Basic Tool Kit: Linux

What is it and how to use it

What you are going to learn

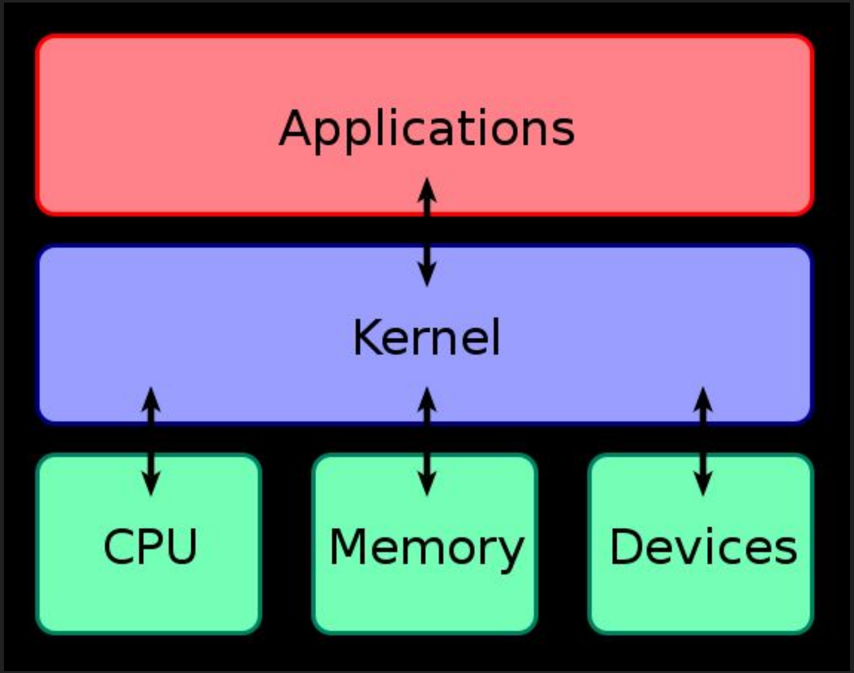
- Clear misconceptions
- Understand why Linux is so important
- The basics of it
- Resources to grow your skills with the basics

Why?

- I sure wish I learnt it earlier.
- Besides helping you landing interviews (depending on your role obviously) Linux:
  - Is used on almost every server (68% of 15.1M, Worldwide Server Operating Environment Shipments/Subscriptions and Nonpaid Deployment Share by Operating Environment, 2017)
  - The norm for Development environments
  - Has a powerful native terminal
  - Open source
  - Higher stability than a lot of other systems
  - **It is more secure**

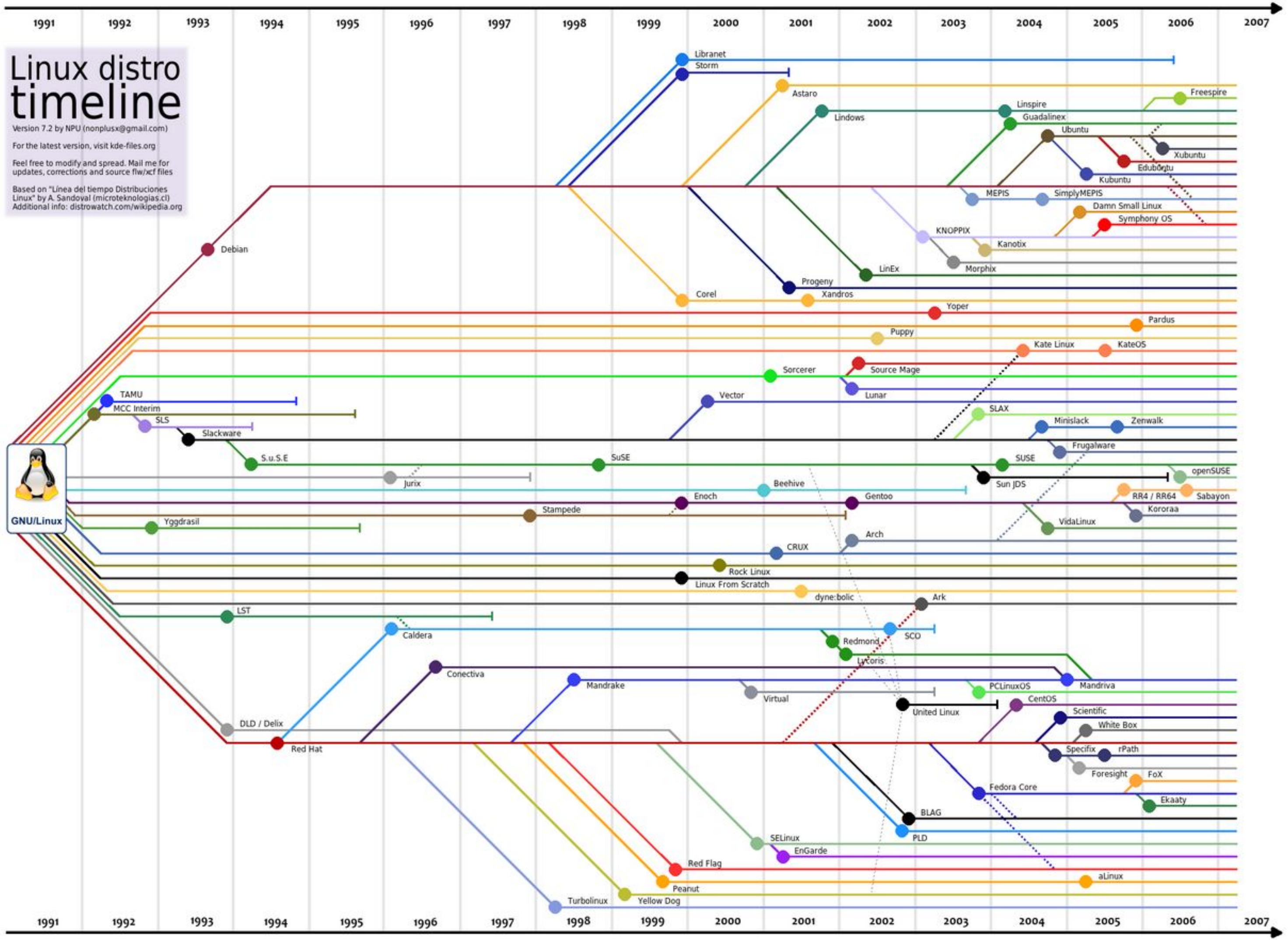
Linux History

- Based on Unix operating system built by AT&T by Ken Thompson
- Open-source
- Developed by Linus Torvald 1991
- A kernel, not really an operating system by itself
  - Kernel is the core of an operating system
  - Usually used with GNU



Linux Operating Systems

- Many Linux-based operating systems ("flavors"), optimized for various tasks. Think of how you use various programming languages for different projects (although this is is a dangerously dissimilar analogy).
- Popular ones are Ubuntu, Knoppix, Parrot, CentOS, SUSE, Gentoo and OpenWrt.



Linux distro timeline

Version 7.2 by NPU (nonplusx@gmail.com)

For the latest version, visit kde-files.org

Feel free to modify and spread. Mail me for updates, corrections and source flw/xcf files

Based on "Línea del tiempo Distribuciones Linux" by A. Sandoval (microteknologias.cl)
Additional info: distrowatch.com/wikipedia.org

Kali Linux

- Kali Linux is a Debian-based Linux distribution created by Offensive Security in early 2013 and geared towards various information security tasks, such as Penetration Testing, Security Research, Computer Forensics, and Reverse Engineering.
- Basically a flavor of Linux that comes pre-installed with security tools
- You can get the tools without Kali Linux

the shell

- Kali Linux has a GUI but that does not mean you can escape the terminal (and why would you want to?)
- Technically speaking, a shell is a program that processes commands and returns output - but it is also colloquially used as a synonym for the terminal or console.
- Types of shells in Linux are The Bourne SHell (sh), Bourne-Again SHell (Bash), Korn Shell (ksh), Z SHell (zsh)
- They all serve the same basic purpose but are specialized in some tasks

Command line basics

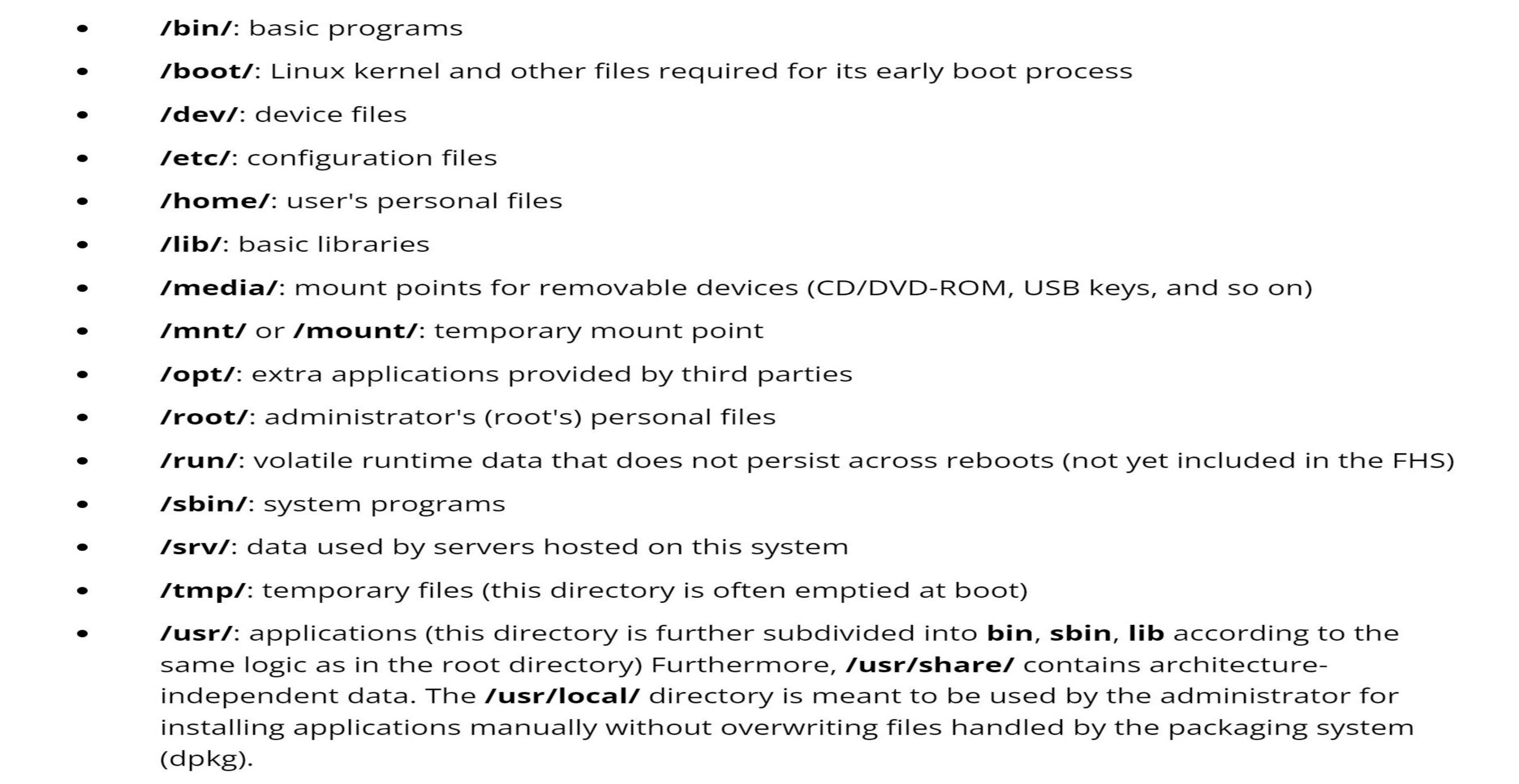
- There was a talk on this so I assume you are comfortable with navigating the file system but, to reiterate, here are some basic commands:
  - Whoami
  - Pwd
  - Mkdir
  - Rm (-r)
  - Cd
  - Cd ..
  - Touch
  - Ls
  - cat

Linux file system

Since there are many distributions and flavors of Linux, the Linux Foundation has developed a standard called the Filesystem Hierarchy Standard (FHS).The FHS exists so that when users interact with an unfamiliar Linux environment, they can still find their way around the machine.

The FHS defines the purpose of each main directory on a Linux system. The top-level directories are described as follows:

Linux file system



- **/bin/**: basic programs
- **/boot/**: Linux kernel and other files required for its early boot process
- **/dev/**: device files
- **/etc/**: configuration files
- **/home/**: user's personal files
- **/lib/**: basic libraries
- **/media/**: mount points for removable devices (CD/DVD-ROM, USB keys, and so on)
- **/mnt/** or **/mount/**: temporary mount point
- **/opt/**: extra applications provided by third parties
- **/root/**: administrator's (root's) personal files
- **/run/**: volatile runtime data that does not persist across reboots (not yet included in the FHS)
- **/sbin/**: system programs
- **/srv/**: data used by servers hosted on this system
- **/tmp/**: temporary files (this directory is often emptied at boot)
- **/usr/**: applications (this directory is further subdivided into **bin**, **sbin**, **lib** according to the same logic as in the root directory) Furthermore, **/usr/share/** contains architecture-independent data. The **/usr/local/** directory is meant to be used by the administrator for installing applications manually without overwriting files handled by the packaging system (dpkg).

How to make Linux work for you

- Lots of apps have command line interfaces
    - e.g. gdb, valgrind

```
sudo apt-get  update
sudo apt-get install gdb
```

- Be careful about installing apps globally. Ensure you install it install it in a virtual environment (venv, virtualenv etc.)

SSH

- SSH (Secure Shell) to connect to remote machines
- Reasons include:
  - Use applications installed of remote machine
  - Access information on remote machine
  - Different operating system

```
ssh username@ip-address -p port-number
```

More things you want to know about Linux

- Piping and Redirection
- Searching and text manipulation
- Managing the running of processes
- File and Command Monitoring
- Scheduled tasks
- Logs
- Disk Management
- File permissions
- User and group

Classes where this skill will help A LOT

- ECE 391: System Programming or CS 241: System Programming
- ECE 422/CS 461: Computer Security 1
- ECE 424/CS 463: Computer Security 2
- CS/ECE 438: Communication Networks

Where to get help

- The man page (or using -h)
- Offensive Security’s PEN 210 course (here is the discord link: https://discord.gg/89frj7vN)
- Have you ever heard of StackOverflow?

References

https://www.cyberciti.biz/tips/linux-kernel-history-and-distribution-time-line.html
https://en.wikipedia.org/wiki/Kernel_(operating_system)

https://www.offensive-security.com