Course (Unofficial workshop): CompTIA IT Fundamentals+ Preparation
Institution: Irvine Valley College
Professor: Michael Franklin
Semester: Spring 2019
Note compiled by: Bian Lee

Table of Contents

1. IT Concepts and Terminology

- Decimal: Number system that has a base of 10
- Binary: Number system with a base of 2
    - Can only be 0s and 1s
- Bits and bytes: Measurements of binary data
    - Byte (B) = 8 bits
    - Kilobyte (KB) = 1024 bytes (10^3) bytes
    - Megabyte (MB) = 1024 KB (10^6) bytes
    - Gigabyte (GB) = 1024 MB (10^9) bytes
    - Terabyte (TB) = 1024 GB (10^{12}) bytes
    - Petabyte (PB) = 1024 TB (10^{15}) bytes
    - Exabyte (EB) = 1024 EB (10^{16}) bytes
- Hexadecimal: Number system with a base of 16. Has letters in them
    - 0000 → 0, 0001 → 1, 0010 → 2, 0011 → 3, 0100 → 4, 0101 → 5, 0110 → 6, 0111 → 7, 1000 → 8, 1001 → 9, 1010 → A, 1011 → B, 1100 → C, 1101 → D, 1110 → E, 1111 → F
- ASCII (American Standard Code for Information Exchange)
    - 8-bit character that can define 96 uppercase and lowercase letters and 32 other characters
    - Provides uniformity between the computer and peripheral devices such as printers in exchanging texts
    - Differs from Unicode, which has over thousands of characters, including foreign language (besides english) and even emojis
- Unicode
    - Another standard for representing characters. These characters are uniform on any computer platform. Unlike ASCII which is only represented in English, Unicode is uniform across most languages in addition to English.
- Data types
    - Char: Consists of a single character
    - String: Consists of multiple characters

    - Integer (int): A whole number
    - Float & Double: A number with a decimal point
    - Boolean: Truth table options, can only be true or false
- Input
    - Method of entering data into the computer
    - Keyboard, mouse, microphone
- Processing:
    - How computer interprets data that has been inputted
    - Converts data into machine-readable form
    - Processing primarily occurs in the CPU, known as the Central Processing Unit
    - Includes defined operations on data
    - CPU performs arithmetic and logical operations (ALU) as well as directing data, which happens inside the Control Unit
- Output
    - End result of the processing portion.
    - Monitor, speakers, printers
- Storage
    - Hardware used to store data for the end user
    - Can hold information temporarily and/or permanently
    - Hard drive (HDD), USB Flash drive, Solid State Drive (SSD)
- RAM vs Hard Drive
    - RAM: Volatile, temporary, primary and dynamic
    - Hard Drive: Non-volatile, permanent, secondary and static
- Throughput
    - Speed of data transfer (bandwidth) is measured by bits per second
    - Internet Service Provider (ISP) controls and maintains the internet connections between house and global internet
    - Average bandwidth in the US → 100Mb/s
    - https://speedtest.net
- Processing Speed
    - Also known as clock speed or internal speed, processing speed refers to how quickly data can be processed in the processor (CPU)
    - 1 cycle/second is equivalent to 1 hertz. The speed of internal components are classified to be Megahertz (MHz) or Gigahertz (GHz)
    - More RAM = faster speed of your computer
- Troubleshooting Methodology
    - 1. Identify a problem
        - Collect as much information about the problem as possible
        - Listen to what the user is saying
        - Understanding what the user describes as the problem is beneficial to learning potential fixes to the problem
    - 2. Research knowledge base/internet
        - With the new information, check previous reports to see if others have come across the same problem

        - Search through search engines, and online forums
        - User open-source intelligence techniques to find deeper, publicly available information
    - 3. Establish a theory of probable cause
        - Come up with a theory that may potentially be causing the issue
    - 4. Test the theory to determine the cause
        - Continue making theories and testing them to understand the cause of the problem
    - 5. Establish a plan of action to resolve the problem and identify potential effects
        - This may prove useful if the solution affects more than one user
    - 6. Implement the solution or escalate as necessary
        - If the solution is within your scope of expertise, implement the solution
        - If it requires a person of high authority or knowledge, escalate the problem to the appropriate person/department
    - 7. Verify full system functionality and implement preventative measures
        - It's important that after the solution has been implemented, the system is thoroughly tested
        - May involve checking all devices that were affected in the process of solving the problem
        - There is nothing worse than having what is thought to be a new problem, when it's simply problem that was caused by a previously implemented solution
    - 8. Document finds/lessons learned, actions, and outcomes
        - Each time you succeed or fail at a possible solution, document it to understand what you have done
        - Knowledge base refers to these collection of documents

2. Infrastructure

- Interface
    - Types of connections a computer will use to connect to input or output devices
    - An input device is used by users to send data to the computer, while an output device will receive data from the computer and output it out in a desired way
    - Network interface refers to how a device connects to a network. There are two types: wired and wireless
    - The term Interface can refer to either a hardware connection or a user interface. Or, it can also be used as a verb to describe how two devices connect to each other
    - However, it is not to be confused with "interface" in object oriented programming, that refers to abstract type that is used to specify a behavior that classes must implement
- Wired Network Interfaces (2 wired interfaces that are being used today)
    - RJ (Registered Jack) 11: Used for connecting telephone wires, and it is smaller in size
    - RJ (Registered Jack) 45: Used with ethernet cable, and it is larger
- Wireless Interfaces (see below for detailed description)
    - Bluetooth

    - Radio-Frequency Identification
    - Near-field Communication

- Bluetooth
    - Short range interface that can extend for a few feet (depending on the antenna)
    - Peripheral devices such as keyboards and mice can connect via USB or through Bluetooth
    - Process of connecting bluetooth devices is called pairing
    - The peripheral device you are connecting would go into a state called “Discoverable” mode as it broadcasts to pair
    - These pair require an authentication method such as confirming on the end device or by entering PIN code (to ensure one doesn’t randomly connect to an unintended device)
- Radio Frequency (RF)
    - Range of electromagnetic frequencies between 10 kHz - 300 GHz
    - RF has a range of up to 2 meters
    - Devices that use the same wavelength may conflict with each other
    - Example of device that uses RF: Wireless garage door opener
- Near Field Communication (NFC)
    - Offshoot of radio frequency (RF)
    - Designed for close proximity communication between devices within only a few inches apart
    - Can be used for badge / ID scanning, mobile pay, etc
- Universal Serial Bus (USB)
    - The most commonly used device interface in the world
    - Universal, meaning they have the capability to be used anywhere for almost anything
    - Latest model: USB 3.2, which has the ability to provide power, video/audio, other data
    - Generation 1: 9.8ft (max cable length); 12 Mb/s (speed)
    - Generation 2: 16.4ft; 480 Mb/s
    - Generation 3: 9,8 ft; 5 Gbps
    - Generation 3.1: 9.8ft; 10 Gbps
    - Generation 3.2: 3.3ft; Up to 20 Gbps
- Firewire
    - Developed by Apple in the late 80s to compete against USB
    - Primarily used for digital audio and video
    - Firewire 400: 400 Mbps (speed)
    - Firewire 800: 800 Mbps
- Thunderbolt
    - Developed by Intel with Apple in 2009 to replace Firewire
    - Supports USB-C, DisplayPort (Thunderbolt 2 port and Mini DisplayPort are identical, and so are the Thunderbolt 3 and USB-C)
    - Provides up to 100W of power at high speed
    - Thunderbolt: 10 Gbps (speed)
    - Thunderbolt 2: 20 Gbps
    - Thunderbolt 3: 40 Gbps

- Graphic Device Interfaces
    - Due to high usage, video has a dedicated interface that consists of an application programming interface (API) to display graphics and formatted text on video display and printer
    - Hardware devices include: VGA, HDMI, DVI, DisplayPort, Mini DisplayPort
- Video Graphics Array (VGA)
    - Introduced by IBM in 1987
    - Uses analog signal
    - Developed for 640 x 480 resolution (quite low)
- Digital Visual Interface (DVI)
    - Introduced by Digital Display Working Group (DDWG)
    - First to have digital signal
    - Designed for 1900 x 1200 resolution
- HDMI (High Definition Multimedia Interface)
    - Introduced by Hitachi, Panasonic, Philips, Silicon Image, Sony, Thomson, RCA, and Toshiba in 2002
    - More powerful digital signal
    - High definition video with audio
- DisplayPort
    - Introduced by VESA in 2008
    - Uses digital signal
    - High definition video and audio (but designed primarily for video as audio is transferred with low priority)
    - It can also carry audio, USB and other forms of data
- Mini DisplayPort
    - Developed by Apple using a license from VESA, for the Macbook Pro
    - Same properties as DisplayPort
- Device Configurations (see below for detailed description on each)
    - Plug-and-Play (PnP)
    - Driver Installation
    - Custom Configurations
    - IP-based Peripherals
    - Web-based Configuration
- Plug-and-Play (PnP)
    - Requires no additional action from the user (user literally “plugs” in the device to use)
    - Device that use PnP utilizes the operating system’s default device driver, meaning no special driver would be needed to use the device
    - Computer would automatically recognize the device without external verification or additional software
    - Examples: Video card, hard drive, USB (or other flash drives), keyboard, etc
- Driver Installation
    - For special devices that require additional resources that the default drivers on the operating system cannot provide, it’s required to install driver, piece of software that the

manufacturer provides in order to allow your computer to communicate with connected device
    - Devices such as a mouse and keyboard would work on default drivers, but specific drivers would be needed if you would like additional functions such as configuring the RGB on them.
    - These drivers would come packaged in a CD or on the manufacturer's website in the Support Section
- IP-based Peripherals
    - These devices can be configured through the network rather than directly on your computer. These devices usually ask you to connect via their own WiFi broadcast or IP address.
    - These devices can be accessed by anyone on the same network.
    - Printers can also be considered IP-based peripherals, since it can be configured by typing its IP address (printer has a unique IP address itself), and multiple computers can connect to a single printer
- Web-based Configuration
    - This type of installation runs through a web browser such as Firefox or Chrome. The devices that host web-based configurations have built-in web servers that broadcast HTTP/S signals for communication.
- Motherboard
    - Hub that connects all of your other internal components together
    - Biggest internal component of the computer.
    - Each motherboard has a collection of chips and controllers that make up the chipset. These chipsets allow efficient and fast communication between the CPU and the rest of the computer
    - Form Factors
        - Mini ATX ATX
        - Advanced Technology eXtended
        - Micro ATX
- Firmware/BIOS
    - Short for Basic Input/Output System.
    - The BIOS is the foundation of which the computer communicates between the hardware and the software of the computer. At boot, the BIOS runs a hardware check to ensure all the components are operational.
    - Allows Dual-booting (two OS on one computer; selected when booting) or Operating System Booting from a Bootable Flash Drive
    - To enter into BIOS, press F10, F2, F12, F1, or DEL before booting into an OS
- RAM (Random Access Memory)
    - Random Access Memory is a temporary storage space for the operating system to utilize during operation. Each program you open on the computer uses the RAM as a temporary storage device to allow for quicker speed.
    - The are volatile, and temporary, in contrast to hard drive (HDD) or solid state drive (SSD)
- Internal Storage

    - Hard Drive Disk: Non-volatile devices that permanently stores and retrieves data using a magnetic head.
    - Solid State Disk: Non-volatile device that uses no mechanical moving parts. This allows it to be faster and more reliable.
    - SSD M.2: The M.2 is a variation of the SSD, but the form factor is significantly smaller. With its compression, it allows for an even faster speed with a higher efficiency rate. Due to the size and speed, these devices heat a lot quicker than the others
- Graphics Process Unit (GPU)
    - GPUs assist in the creation of 2D and 3D images. They can be either integrated in the CPU or a dedicated card. A dedicated card allows the CPU to focus on non-graphical tasks.
- Cooling Devices
    - Fans are used for air cooling the computer. This is the safest way to cool a computer.
    - Heat sinks are transfer cooling devices that draw the heat away from the component into a larger surface area
    - Liquid Cooling utilizes water or specialized coolant that is pumped throughout the computer. This is the most risky way to cool a computer due to leaks, but it is the most effective compared to the others.
- Network Interface Card (NIC)
    - NICs allow the computer to connect to the network. This is the card that contains either an ethernet port or antennas for wireless
- Internet Service Types (see below for detailed description on each)
    - Coax Cables
    - Digital Subscriber Line (DSL)
    - Fiber Optic
    - Wireless
        - Radio Frequency (RF)
        - Satellite
        - Cellular
- Coax Cable
    - Primarily used for video and audio communication (but also carry data as well)
    - This cable directly plugs into cable modem
- Digital Subscriber Line (DSL)
    - Sends internet data through telephone lines.
    - These speeds tend to cap out at 30Mbps.
    - Although it is slower than cable, it is still one of the most popular, widely-used Internet Service today
- Fiber Optics
    - Fibers of glass coated with plastic that carry data through pulses of light.
    - Although these types of cables are primarily seen in corporate or world-wide networks, there has been movement to move fiber optic onto the consumer industry.
- Radio Frequency (RF)
    - A tower would broadcast a signal and the consumer would need to have an antenna and receiver.

    - This is still a new technology and is not seen in the market yet
- Satellite
    - Out of all the types of wireless connectivity, it offers the most latency and obstacles.
    - High latency can range from 250 to 300 milliseconds due to signal travel.
    - Weather must be clear in order for a stable connection to be established
- Cellular
    - Primarily used for modules and mobile devices.
    - This connection type utilizes a cellular tower to communicate.
    - There are 2 standards that are used. Global System for Mobile Communication (GSM; used by AT&T, T-Mobile) and Code Division Multiple Access (CDMA; Used by Spring and Verizon)
    - They can connect to the internet anywhere there is a tower and this service is more expensive than the others

3. Applications & Software

- Network Storages
    - NAS (Network-Attached Storage): These are drives that are attached to the network via USB into the router or by ethernet. Anyone on the network can access the drive.
    - A File server: Server dedicated to host files that can operate programs within it as well. Compared to a NAS, a file server has computational power.
    - Cloud storage: Network of file servers connected to provide storage capabilities through a remote connection. Instead of having data stored physically on your device, the data is saved remotely on what is referred to as the “cloud”
- Mobile Phones & Tablets & Laptops
    - Mobile Phone: Referred to as the cell. It allows a user to communicate almost anywhere in the world due to the massive cellular network. Motorola was the one who invented the first cellular phone by Martin Cooper.
    - Tablets: A tablet is a larger mobile device that has similar capabilities as a mobile phone. The concept of the tablet was sketched by Alan Kay at Xerox in 1971, but the first successful tablet was the Apple iPad released in 2010.
    - Laptop: Also known as the notebook. A laptop is a portable computer that contains most of the capabilities as a desktop computer. Laptops contain NiMH, NiCad, or Li-ion battery packs to function with mobility.
- Workstations
    - dedicated computer designed for the work environment. These workstations tend to be a smaller form factor to fit on or near the desk. Workstations can range from a high performance PC to a lower performance PC depending on the work that is required.
    - It generally has greater power than a desktop computer, as it can handle more complex tasks such as CAD (Computer Aided Design), Animation, Data analysis, and photorealistic renderings, and other works that require much more processing.
- Servers

    - High performance computer that is meant to manage network communications. Network services that servers manage can include email, DNS (Domain Name System), FTP (File Transfer Protocol), and Web servers (for holding web applications.
    - DNS (Domain Name System) Translates domain names of websites to IP addresses so browsers can load internet resources and clients can connect to web servers holding the data.
    - FTP is used to transfer files between computers on a network, and uses SSL (Secure Socket Layer) or TLS (Transport Layer Security) encryption to encrypt the data that's being transferred back and forth.
- Gaming Consoles
    - Gaming Consoles are dedicated computers that specialize in processing video games. They connect to the internet, meaning they could just as well be hacked.
- IoT (Internet Of Things)
    - Devices are devices that have a separate function, but with an added internet capability.
    - Have the ability to transfer data over a network without requiring human-to-human or human-to-computer interaction.
    - They have their own operating system that's different from OS on desktop computers or mobile devices, and usually run on programming languages such as C (widely used for applications or operating systems), C++ (general-purpose) or Java (general purpose; write once, run anywhere).
    - Examples: Smart TV, Toys (with internet capability), Amazon's Smart Microwaves, Smart Fridge, and other "smart" appliances.
- Packet Transmission
    - Packet: Package of data that has been compressed for transfer. Data is divided into multiple packets to allow quick transfers. Inside a packet is a source, destination, data, size and other information to help it reach its destination.
    - Cisco's packet tracer software allows users to create computer networks and simulate the configuration of Cisco routers and switches.
- Local Area Network (LAN)
    - Small area network that is composed of computers that are in close proximity to each other. A LAN would be a network of computers in a computer lab or inside a college.
    - Internet is a connection of millions of LANs, and the concept of LAN came before World Wide Web
- WAN (Wide Area Network)
    - Wide Area Network (WAN) is a collection of LAN networks that comprise a geological area. These are essentially large LANs that connect together to form the Internet.
- Device Addresses
    - IP Addresses are the network addresses of the device on a network.
        - IPv4 uses a 32-bit long sequence (4 billion possible addresses. This is 2 to the 32nd power)
        - IPv6 uses a 128-bit long sequence. (much more possible addresses) IPv6 is more recent, and constantly being used widely in regions with few IP addresses left.

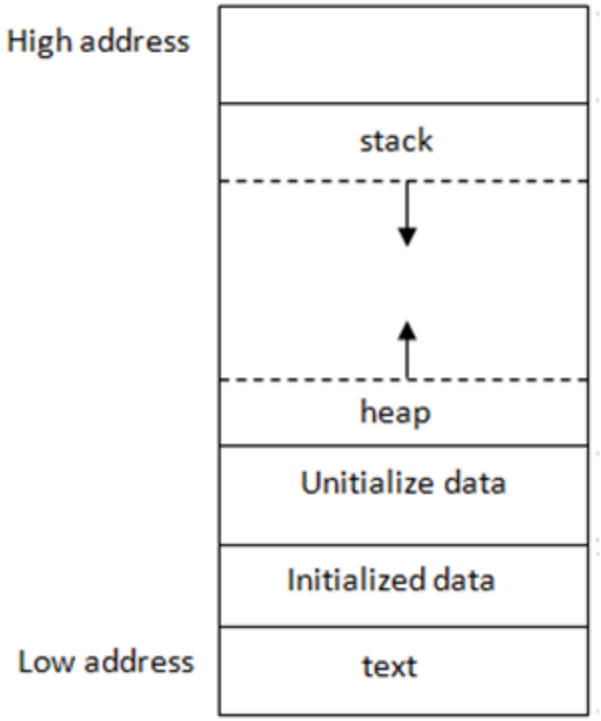
    - MAC addresses: Physical device address which is encoded when the device is created. This is directly encoded into the hardware and cannot be changed without expertise. No device has the same MAC address.
- HTTP vs HTTPS
    - HTTP is the protocol that allows for web communication (web browsers to communicate on the internet)
    - HTTPS is the secure version of HTTP. HTTPS is secured through SSL (Secure Socket Layer). HTTPS is recommended for sites that hold sensitive data, such as entering passwords or credit card information.
- Email
    - POP3: Post Office Protocol
        - You can only receive emails through POP.
        - It is most commonly used to receive email on many email clients.
        - There are two different versions of POP; POP2 and POP3. POP2 was an early standard of POP that was only capable of receiving email and required SMTP to send an email. POP3 is the latest standard and can send and receive email using POP.
    - IMAP: Internet Message Access Protocol
        - Retrieves emails from a server.
        - It is a protocol for retrieving email from a server, similar to POP.
        - The secure version of IMAP is called IMAPS, which stands for IMAP over SSL.
    - SMTP: Simple Mail Transfer Protocol
        - Sends emails from server to server.
        - While it is mostly used for the transfer from one mail server to another, some client mail applications use SMTP for relaying messages; whereas receiving happens via POP or IMAP.
- Modem (Short for modulator/demodulator)
    - Hardware device that allows a computer to send and receive information over telephone lines.
    - When sending a signal, the device converts ("modulates") digital data to an analog audio signal, and transmits it over a telephone line. Similarly, when an analog signal is received, the modem converts it back ("demodulates" it) to a digital signal.
- Router
    - Hardware device designed to receive, analyze and move incoming packets to another network. It may also be used to convert the packets to another network interface, drop them, and perform other actions relating to a network.
    - It has more capabilities than other network devices including hub or switch (which can only perform basic network functions). Not only does router transfer data, but it can also analyze it and send it to another network or a different network on its own
- Switch
    - hardware device that filters and forwards network packets, but often not capable of much more. A network switch is more advanced than a hub but not as advanced as a router.
- Access Point

    - Base station and wireless router, an access point is a wireless receiver which enables a user to connect wirelessly to a network or the Internet. This term can refer to both WiFi and Bluetooth devices.
- Firewall
    - Software utility or hardware device that acts as a filter for data entering or leaving a network or computer. A firewall works by blocking or restricting network ports or unknown connections
    - Firewalls are commonly used to help prevent unauthorized access to both company and home networks.
    - It could be used to prevent simple DoS (Denial of Service) attacks. (Although stopping DDoS would be complicated)
- Institute of Electrical and Electronics Engineers (IEEE) 802.11 Standards
    - 802.11a: Capable of transmissions of up to 54 Mbps and operates in the 5 GHz band.
    - 802.11b: Capable of transmissions of up to 11 Mbps and operates in the 2.4 GHz band, divided into 11 channels
    - 802.11g: Capable of transmissions of up to 20 Mbps and operates in the 2.4, 3.6, and 5 GHz bands.
    - 802.11n: Operates using the 2.4 GHz and 5 GHz bandwidths. Utilizes MIMO (multiple-input, multiple output) antennas to improve data transfer speeds.
    - 802.11ac: Operates using the 5 GHz bandwidth. Utilizes MIMO
- Guidelines when setting up wireless networks
    - Change SSID
        - SSID is a 32 alphanumeric identification given to devices on a wireless network.
        - A device wanting to connect to a wireless network with an SSID enabled must have the same SSID to communicate.
        - When connecting to a home network, you may see multiple SSIDs from your neighbor's wireless routers which is why you should make your SSID descriptive to your home.
    - Change default password
        - Most routers with the same manufacturer have a default built-in password, which means that any neighbor with the same router would know your password, until you change them.
    - Define Encrypted or unencrypted security
        - If your network is an open network (unencrypted), anyone close to your router can connect to your network. It is recommended that you use WPA or WPA2 for security schemes (over WEP).
- Operating Systems (OS)
    - Software that provides the direct connection between the end user and computer. At its fundamental foundation is the user interface (often GUI) with which a user can communicate with a computer. Early operating systems were mostly command line utilities
    - Creates a user-friendly environment that enables users to use a computer efficiently without having to know the underlying technologies. Depending upon the version and manufacturer, the features of the user interface and functionality vary

    - Windows, MacOS, Linux, Chrome OS
    - The most common language choice for operating systems is C.
- Windows
    - Graphical User Interface (GUI)
    - Minimum of 32-bit processing, native networking support. Comes with built in applications. Largely pre-installed on personal computers and sold commercially
- MacOS
    - OSX is a Linux derivative (but not open-sourced) and consists of UNIX based operating systems and GUIs.
    - Safari web browser, native TCP/IP networking, network-level security features, hardware device support, etc
- Linux
    - Open-standards UNIX derivative originally developed and released by Linus Torvalds
    - Because the source code is open, it can be downloaded, modified, and installed freely. However, many organizations prefer to purchase and implement a Linux distribution
    - Linux distro is a complete Linux implementation, including kernel, shell, applications, utilities, and installation media, that is packaged, distributed, and supported by a software vendor or group
    - Ubuntu, Fedora, Arch, Debian, Mint, Kali, etc
- Chrome OS
    - Built on the open source Chromium OS, the Chrome operating system was developed by Google as its commercial OS. With manufacturing partners, the Chrome OS is installed on chromebooks
- iOS
    - Base software that allows all other applications to run on an iPhone, iPod touch, or iPad.
    - The iOS user interface supports direct touch, multitouch, and using the accelerometer. Interface control elements consist of switches, buttons, and sliders.
- Android
    - Layered environment built on the Linux kernel foundation that includes not only the operating system, but middleware, which provides additional software for the operating system and additional built-in applications.
    - It supports open-source–developed applications and functions and comes with basic operating system services, message passing, and so on.
- BlackBerry OS
    - Primarily used by professionals to conduct business operations and tasks.
- Windows Phone OS
    - Maintained and developed by Microsoft.
    - Features include a suite of Microsoft Office applications, Outlook Mobile, web browsing, Windows Media Player, and other advanced features.
- Ubuntu Touch
    - Mobile version of the Ubuntu operating system, terminated support in 2017.
- Server OS
    - A server is a network computer that shares resources with and responds to requests from other servers on the network.

    - Servers provide centralized access or resources that can include applications, files, printers, and other hardware as well as services, such as email.
- Embedded OS (Firmware)
    - The Operating System in these devices are usually very hardware specific.
    - It usually cannot be updated like other Operating Systems. The entire software must be removed and replaced by an updated OS.
- Hypervisors
    - Operating System or program that makes it possible to create virtual machines.
    - A virtual machine is a computer with no physical components.
    - Virtualization: Components are files that interface with hypervisors and Operating Systems recognize as physical hardware.
    - In a virtualized environment, it's possible to host multiple logical operating systems (virtual machines).
- Dual Booting
    - Act of installing multiple operating systems on a single computer, and being able to choose which one to boot on BIOS.
- File Extensions
    - OS, such as Microsoft, use file extension to identify the type of file / data. Linux, on the other hand, does not necessarily use file extensions
    - Documents: .txt, .rft, .doc, .docx, .xls, .xlsx, .ppt, .pptx, .pdf
    - Audio: .aac, .flac, .m4a, .mp3, .wav, midi
    - Images: .bmp, .gif, .jpg/jpeg, .png, .tif, .tiff
    - Videos: .avi, .flv, .mp4, .mpg, .mpeg, .wmv
    - Executables: .app, .bat, .com, .exe, .msi, .scexe
    - Compression Formats: .iso, .dmg, .gzip, .gz, .jar, .rar, .7zip, .7z, .tar, .zip
- Basic commands in Linux (run them on terminal / console)
    - cd: Change directory
    - mkdir: Create new directory
    - cat: Display contents of a file
    - chmod: Change the read, write and execute permissions on files and directories
    - ls: List directories and files
    - ls -a: -a flag means "all" so this command would list directories and files including hidden ones
    - pwd: Path of a current working directory
    - cp: Copy files from the current directory to a different directory
    - touch: create a blank new file
    - find: Search for files and directories
- Disk Management
    - Past the BIOS, the operating system maintains the communication to the hardware components to the user. Windows uses the
        - New Technology File System (NTFS)
        - File Allocation Table (FAT)
        - File Allocation Table16 bit & 32 bit (FAT16 or FAT32)
        - Extended File Allocation Table (exFAT).

    - Mac uses
        - Hierarchical File System (HFS)
    - Macintosh can read and write to all Windows File systems but can only read NTFS.
    - Windows can only read HFS but requires the installation of an Apple HFS Driver or use a third party application like HFS Explorer.
- Disk Management Commands (on Windows)
    - chkdsk.exe (Check Disk Command)
        - Verifies the logical integrity of a file system. Enter chkdsk drive letter, then give /f switch to verify the logical integrity of a file system
    - format.exe (Format command)
        - Formats partitions to a selected file system. You can run the format command at the command line, or right-click a drive letter in Windows Explorer and choose Format.
    - dfrgui.exe (Optimize Drives command)
        - Arranges stored data on a disk into continuous blocks (reorganizing them). This can affect disk performance.
- Process Management / Scheduling
    - Management and scheduling are the methods used by the Operating System to assign the resources necessary to do tasks.
    - Computational elements such as threads, processes or data flows are scheduled to be performed by hardware resources such as processors, network components, video components or other resources that may be provided by expansion cards.
    - Multitasking is the ability to run many applications concurrently, or at the same time, which is possible because of multithreading.
    - To kill or end a process, use commands on Unix/Linux environments, and use Task Manager GUI interface on Windows.
- Memory Management
    - Process of controlling and coordinating computer memory, assigning portions called blocks to various running programs to optimize overall system performance. Memory management resides in hardware, in the OS (operating system), and in programs and applications.
    - If information must be continuously available, it may hold on to this information within itself, a memory type called cache.
    - If the information is not as crucial, but still necessary to access quickly it may store this information in the primary memory, AKA RAM. If information must be saved for future use and not needed for a while, the user may ask the Operating System to save it in storage.
    - Stack-based memory allocation



- Device Management
    - Process of managing the implementation, operation and maintenance of a physical and/or virtual device. It is a broad term that includes various administrative tools and processes for the maintenance and upkeep of a computer, network, mobile and/or virtual device.
    - Through device management one can view the status of a device, enable or disable a device, determine the driver the device is using, and uninstall or reinstall a device
- Application Software
    - Designed to run on multiple different operating systems. "Mobile" refers to devices such as laptops, smartphones, iPads, and other tablet devices. "Desktop" is the traditional CPU and monitor with all the peripherals. Applications that users access and use through a web browser are known as "web-based".
- Productivity Software
    - Applications that range from those used to create documents to those used to manage your projects and organize your time
- Collaboration Software
    - Designed to facilitate sharing data and resources between users in a variety of locations and using a variety of computing devices.
- Specialized Software
    - Companies in architectural, engineering, medical, and financial fields require software applications that are specific for the documents and files that they need to create and use.
- Services
    - Many programs that run hidden in the background
    - Services usually start at system boot or when launching an application.
    - Type services.msc in the search field of taskbar on Windows to view services

- Processes
    - A process is executing a program; when an application is launched, it spurs at least one process
    - A thread is a unit of allocation that an OS gives the processor
- Utilities
    - Every operating system comes with a host of utilities designed to help you diagnose and troubleshoot problems and simplify tasks.
- Interfaces
    - Interface is how a user communicates with the computer.
    - Can be either GUI (graphical) or CLI (command line)

4. Software Development

- Interpreted Programming Language
    - Type of high-level language that is run directly from the source code by an interpreter program without the need to compile.
    - Program is not translated into “machine code” until runtime
    - Perl, Python, Matlab
- Scripting languages
    - Type of interpreted programming language designed to execute tasks using a runtime environment.
    - Pretty vague term
    - Javascript, PHP, Bash
- Scripted Languages
    - Not to be confused with scripting languages
    - Programming language that allows all different types of programs from industrial, embedded, and games to expand on the user experience.
    - Lua
- Markup Languages
    - Language that is used to annotate text using tags that tell a computer how to display specific portions of the text.
    - You can’t really “program” as you cannot create mathematical functions and algorithms (not a computational language)
    - HTML, XML
- Compiled Languages
    - Language that must be compiled prior to being executed. This means that the program must be converted to machine code before running as an executable
    - A Java developer would use JDK, Java Development Kit and JRE (Java Runtime Environment) to execute a .jar file. When compiling java code, it creates a .class file which is used for execution
    - Java, C, C++, Fortran
- Query Programming Languages

    - Query languages are created for selecting, creating, updating, or deleting data in a database.
- Assembly Language
    - Low-level programming language that allows a programmer to give specific instructions to a piece of hardware such as a processor or create a device driver for hardware such as video or sound cards.
    - Known as a symbolic programming language which means it is the closest you can get to machine language without actually using machine code such as binary or hexadecimal.
- Identifiers & Variables & Constant
    - Identifiers are named component created by the programmer to contain a single value
    - Variables are identifiers whose value can change over time
    - Constants contain value that cannot be changed
- Containers
    - Arrays and Vectors
    - A container is a type of variable or constant that allows a programmer to group similar data types together in a single identified container
    - Array: List of values of the same data type with a fixed size
    - Vectors: Just like arrays, but elements do not need to be the same data type
- Functions
    - Also known as methods, subroutines, and procedures
    - These allow programmers to create blocks of reusable code throughout the program.
- Objects
    - They have attributes that define them and you can take actions based on how you can use the object.
    - Often, Classes define the attributes of objects
    - Used in Object Oriented Programming (OOP)
- Logic Component
    - Sequence: Analyzing the order of the code to understand its purpose
    - Branching: Separate routes that the code can take through Boolean options
    - Looping: A circular logic that allows for repetition until an expression is satisfied
    - While: Continues to loop until the condition is false.
    - For: Continues to loop until the condition is false. Each iteration has an increment.
    - Do While: Runs a single iteration regardless whether the condition is true or false. After the single iteration, a while loop takes effect
- Comparison Operators
    - >, <, >=, <=, ==, !=
    - Greater than, less than, greater than or equal to, less than or equal to, equal to, not equal to
- IF ELSE Statements
    - Set up conditions in which certain parts of code can be implemented based on conditions

5. Database Fundamentals

- Database
    - Large quantity of indexed digital information. It can be searched, referenced, compared, changed or otherwise manipulated with optimal speed and minimal processing expense.
    - Alternatively referred to as a databank or a data store
    - A database is built and maintained by using a database programming language. The most common database language is SQL, but there are multiple versions of SQL, depending on the type of database being used.
    - Database can be built on data files like Excel, CSV (comma separated values), text document, or manual typed data
    - Query searches sort and configure the data in as many possible ways as can be imagined by the database programmer.
    - After the query, report is created (which is like a “hard copy” of data)
- Flat File vs Database
    - Flat File
        - File of data that does not contain links to other files or is a non-relational database
        - Spreadsheets, CSV
        - Can only store text or numeric data
        - Changes made to data would be lost if power is lost before saving
    - Database
        - Allows storage of sound clips, pictures, videos, and other types of data
        - Database creates data persistence (by using files that log changes to the data)
    - Advantages of using database
        - Allow for multiple concurrent users
        - Can maintain millions of records
        - Faster access with better organization of daata
        - Storage of more advanced data types
        - Data persistence
- Structured vs Semi-Structured vs Unstructured
    - Structured
        - Specific rules must be followed
        - Database is organized and conforms to these rules
        - Example: relational database
    - Semi-structured
        - Can be sorted through metadata, and get organized in a different way
        - Example: Metadata, hashtag,
    - Unstructured
        - No organization, but merely a collection of data
        - Example: Pictures on phone, files listed in a folder (with no sort)
- Relational Databases
    - Provide an environment from which data can be accessed or reassembled in a variety of different ways without needing to reorganize the database tables

    - All data is stored in tables, which is an arrangement of information in rows and columns containing cells that make comparing and contrasting information easier. In a database, the rows of a database are records, and the columns are fields.
    - Schema: Specific rules that define structured databases. A schema refers to any plan or vision that is well thought out and documented with set rules and restrictions.
    - Primary Key: The primary key is one or more fields whose data is used to identify a record uniquely, for example an email address or username
    - Foreign Key: One or more columns in a table that refers to the primary key in another table . It is used to link two tables together
- Non-relational databases: key/value database
    - Non relational database that uses a simple key-value method to store data.
    - Due to extremely simple structure, it can handle massive amounts of traffics
- Non-relational databases: Document Database
    - Contains documents, which are records that describe the data in the document, as well as the actual data.
    - Documents can be as complex as you choose
    - You can use nested data to provide additional sub-categories of information about your object. You can also use one or more documents to represent a real-world object.
- Database Access Methods
    - Direct/manual Access: Manual editing of data within a database table.
    - Programmatic Access: Access through languages like SQL or through commands
    - User Interface and Utility: A form is an interface used to input or search data for editing.
- Relational Methods
    - CREATE: Used to create database or table
        - CREATE DATABASE *database_name*
        - CREATE TABLE *table_name*(column1 datatype, column3 datatype, …);
    - ALTER: Change structure of a table
        - ALTER TABLE *table_name* ADD *column_name datatype*
        - ALTER TABLE *table_name* DROP COLUMN *column_name*
        - ALTER TABLE *table_name* ALTER COLUMN *column_name* datatype;
    - DROP: Permanently remove a database or table and all stored data within
        - DROP DATABASE *database_name*
        - DROP TABLE *table_name*
    - SELECT: Extract data from the database according to specific condition
        - SELECT column1, colum2 … FROM *table_name* WHERE condition1 AND condition2 AND condition 3 ORDER BY column1;
    - INSERT: Put new data into database according to specific condition
        - INSERT INTO *table_name*(column1, column2, …) VALUES (value1, value2, value3…);
    - DELETE: Remove entire records or even just a single record from a database according to a specific definition
        - DELETE FROM *table_name* WHERE condition;
    - UPDATE: change the data in records in a database according to a specific definition

        - UPDATE *table_name* SET column1=value1, column2=value2 . . . WHERE condition;
- Export/Importing Data
    - Backup
        - Procedure of exporting data to a second location (cloud or offsite)
        - A backup should be done regularly and should not only include the data but the schema of the database also.
        - Besides tables, reports, queries and forms should also be backed up
        - Database dump
    - Sample import statement
        - LOAD DATA INFILE 'sample.csv' INTO TABLE Students FIELDS TERMINATED BY ' , ';
- Permissions
    - Permissions are hierarchical in nature. If permission is established on a database, then by default it applies to all tables in the database.
    - Db_owner: Full access (read, write, delete, backup)
    - Db_datareader: Read data
    - Db_datawriter: Add, delete, modify data
    - Db_bckupoperator: Backup database
    - Db_denydatareader: can't view data
    - Db_denydatawriter: can't add, delete, or modify data
- SQL Injection
    - Attack in which SQL statements are inputted in input box (such as user ID) to retrieve data (or to delete records in database)

6. Security

- Confidentiality Concerns
    - Snooping
        - Unauthorized access or interception of an organization's data.
        - Sniffing is when an attacker monitors a network using a protocol analyzer. It will allow them to capture network traffic from a physical or wireless network and analyze the contents of the data
    - Eavesdropping
        - Microphones and video cameras are being used to listen to conversations
        - These can do so with permission via applications we have authorized to listen in, but also without permission if a malware application is installed listening to your conversations.
    - Wiretapping
        - Authorized or unauthorized monitoring and recording of communications between two parties
    - Social Engineering

        - Type of attack that uses deception and trickery to convince unsuspecting users to provide sensitive data or to violate security guidelines.
        - Shoulder surfing, spoofing, impersonation, hoax, phishing, vishing, whaling, spam and spim
    - Dumpster Diving
        - Hackers do it to find confidential informations such as bills & invoices, business cards, customer lists, employee lists, or other records
- Integrity Concerns
    - Integrity means that data has been maintained with consistency, accuracy and trustworthiness through the life of that data.
    - Man-in-the-Middle (MITM)
        - An attacker impersonates a network to make it look legitimate, while intercepting data transferred.
    - Replay Attack
        - Attacker captures a piece of data or a message sent by a user then later tries to replay it with the intention of gaining unauthorized access.
    - Impersonation
        - Both a human or technology-based attack depending on how the attack is initiated.
    - Unauthorized Information Alteration
        - After an attacker is into a system, they may have the ability to alter information that will cause damage to the target.
        - This information could be anywhere from being on a server, a desktop computer, a file share, or a database.
- Availability Concerns
    - Availability is the ability for a user to access and use data when they need it. In availability, there are few types of issues you need to be aware of including service issues and hardware failure.
    - Denial of Service Attack (DoS Attack)
        - In this attack, a service or web host is disrupted by a flood of information that overloads the systems and prevents you from accessing the data.
        - When it comes from a single IP address, it can simply be shut down by blocking IP address via firewall
        - In case of Distributed Denial of Service Attack (DDOS), there are multiple computers and servers used to target a single computer or a network.
    - Power Outage:
        - Power outages cause information systems to no longer be accessible by the fact that power is required for all electronic equipment between where you are and where the remote computer or service is at
    - Hardware Failure
        - Make sure backups are done regularly and use redundant storage such as a Redundant Array of Independent Drives (RAID).

        - Depending on the type of storage, some devices like Network Attached Storage (NAS) have built in monitoring of drive health and will tell you when a drive is about to fail.
    - Destruction
        - Physical destruction / damage of computing device
        - Physical security necessary
    - Service Outage
        - Businesses like Amazon Web Services (AWS) sell their services to other businesses for servers, data storage, networks and more. If they go down then all the software or infrastructure you use is no longer available
- Malwares
    - Virus: A piece of code that spreads from one computer to another by attaching itself to other files.
    - Worm: A piece of code that spreads from one computer to another on its own, not by attaching itself to another file.
    - Trojan Horse: Type of malware that is itself a software attack and can pave the way for a number of other types of attacks.
    - Spyware: Surreptitiously installed malicious software that is intended to track and report the usage of a target system, or to collect other data the author wishes to obtain.
    - Adware: Software that automatically displays or downloads advertisements when it is used
    - Rootkit: Code that is intended to take full or partial control of a system at the lowest levels.
    - Ransomware: Ransomware is malicious software that prevents you from using your computer.
- Antivirus/Anti-Malware
    - On a Windows 10 computer, the easiest antivirus to use is Windows Defender which is a part of Windows Security (which comes pre installed on Windows)
    - On MacOS, use softwares like Malwarebytes or Sophos Home
    - There are very little malware on Linux, so in most cases (especially computing at home), malware is not necessary
- Hosting Firewall
    - The rules used by a firewall can use any combination of criteria including: Applications, IP addresses, Domain Names, Protocols, Ports, Keyword / Phrases, Types of Files
    - Services firewall offers
        - Packet Filtering: Stateless inspection of each packet against a predefined rule set.
        - Stateful Inspection: Monitoring of an entire session of Transmission Control Protocol (TCP), from handshake to teardown, or User Datagram Protocol (UDP), through requested and opened ports
        - Content filtering: Permit or block specific attachment and payload types, keywords, and file formats.
        - Proxying: Placing the client session on hold while retrieving content on behalf of the client and caching the content for later use.
- Web Browsing

    - Cookie
        - Text file that is created by a web site and stored on the hard drive of a computer
        - Contains information about the user, how to identify them, and customize the web experience.
        - Can also store technical information about the user such as actions and pages visited, as well as, personal information such as form information and interests.
        - Temporary cookies only last for the duration of the web session
        - Persistent cookies are saved on the hard drive and remain even after browsing session ends and computer is turned off
    - Internet cache or browser cache
        - Storage area on browser for the files that make up a website
        - When you return, they are loaded up from cache in order to speed up the loading time of the web site.
- Browser enhancements & extensions
    - Plugins
        - enables a browser to process content on a web page other than what it can normally handle.
        - Example: Adobe flash
    - Extension
        - Adds additional features to a browser and becomes part of the application
        - Some of the extensions you might install may enhance browsing by adding toolbars, shortcut options and helpers' objects that are loaded when the browser is launched
- Secure web connections
    - Certificates
        - Electronic document that enables the secure exchange of information over a network including on web sites.
        - Verifies the validity of a web site, identity of a person, or integrity of a file.
        - Signed by a digital authority or certificate authority and are issued to individuals, computers, services, web site domains, files and more.
        - You may receive a warning if a website has an invalid certificate
    - HTTP vs HTTPS
        - As described in Section 3: Applications & Software
- Autofill Forms & Privacy
    - Makes filling out forms fast and easy, yet can be risky since it holds PII
    - PII (Personal Identifying Information): Information that can identify who a person is individually, including social security, driver's license, name, birthdate, address, etc
- Patching / Updates
    - Patch
        - Small units of supplemental code meant to address either a security problem or a functionality flaw in a software package or operating system.
    - Hotfix
        - Patch that is often issued on an emergency basis to address a specific security flaw.

    - Service Pack
        - Larger compilation of system updates that can include functionality enhancements, new features, and typically all patches, updates, and hotfixes issued up to the point of the service pack release.
    - Rollup
        - Collection of previously issued patches and hotfixes, usually meant to be applied to one component of a system, such as the web browser or a particular service
- OEM vs Third Party
    - OEM (Original Equipment Manufacturer)
        - Company that produces the hardware and software used in computing technology.
        - As the original manufacturer, you can trust the software you download from their website as long as you are sure it is the OEM site
    - Third-Party websites
        - Third parties may be a legitimate vendor offering software that fills a need. But they can also be illegitimate and contain some form of malware. (Sometimes come in forms of piracy)
        - Always best to approach with caution
- Steps to removing malicious software
    - 1. Disconnect from any Networks and the Internet
    - 2. Reboot into Safe Mode
    - 3. Avoid logging into accounts on the infected device
    - 4. Check your Activity Monitor/Task Manager
    - 5. Start Running your Antivirus/Anti-Malware software
    - 6. If it was not successful in removing the virus, use a Bootable Antivirus Rescue Disk.
    - 7. Fix your Browsers
    - 8. Restart your Computer normally.
    - 9. Worst case, you will need to reinstall the OS from scratch, possibly losing files, if you have not externally saved them. (Always backup!)
- AAA (see below for detailed description on each)
    - Authentication, Authorization, Accounting
- Authentication
    - Single Factor
        - Single Factor Authentication (SFA) is the simplest of all the authentication factors. In this authentication scheme, a single set of identification credentials is provided by the user or system for identification and authentication.
    - Multifactor
        - Multi Factor authentication (MFA) is any authentication scheme that requires validation of two or more authentication factors. It can be any combination of who you are, what you have, what you know, where you are or are not, and what you do.
- Authorization
    - Role Based Access
        - Anadministrator sets up and defines the different roles and permissions for each

role in a system. These access levels can be based on anything such as; organization of a business, job function, custom access rules defined by a business, or required user account types.

    - Rule-Based Access
        - Access is granted based on rules
        - These types of access control systems use Access Control Lists (ACL) to determine what are the rules and how to allow or deny access to a resources
        - Examples: Firewall can have a rule that permits access from a specific IP address block but denies from anything else
    - Mandatory Access Controls
        - Most restrictive access control
        - Also uses Access Control Lists (ACL) to determine what are the rules and how to allow or deny access to a resource.
    - Discretionary Access Controls
        - Unlike mandatory access controls, in discretionary access controls users control who can access data on a system
        - Found on operating systems where users can add resources to access control lists that allow an individual user or groups of users to access a resource
- Accounting
    - Logging is the most common method of tracking those key actions.
    - In a system log, key actions are added to the date/time, task type, task status, task id, etc
    - Every operating system contains a log where events are tracked and recorded to a file
    - Security, system and application events are tracked and are available to be reviewed via a system log viewer.
    - Windows: Event Logging Doc
    - MacOS: See Console User Guide
- Password Practices
    - Length & Complexity
        - At minimum passwords should be at between 8 to 64 characters in length, however these lengths are determined by the provider
        - According to the National Institute of Standards and Technology (NIST), you should use the longest available length the provider permits.
    - Password History
        - Password history is the number of unique new passwords a user must use before an old password can be reused.
    - Password Expiration
        - Recommended that you change your password every 60-90 days
    - Password Reuse Across Sites
        - Come up with multiple passwords to use across different sites
- Secure Communication
    - Steganography: messages are hidden
    - Cryptography: messages are scrambled (not necessarily hidden)
        - Substitution: Cipher replaces letters, code replaces words
        - Transposition

- Cryptography
    - Monoalphabetic ciphers
        - One letter maps to another single letter
        - Primitive and very insecure (can be cracked with frequency analysis)
        - Caesar, Affine, ROT 13, Atabsh
    - Polyalphabetic ciphers
        - One letter does not necessarily map to another specific letter
        - Use of Keywords that determine how each letter is enciphered
        - Much more secure than monoalphabetic (frequency analysis is most often useless), but still not secure enough to be used in technology
        - Vigenere
- Encryption
    - Encryption on most modern operating systems can be done one of two ways, at the file level or disk level
    - The difference between the two is that in the file level, you choose which files are encrypted and which are not, while the disk level encrypts everything including the operating system.
    - File Level encryption
        - Allows you to specific files or folders on a device to encrypt
        - Done manually or automatically depending on the encryption software and will render the files unreadable without the decryption software and key
    - Disk Level encryption
        - Will encrypt the entire disk volume including the operating system
        - Depending on the software, it will protect the contents of the entire device and prevent the hard disk from being transferred to another computer