s specification limit of SATA II

PCIe refers to PCI Express, a multifaceted interface on modern motherboards that provides everything from larger sockets for graphics cards, to smaller ports for add-in cards for Wi-Fi, USB ports, and more

Direct Current => in a one way
Alternating current => in both ways (this is converted to dc for computer)

Voltage means like in a water supply the pressure determines the speed of water like that higher voltage means high throughput that the computer needs it will get

MOBILE DEVICES:-

System on a Chip (SoC)

Packs the CPU, RAM, and sometimes even the storage onto a single chip

CHARGE CYCLE IS THE 1 cycle of charge and discharge of battery

Basic Input Output Service(BIOS) tells the computer about the hardware and keeps up and running

Usually BIOS are stored in a special ROM chip in motherboard

Unified extensible firmware interface (UEFI)

Performs the same function of starting your computer as the traditional BIOS, but it's more modern and has better compatibility and support for newer hardware

Reimaging means wiping and reinstalling the operating system

Even the slightest bit of electricity can cause damage to delicate computer components, so you should always make sure to ground yourself.(like wearing a device(like glouse) by connecting to the physical metal part)

After we install the cpu in the mother board we need to install the heat sink on top of the cpu (it will get the heat through the copper wire it has and blows it off through the fan it has) and a thermal paste that makes the heat go to the heat sink in a good way

A molex is a component connector that is with the heat sink and the motherboard that controls the fan speed

POWER SUPPLY TO CPU AND MOTHERBOARD

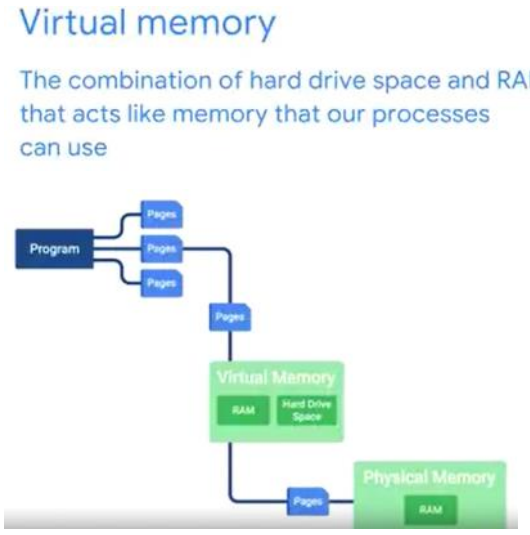
(MOTHERBOARD,CPU,HEAT SINK,THERMAL PASTE,RAM,POWER SUPPLY,HARD DRIVES,GRAPHICS CARDD)

CMOS is the memory on a motherboard that stores the BIOS settings. A small battery, called a CMOS battery, keeps it powered

The BIOS is the program that starts a computer up, and the CMOS is where the BIOS stores the date, time, and system configuration details it needs to start the computer.

The BIOS is the program that starts a computer up, and the CMOS is where the BIOS stores the date, time, and system configuration details it needs to start the computer.
DVI: DVI cables generally just output video
NVMe (NVM Express): interface standard which allows greater throughput of data and increased efficiency
POST (Power On Self Test): It figures out what hardware is on the computer

OPERATING SYSTEM:



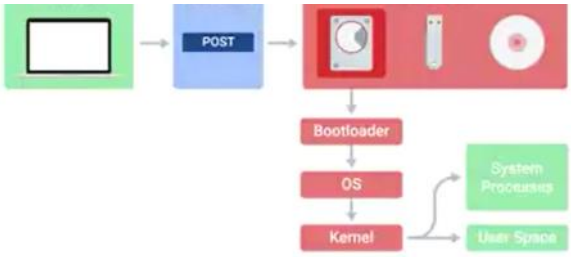
If any slowness is happening then we need to see whether the devices connected have the process for in and out with max rate

We can use logs to see the system events

A low-level software that initializes our computer's hardware to make sure everythi is good to go

Bootloader

A small program that loads the operating system



External options

- **USB drive:** You use a USB drive loaded with resources needed to boot the computer. This drive is inserted into a USB port and chosen at startup.
- **Optical Media:** You use an optical media disk loaded with booting resources. This disk can be a DVD, CD, or Blu-ray disk and is loaded through the computer's optical drive.

  The USB drive and optical media methods are useful for recovering a computer with a corrupted OS. They can also be used to start up a computer with a different OS. For example, you might boot a Windows computer in a Linux environment by using a USB with Linux OS. You will need to prepare these media with a bootable OS in order to use them as a boot method (see resources linked below).
- **Solid State Boot Drive:** You can use a solid state drive to boot your computer. Solid state drives do not use spinning discs or moving parts. This solid state drive can be installed in the computer or can be a smaller device such as a flash drive.
- **External hot-swappable drive:** You may boot from an external hard drive that can be moved between computers without turning it off.
- **Network boot:** You can boot an operating system directly from a local area network (LAN) without using a storage device. Your computer must be connected to a LAN for this option. The network boot is used when the computer does not have an OS installed, among other things. To boot from a network, you will need to set up the Preboot Execution Environment (PXE) capability on the BIOS and have the network environment prepared for this type of request (see resources linked below).
- **Internet-based boot:** You boot the computer from an internet source, as long as it is a secure source. If you are in charge of a network and your server is down for any reason, you can use this boot method to remotely power on the server and restart network operations. Internet-based boot can be achieved in one of two ways:

1. Remote access. Remote Access Controller (IPMI or similar) has to be enabled on the BIOS and the computer needs to have a Remote access control device, such as IDRAC (see resources linked below).
2. Wake on LAN (WoL). This process requires the WoL option enabled on the BIOS (see resources linked below). The WoL instruction should come from a device in the network or use a WoL gateway, and the network card should have WoL capability.

- Windows environments: batch scripts (.bat), Powershell (.ps1), Visual Basic Script (.vbs)
- Linux/Unix environments: shell scripts (.sh)
- Most OS environments: javascript (.js), Python (.py)
  Scripts have multiple helpful uses, such as:

- Basic Automation
- Restarting Machines
- Remapping Network Drives
- Installing Applications
- Automating Backups
- Gathering of information/ data
- Initiating Updates
  There are risks in using scripts, including:

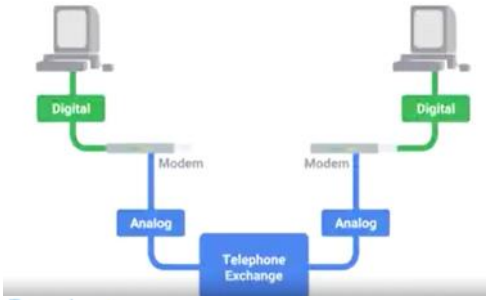
- Unintentionally introducing malware
- Inadvertently changing system settings
- Browser or system crashes due to mishandling of resources

The assembly languagaes used programming lie take this variable from this register and add it to another register like

Reverse proxy

A service that might appear to be a single server to external clients, but actually represents many servers living behind it

A dial-up connection uses POTS for data transfer, and gets its name because the connection is established by actually dialing a phone number.



Baud rate

A measurement of how many bits can be passed across a phone line in a second

Netcat command to see if the port is able to connect

nc google.com 80(will blink in the cursor if succeeds)

-z (zero i/o mode)
-v (verbose)

Test-Netconnection google.com -port 80

Windows:
Select-String string filename/filenameswithwildcards
(gives the files with that character in it)

Computer management application for seeing and managing users and groups in windows
Here it will contain task scheduler(shurdown at 6pm),event viewer(logs),shared folders,users,groups
CLI: Get-LocalGroup,Get-LocalUser
Get-LocalGroupMember Administrators (lists users on that group)

Net user username "password"
Net user username *(asks passwd in the below linux like one)
Net user adrea * /add(adds user)(/del to delete)
Remove-LocalUser adrea
Icacls foldername(see permissions on that folder)
Icacls /?(for help in the command)
Icacls U:/USER/DESKTOP /grant 'Everyone:(OI)(CI)®'
'Authenticated Users:'

Linux:
Sudo su - (goes to the root so don't need to specify sudo for each)
Sudo cat /etc/sudoers

Sudo cat /etc/group (lists users with access showing the group and its encrypted password group id and user)

Sudo cat /etc/passwd(lists users)
Passwd username(to change the password)

When you set a password it's securely scrambled, then stored in a special privileged file called /etc/shadow.

Sudo passwd -e victor(expire the password for victor)

Sudo useradd juan(add user)
Sudo userdel juan

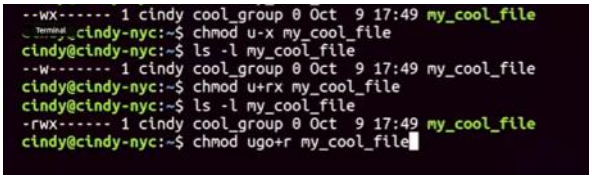
Ls -l ~/fiel(list permissions)
-rwr-rwr--(first - represents directory of file indicated with d for directory, first tri is for permission for owner of the file , second one for group,thrid one for all users)

```
cindy@cindy-nyc:~$ ls -l ~/my_file
-rwxrw-r-- 1 cindy cool group 0 Oct  9 17:48 /home/cindy/my_file
cindy@cindy-nyc:~$
```

```
cindy@cindy-nyc:~$ ls -l my_cool_file
--w------- 1 cindy cool_group 0 Oct  9 17:49 my_cool_file
cindy@cindy-nyc:~$ chmod u+x my_cool_file
cindy@cindy-nyc:~$ ls -l my_cool-file
ls: cannot access 'my_cool-file': No such file or directory
cindy@cindy-nyc:~$ ls -l my_cool_file
--wx------ 1 cindy cool_group 0 Oct  9 17:49 my_cool_file
cindy@cindy-nyc:~$ chmod u-x my_cool_file
cindy@cindy-nyc:~$ ls -l my_cool_file
--w------- 1 cindy cool_group 0 Oct  9 17:49 my_cool_file
cindy@cindy-nyc:~$ chmod u+rx my_cool_file
```

The numerical equivalent of rwx is:

- 4 for read or r
- 2 for write or w



- 4 for read or r
- 2 for write or w
- 1 for execute or x

u-user,g-group,o-allusers
Sudo chown devan filename(to own the file)
Sudo chgrp newgroupname filename(to change the group)

special permission bit is used to allow a file to be run as the owner of the file SetUID (u+s)

Microsoft install package (.msi)

Used to guide a program called the Windows Installer in the installation, maintenance, and removal of programs on the Windows operating system

These .msi files are contained within a portable executable (PE), which is a format specific to Windows. The file type extension for a PE is .exe. Although these PEs commonly include instructions for the computer to run, such as the .msi files, they may also have images that the program may run or computer code

Software installation package, update package, or hotfix package created with the Microsoft Self-Extractor, can be executed using the following command lines:

- **/extract:[path]**: Extracts the content of the package to the path folder. If a path isn't specified, then a Browse dialog box appears.
- **/log:[path to log file]**: Enables verbose logging (more detailed information recorded in the log file) for the update installation.
- **/lang:lcid**: Sets the user interface to the specified locale when multiple locales are available in the package.
- **/quiet**: Runs the package in silent mode.
- **/passive**: Runs the update without any interaction from the user.
- **/norestart**: Prevents prompting of the user when a restart of the computer is needed.
- **/forcerestart**: Forces a restart of the computer as soon as the update is finished.
  You can always type **/?**, **/h**, or **/help** from the command line to view these options.

Installing debian package:
(Linux)
Sudo dpkg -i atom-amd64.deb
-r (remove)
-l (lists)

Compress-Archive -Path sourcepath targetfilepath
Tz e archive.tar(to extract)

In windows for a application dll files serves like the external dependencies packaged for reuselike for graphics one dll and for video rendering another dll

Find-Package sysinternals -IncludeDependencies(finds in the system whether this package is available)

Register-PackageSource -Name chocolatey -ProvideName Chocolatey -Location http://chocolatey.org/api/v2
Get-PackageSource
Get-Package -Name pkgname
Install-Package -name pkgname
Uninstall-Package -Name name

Sudo apt install/remove name

Dynamic link library (DLL)

Windows DLL files are vital to the core functions of the Windows operating system (OS). Some Windows-compatible applications also use DLL files to function. DLLs are made up of programming modules that contain reusable code. Multiple applications can use and reuse the same DLL files. For example, the Comdlg32 DLL file is used by many applications to provide Windows dialog box functions. The reusable feature helps Windows conserve disk space and use RAM more efficiently, which improves the operating speed of the OS and applications. The modular structure also makes updating a DLL file fast and simple, eliminating the need to update the entire library. DLL updates are installed once for use by any number of applications.

A few common DLLs used by Windows include:

- **.drv files** - Device drivers manage the operation of physical devices such as printers.
- **.ocx files** - Active X controls provide controls like the program object for selecting a date from a calendar.
- **.cpl files** - Control panel files manage each of the functions found in the Windows Control Panel.
  An application can use DLLs to load parts of the app as modules. This means that if the application offers multiple functions, the app can selectively load only the modules that offer the functionality requested by the user. For example, if a user does not access the Print function within an application, then the printer driver DLL file does not need to be loaded into memory. This system requires less RAM to hold the application in working memory, which improves operating speeds.

Side-by-side assemblies

DLLs and dependencies can also be located in side-by-side assemblies. A side-by-side assembly is a public or private resource collection that is available to applications during run time. Side-by-side assemblies contain XML files called manifests. The manifests contain data similar to the configuration settings and other data that applications traditionally stored in the Windows registry. Instead of registering this data in the Windows registry, the applications store shared side-by-side assembly manifests in the WinSxS folder of the computer. Private manifests are stored inside the application's folder or they can be embedded in an application or assembly. The metadata of a manifest may include:

The repository source file in Ubuntu is /etc/apt/sources.list.

Here sometimes we need to add the source externally for some installation to work

Using a Personal Package Archive (PPA), you can distribute software and updates directly to Ubuntu users. Create your source package, upload it and Launchpad will build binaries and then host them in your own apt repository.

That means Ubuntu users can install your packages in just the same way they install standard Ubuntu packages and they'll automatically receive updates as and when you make them.

Orca.exe is a database table editor for creating and editing Windows Installer packages and merge modules. The tool provides a graphical interface for validation, highlighting the particular entries where validation errors or warnings occur.

LINUX:

Character devices

Like a keyboard or a mouse, transmit data character by character

Block devices

Like USB drives, hard drives and CDROMs, transfer blocks of data; a data block is just a unit of data storage

If we have ls -l cmd then in the starting it will indicate c or b to say it is character or block devices

- /dev/sda
- /dev/sdb
- /dev/sdc

- **/dev/sda** - First SCSI drive
- **/dev/sr0** - First optical disk drive
- **/dev/usb** - USB device
- **/dev/usbhid** - USB mouse
- **/dev/usb/lp0** - USB printer
- **/dev/null** - discard

Some of the Linux device categories include:

- **Block devices:** Devices that can hold data, such as hard drives, USB drives, and filesystems.
- **Character devices:** Devices that input or output data one character at a time, such as keyboards, monitors, and printers.
- **Pipe devices:** Similar to character devices. However, pipe devices send output to a process running on the Linux machine instead of a monitor or printer.
- **Socket devices:** Similar to pipe devices. However, socket devices help multiple processes communicate with each other.

lpadmin -p printername -m driverfilename.ppd

- **Lpadmin** is the printer administrator command.
- The **-p printername** command adds or modifies the named printer.
- The **-m driverfilename.ppd** command installs the postscript printer description (PPD) driver filename that you provide. The file should be stored in the **/usr/share/cups/model/** directory.
- Enter **$ man lpadmin** to open the manual for the lpadmin command to find additional command line options.

- **$ ls /dev** - Lists all devices in the /dev folder
- **$ lscpci** - Lists devices installed on the PCI bus
- **$ lsusb** - Lists devices installed on the USB bus
- **$ lsscsi** - Lists SCSI devices, such as hard drives
- **$ lpstat -p** - Lists all printers and whether they are enabled
- **$ dmesg** - Lists devices recognized by the kernel

Uname -r(see the kernel version we have)
Sudo apt full-upgrade(installs a new kernel version if available)

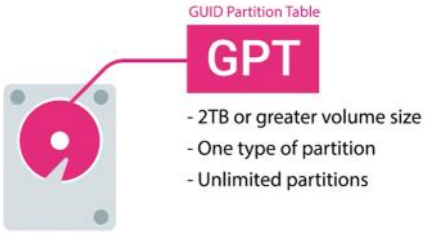
Sysinternals package: A set of tools released by Microsoft that can help you troubleshoot

Filesystems recommended:

Ntfs usb can be transferred to ntfs,ext4 but ext4 usb can only be transferred to ubuntu not windows

Traditional partitioning table schemes:

- Master Boot Record (MBR)
- GUID Partition Table (GPT)



For UEFI BIOS the partition table should be GPT

Then **allocation unit size** when formatting the external storage means the how much amount of blocks to use like for large files if we want fast read and we specify large unit size only fewer blocks need to be read

In windows cli:
C:\Users\system32>Diskpart
DISKPART> list disk
DISKPART> select disk 1
DISKPART>clean
DISKPART>create partition primary
DISKPART>select partition 1
DISKPART>active
DISKPART>format FS=NTFS label-my-thumb-drive quick

Mounting

Making something accessible to the computer, like a filesystem or a hard disk

LINUX:
Sudo parted -l (lists disks connected)
(in the list Disk name will be shown and the partition listed with paritiotn number which means /dev/sdb1,/dev/sdb2 etc..)
Sudo parted /dev/sdb
..
..
(parted) mklabel gpt
(parted) print
..
(parted) mkpart primary ext4 1MiB 5iG
..
(parted) quit

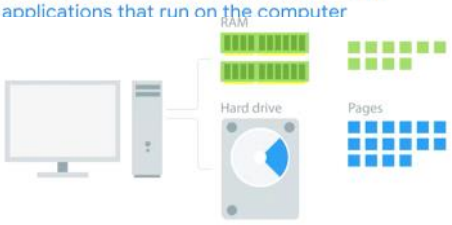
Sudo mkfs -t ext4 /dev/sdb1
Sudo mount /dev/sdb1 /my_usb/
Sudo unmount /dev/sdb1

Sudo cat /etc/fstab (File system table) (contaisn entries like file system, mount point, tpe,etc.. And we can entry here if we want)

Sudo blkid (shows the UUID,type,partuuid for all disks)

Virtual memory

How our OS provides the physical memory available in our computer (like RAM) to the applications that run on the computer

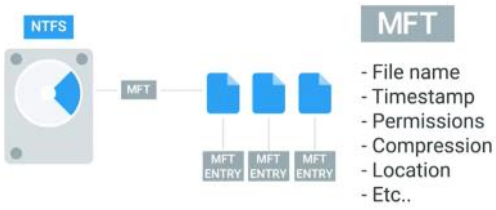


A paging file is an optional tool that uses hard drive space to supplement a system's RAM capacity. The paging file offloads data from RAM that has not been used recently by the system. Paging files can also be used for system crash dumps or to extend the system commit charge when the computer is in peak usage. However, paging files may not be necessary in systems with a large amount of RAM.

Swap space

In Linux, the dedicated area of the hard drive used for virtual memory

Sudo mkswap /dev/sdb2
Sudo swapon /dev/sdb2



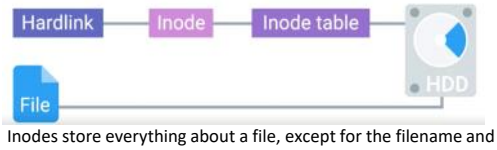
If we create a shortcut for a file when we open it it will be encrypted but we can create symbolic link to link to a file

Mklink file1_symlink file_1.txt(symbolic link) /H for hard link(even if we change the name of original file it will point)

The idea behind disk **defragmentation** is to take all the files stored on a given disk, and reorganize them into neighboring locations.

Disk defragment(which is schedulef automatically regularly) tool in window UI

LINUX:



Inodes store everything about a file, except for the filename and the file data.

Ln -s sourcefile targetfilename(for softlink)
Ln source target(hardlink)

In the ls -l for that file after permissions the number indicates the number of links for that

Du -h (disk usage)
Df -h

Data buffer

A region of RAM that's used to temporarily store data while it's being moved around

So we need to eject the usb drives so that these buffers also gets copied

Using ntfs logs in windows for troubleshooting for corrupted ones

So we need to eject the usb drives so that these buffers also gets copied

Using ntfs logs in windows for troubleshooting for corrupted ones

fsutil repair query C:

Chkdsk /F D:

LINUX:
Sudo fsck /dev/sda(not recommended since it can not guarantee reliability)

WINDOWS:
1- Session manager subsystem(smss.exe)(when os boots up this is started)
2- Client serverruntime subsystem(csrss.exe)(for widnows GUI,CLI)
tasklist /v /fi "PID gt 1000" /fo csv(To list all tasks with a process ID greater than 1000, and display them in csv format)
tasklist /v /fi "STATUS eq running"
Tasklist(Get-Process in powershell,taskmanager in GUI))
Taskkill /pid 5856

LINUX:
1- Init (PID:1)
Less /etc/filename | grep Hello

Ps -x(processes)
Ps -ef(processes for all users and full information)

Ls -l /proc (since everything in linux is a directory or file)

Cat /proc/(pid)/status (even more info on the process)

Signals:
- SIGINT(signal interrupt)- ctrl+C

In windows we can also download process exlorer file from windows and execute the given file and see the processes(in this one we can kill process,kill process tree,restart,suspend)
https://learn.microsoft.com/en-us/sysinternals/downloads/process-explorer

LINUX:
Kill (SIGTERM-signal,its like give some time to clean up and kill)
Kill pid

(SIGKILL - it will not give time and kills faster)
Kill -KILL pid

*SIGTSTP (sig termial stop) (Ctrl+Z)
Kill -TSTP pid

SIGCONT (continue suspended one
Kill -CONT pid

WINDOWS:
Resource monitor app to check the resource utilizations

Get-Process | Sort CPU -descending | Select -first 3 -Property ID ProcessName CPU

LINUX:
Top (top processes using more resourcwes)

Uptime (system uptime ,user logged in load)

Lsof (tracking down proesses)

In linux we can use scp command
In windows we can use **pscp.exe source target**
Net share ShareMe=C:\Users\cindy\Desktop\ShareMe /grant:everyone full

Event viewer in windows stores all the events/logs in os
Eventvmr.msc in windows+R

In linux in /var/log all the logs are stored
$ sudo apt-get update
$ sudo apt-get install -y logrotate
We create a file that says which log should be rotated

compress

```
/var/log/nginx/* {
   rotate 3
   daily
}

/var/log/nginx/error.log {
   rotate 3
   size 1M
   lastaction
      /usr/bin/killall -HUP nginx
   endscript
   nocompress
} #/etc/logrotate.conf
$ logrotate log-rotation.conf
$ logrotate -f log-rotation.conf  (-f to evaluate)
```

Tail -f /var/log/syslog (to see in realtime)

OS deployment methods:

Disk cloning

Tools: NinjaOne Backup,EaseUS Todo Backup etc..

LINUX:

- Unmount /dev/sdd
- Dd if=/dev/sdd of=~/Desktop/myusb-image.img bs=100M

We can use this cloned disk image to deploy os

PART 4,5

Tuesday, April 4, 2023 3:44 PM

A **KVM switch** (with KVM being an abbreviation for "keyboard, video, and mouse") is a hardware device that allows a user to control multiple computers from one or more[1] sets of keyboards, video monitors, and mice.

Linux:
Service ntp status
Configuration files for installed services are located in the /etc directory
Example configuraiton:
Sudo apt install vsftpd (stored In /etc/vsftpd.conf)
Lftp(client) localhost (try connecting to localhost)
Edit the conf and set anonymous access to YES to test
Reload to revisit the config for the service
Sudo service vsftpd reload

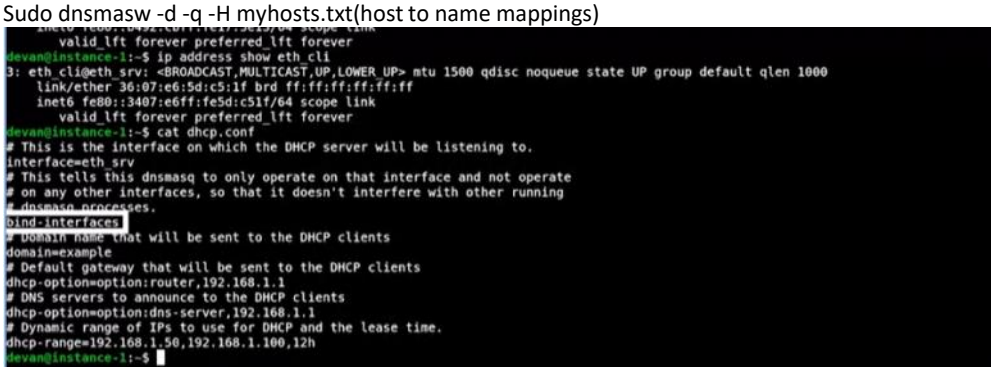
dnsmasq

A program that provides DNS, DHCP, TFTP and PXE services in a simple package

Sudo apt install dnsmasq
Dig(query dns servers and check) www.example.com @localhost(localhost is the dns server in the dnsmasq)

To run the dnsmasq in debug mode (sudo dnsmasq -d -q (it will stream outputs))

Sudo dnsmasw -d -q -H myhosts.txt(host to name mappings)



Windows:
Get-Service wuauserv(windows update service)
Get-Service wuauserv |Format-List *(more info)
Stop-Service svcname
Start-Service
Get-Service

Control panel -> Turn windows features on and off- > Server manager -> it will lead to setting up server available and we need to pick it up -> install it in windows instance

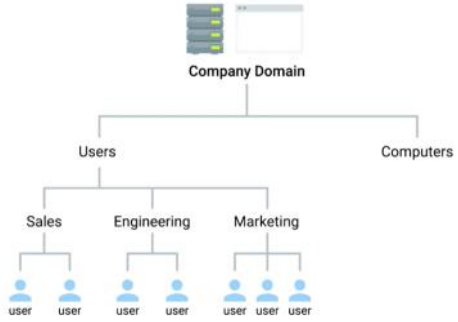
We can paste the html page we have in inetpub directory if we enable webserver IIS as a directory

EMAIL PROTOCOLS:
POP3:(post officeprotocol)
It can be only seen through one device and the email gets deleted form the email server once viewed
IMAP(Internet message access protocol):
Access to multiple devices

SMTP(simple mail transfer protocol):
Other protocols only for retriving email but this one is for sending email also

PRINT SERVICES:
In linux CUPS is a service that we can use for managing pritners and in windows we can go to that features add on where we enabled IIS server we can enable print servicdees in there

DIRECTORY SERVICES:



Each one in the diagram is a Organization unit(OU)

Directory Access protocol(DAP)
Directory system protocol(DSP)
Directory Information shadowing protocol(DISP)
Directory Operational Bindings Managedment protocol(DOP)

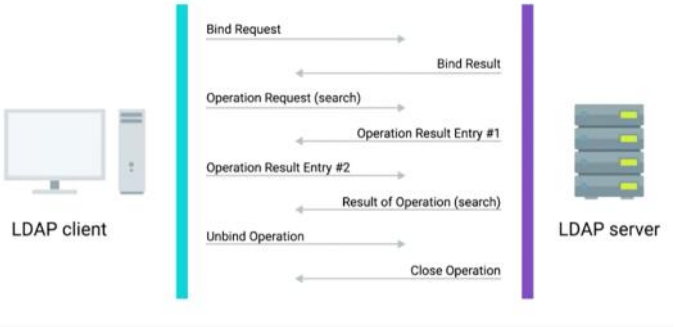
Lightweight Directory access protocol(LDAP)

Directory entry example:

Dn:CN=Devan Sri-Tharan,OU=Sysadmin,DC=example,DC=com

Dn=distinguished name
CN=common name
OU=organizational unit
DC=domain component

Bind operation=> authenticates clients to the directory server



Authentication ways:
- Anonymous
- Simple
- SASL(simple authentication & security Layer)(TLS)

Kerberos

A network authentication protocol that's used to authenticate user identity, secure the transfer of user credentials, and more

Active Directory Administrative Center (ADAC)

A tool that we'll use for lots of the everyday tasks

Organizational Unit (OU)

A folder or directory for organizing objects within a centralized management system

A forest can contain one or more domains and accounts can share resources between domains in the same forest

Domain controllers keeps the copy of the directory db,provide dns resolutions etc..

Security group

Can contain user accounts, computer accounts or other security groups

Distribution group

Only designed to group accounts and contacts for email communication

You can't use distribution groups for assigning permission to resources

Need to brush up good things for active directories

Steganagraphy is to hide the original message in other meesaages like message in a aphoto

Here is one list
"

CISCO CCNA
AZURE
AWS SOLUTION ARCHITECT COURSE
AWS MLS
AZURE VIRTUAL DESKTOP
GOOGLE IT SUPPORT
RHCSA
GCP PCA
CKA(kubernetes administrator)
GCP NETWORK
KUBERNETES
GCP PDE
REACT FULL STACK
ETHICAL HACKING UDEMY
GCP ML
GCP DEVOPS
GCP ACE
TERRAFORM

New Section 1

"

Here is another list

"

REACT FULL STACK
KUBERNETES
GCP PDE
GCP NETWORK,SECURITY
CKA(kubernetes administrator)
GCP PCA
RHCSA
GOOGLE IT SUPPORT
AZURE VIRTUAL DESKTOP
AWS MLS
AWS SOLUTION ARCHITECT COU..
CISCO CCNA
AZURE

"

Give me the remaining values in list 2 which is in list1 and missing in the list2