SIGPwny

FA2023 Week 02 • 2023-09-10

Intro to Terminal and Setup

Emma and Ronan

Announcements

- **Register for Fall CTF!**
  - sigpwny.com/register23
  - Event on September 23rd 12-6 PM, register now!

- Second place (tied for first!) in Patriot CTF
  - Thanks for joining us if you could!
  - If you couldn't make it, no worries! We will play plenty of other CTFs this semester

What is SIGPwny?

- Computer security/hacking club at UIUC
- Largest Special Interest Group within ACM@UIUC

"Don't ever talk to me or my child again"

Join Us for Meetings!

Thursdays at 7–8 PM

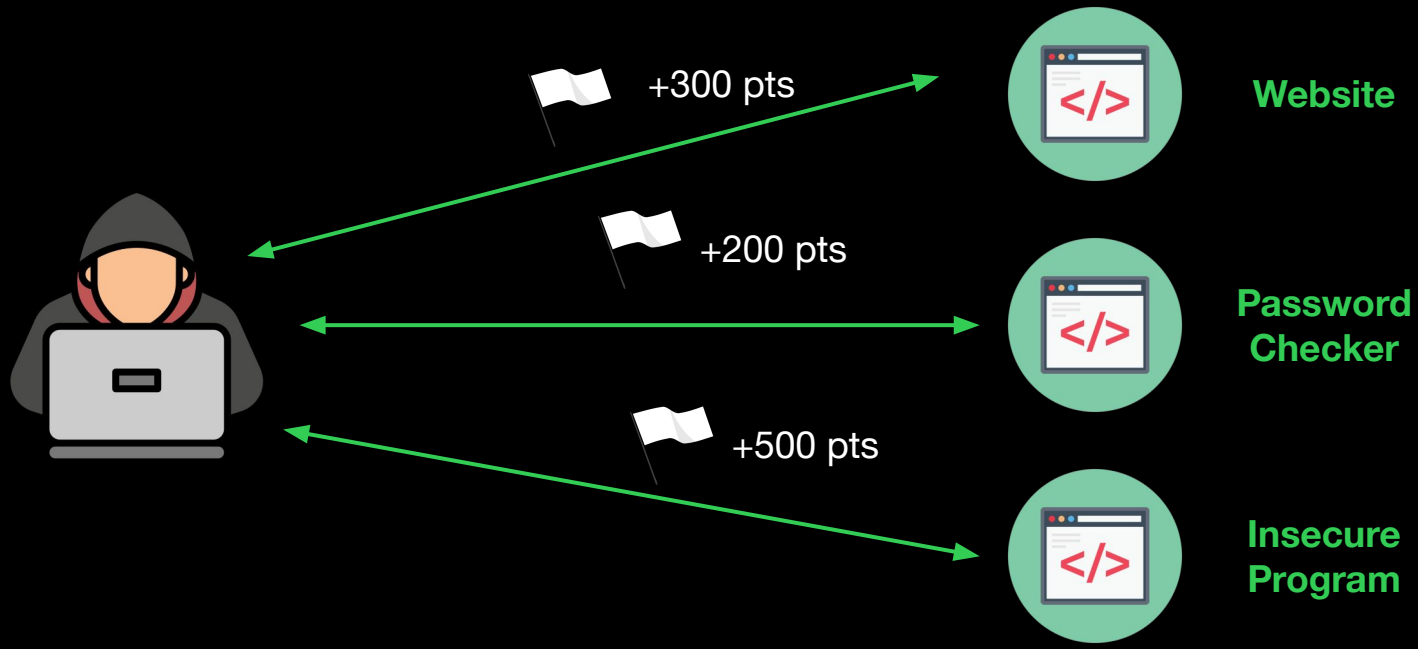
- Siebel CS 1404
- 15 minutes talking
- 45 minutes doing

Sundays at 2–3 PM

- Siebel CS 1404
- 1 hour of extended lecture

Capture the Flag (CTF)

- Cybersecurity competition
- Compete against other teams
- "Jeopardy style" - hack the most (and hardest) things to win
- The best way to practice your security knowledge!



Capture the Flag (CTF)

Overall rating place: **410** with **49.859** pts in 2018

Country place: **48**

Overall rating place: **300** with **77.673** pts in 2019

Country place: **31**

Overall rating place: **136** with **174.389** pts in 2020

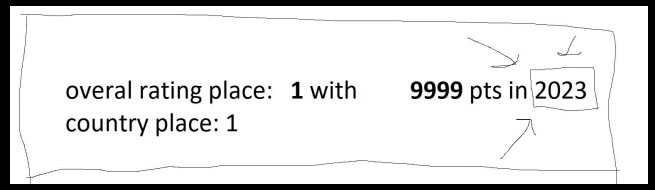
Country place: **19**

Overall rating place: **80** with **243.217** pts in 2021

Country place: **12**

Overall rating place: **48** with **346.020** pts in 2022

Country place: **6**



- We participate in various CTFs hosted by other teams
- Pwny CTF is our internal, 24/7/365 CTF with a leaderboard to compete with friends!
- **Fall CTF 2023 -** September 23rd

  A beginner CTF that SIGPwny runs exclusively for UIUC students and people completely new to cybersecurity! Free food, shirt, PCB badge, and prizes!

Fuzzing Team NEW!

- Find vulnerabilities in programs and get bug bounties ($$$)
- Use fuzz testing to automatically uncover bugs
- Running over the course of the semester
- Systems programming experience highly recommended
- Meetings on **Saturdays at 11am**
- Fill out this form or message `@rliu` or `@shorden` on Discord if interested

Code of Conduct

1. Be respectful.
2. Be inclusive.
3. Nothing illegal.
4. Don't cheat.
5. No NSFW or suggestive content in Discord.
6. Don't spam in Discord.
7. Use common sense.

The full Code of Conduct is available at sigpwny.com/rules.

Report misconduct to sigpwny.com/report.

The "Don’t Get Arrested" Slide

Computer Fraud and Abuse Act (CFAA)

- Attacking "protected" computers
- Anywhere between a fine and **TWENTY** years in jail.
- If you don't have **EXPLICIT** permission to break into it, **DON'T**

Pwny CTF (ctf.sigpwny.com)

- Create an account right now!
- Where we put our challenges for you to build hands on experience
- Solve challenges, find flags, submit flags on website

ctf.sigpwny.com

sigpwny{starting_off_strong}

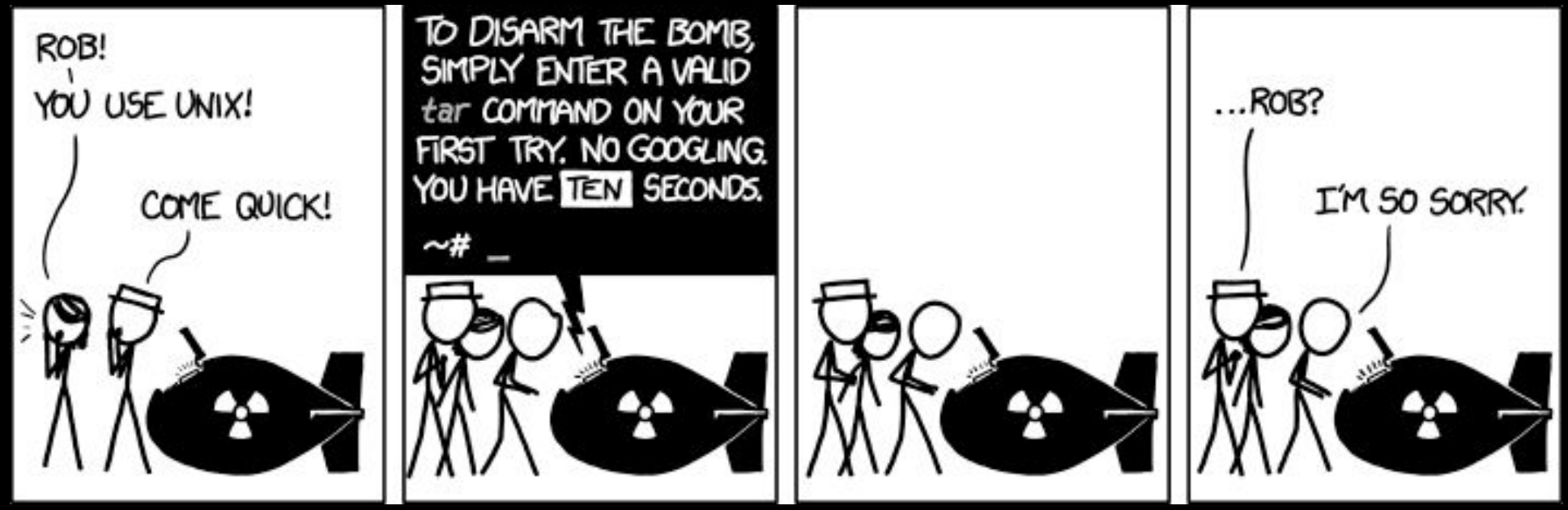


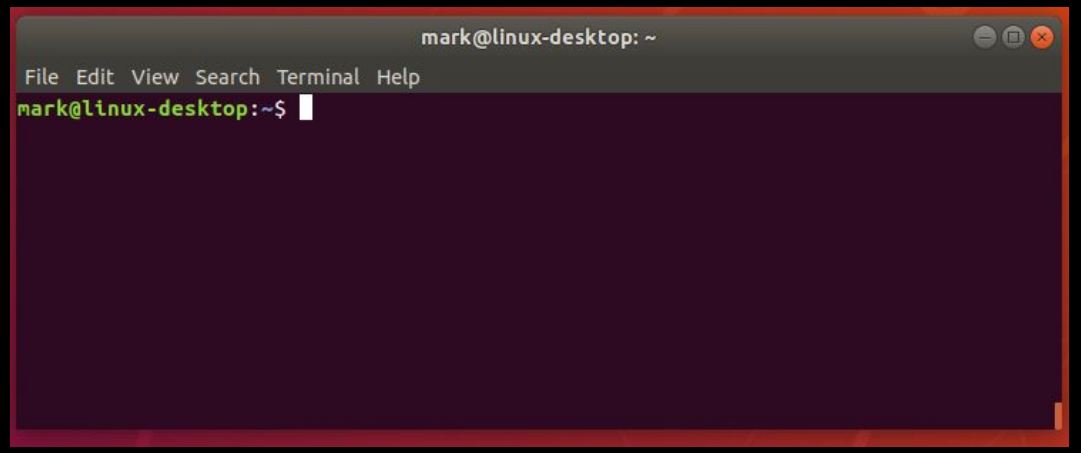
Table of Contents

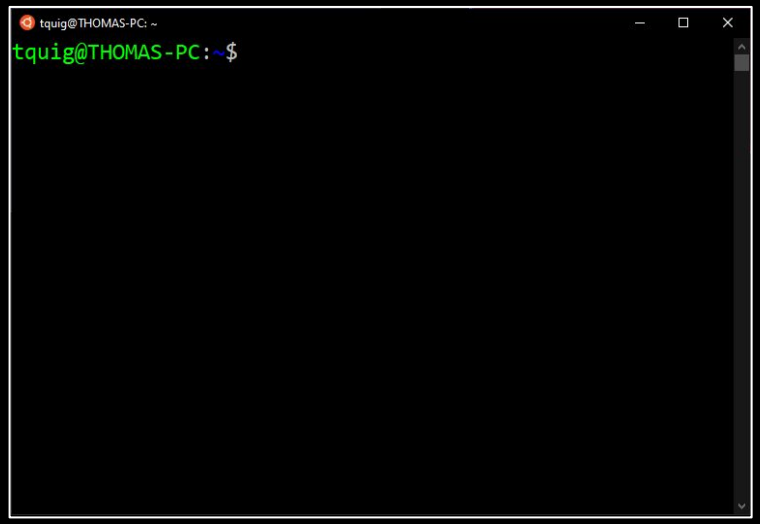
- What is a shell
  - I want one
- Getting into the shell
  - OS Differences + Different Shells
  - WSL or Virtual Machines?
  - Installing WSL
- Starter commands
- Tools to install

> The Terminal

"It’s where things happen" - Ravi

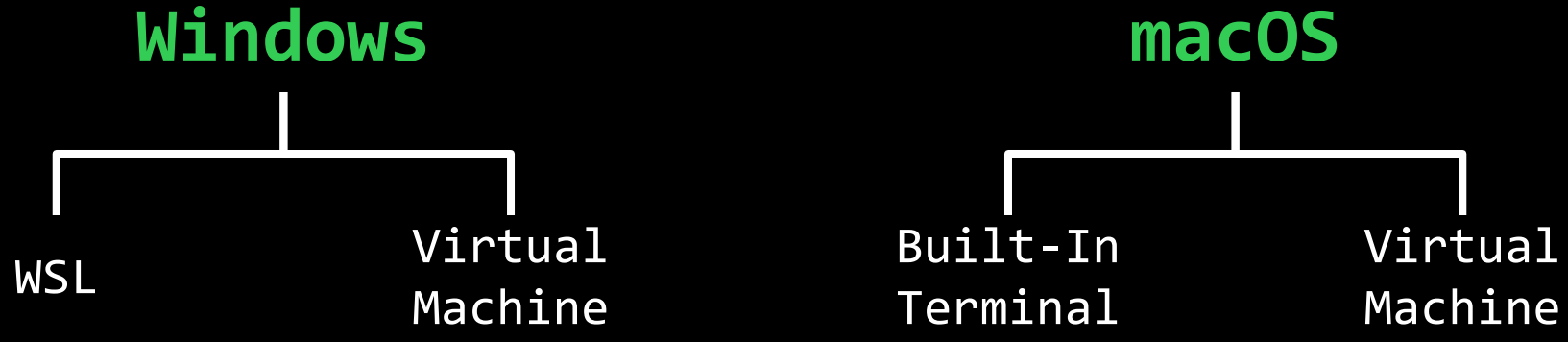

⌥⌘1
/dev/ttys000
→ CSAW2020 ls
bard grid kui_blox1_sol.png
bard.hop grid_solve.py libc-2.27.so
ezbreezy krakme.exe solve_ezbreezy.py
→ CSAW2020


mark@linux-desktop: ~
File Edit View Search Terminal Help
mark@linux-desktop:~$


tquig@THOMAS-PC: ~
tquig@THOMAS-PC:~$

Linux

You’re good to go!


Windows
WSL
Virtual Machine
macOS
Built-In Terminal
Virtual Machine

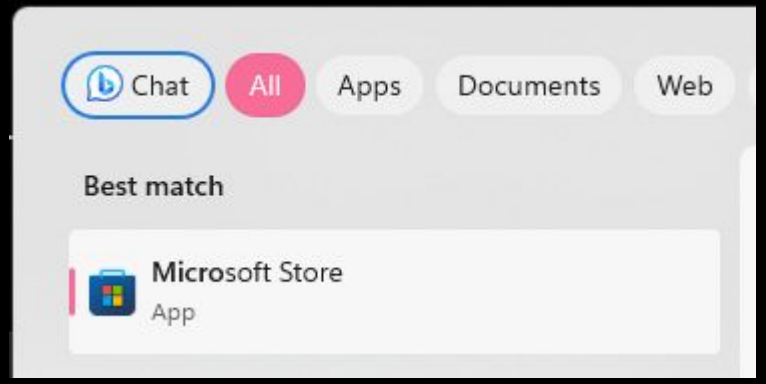
PowerShell? Command Prompt?

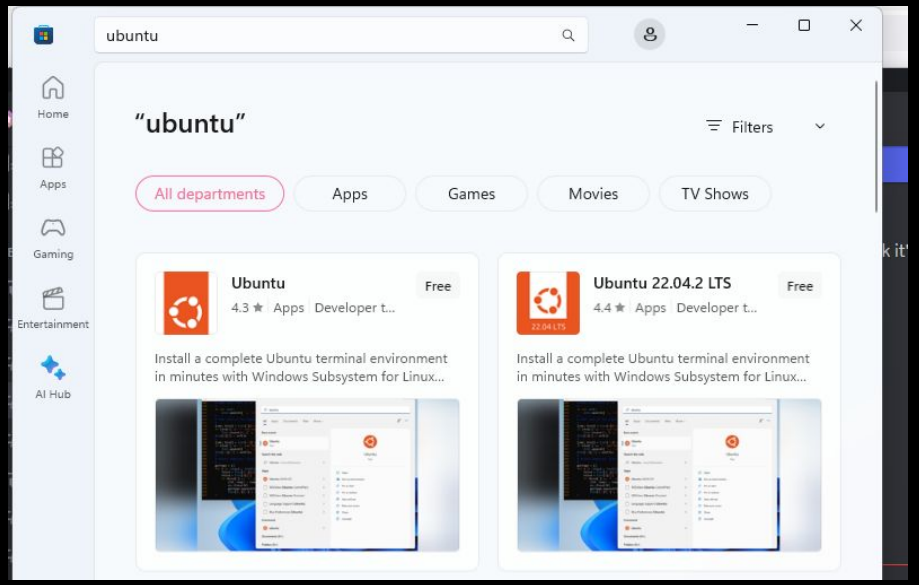
- Those are shells too!
- However, the Windows terminal is built differently than the Mac and Linux terminals (which are both UNIX based)
  - Different command structure/rules
  - Less support for CTF relevant applications

Windows Subsystem for Linux

Getting a Terminal

Open the Microsoft Store → Search "Ubuntu" → Install "Ubuntu" (use the one without a version number)

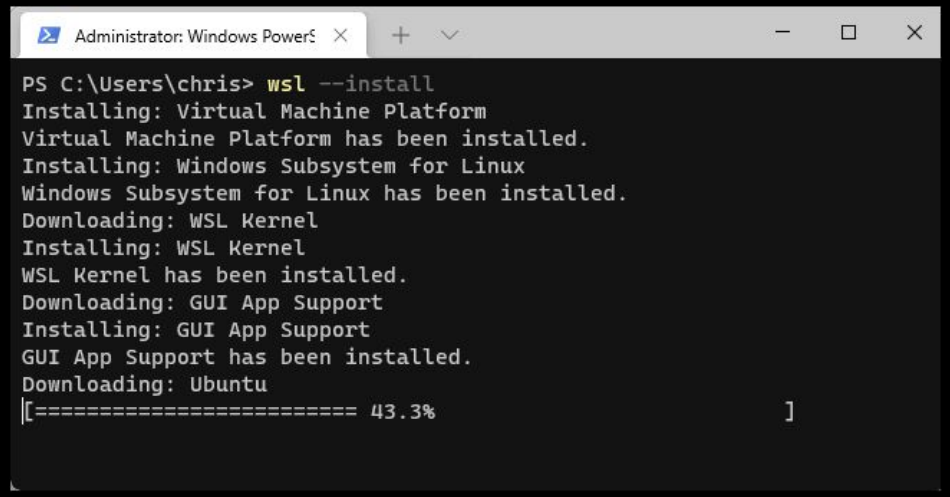




Getting a Terminal (Older W11/W10)

If you get a "Windows Subsystem for Linux is not installed" error when trying to install Ubuntu from the Microsoft Store, try this.

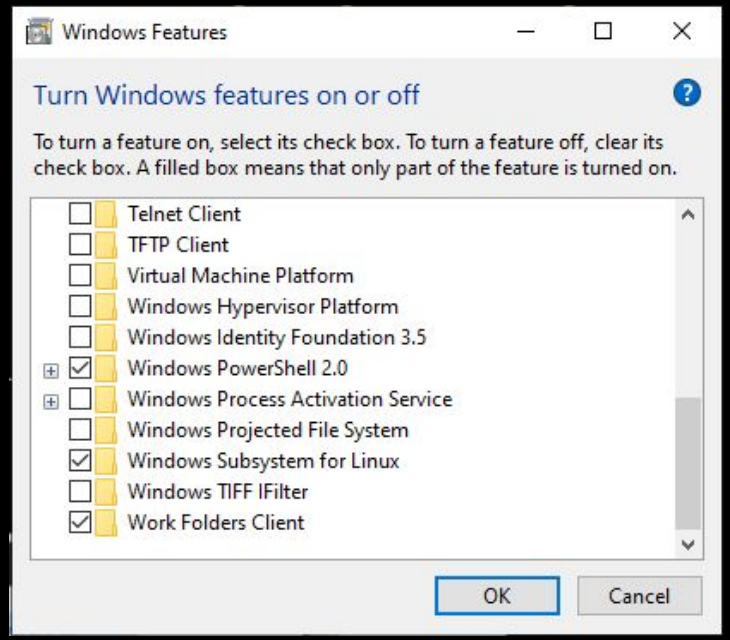
- Open command prompt as administrator
  - (Start button → type **cmd** → right click → "Run as Administrator")
- Type **wsl --install**
- Restart computer
- You should be able to launch Ubuntu from Microsoft Store



Getting a Terminal (Even older W10)

If you get a command not found error when trying to run "`wsl --install`", try this.

- Go to the Windows search bar
- Search "Turn Windows features on or off"
- Check "Virtual Machine Platform" and "Windows Subsystem for Linux"
- Restart computer



Have Docker Installed?

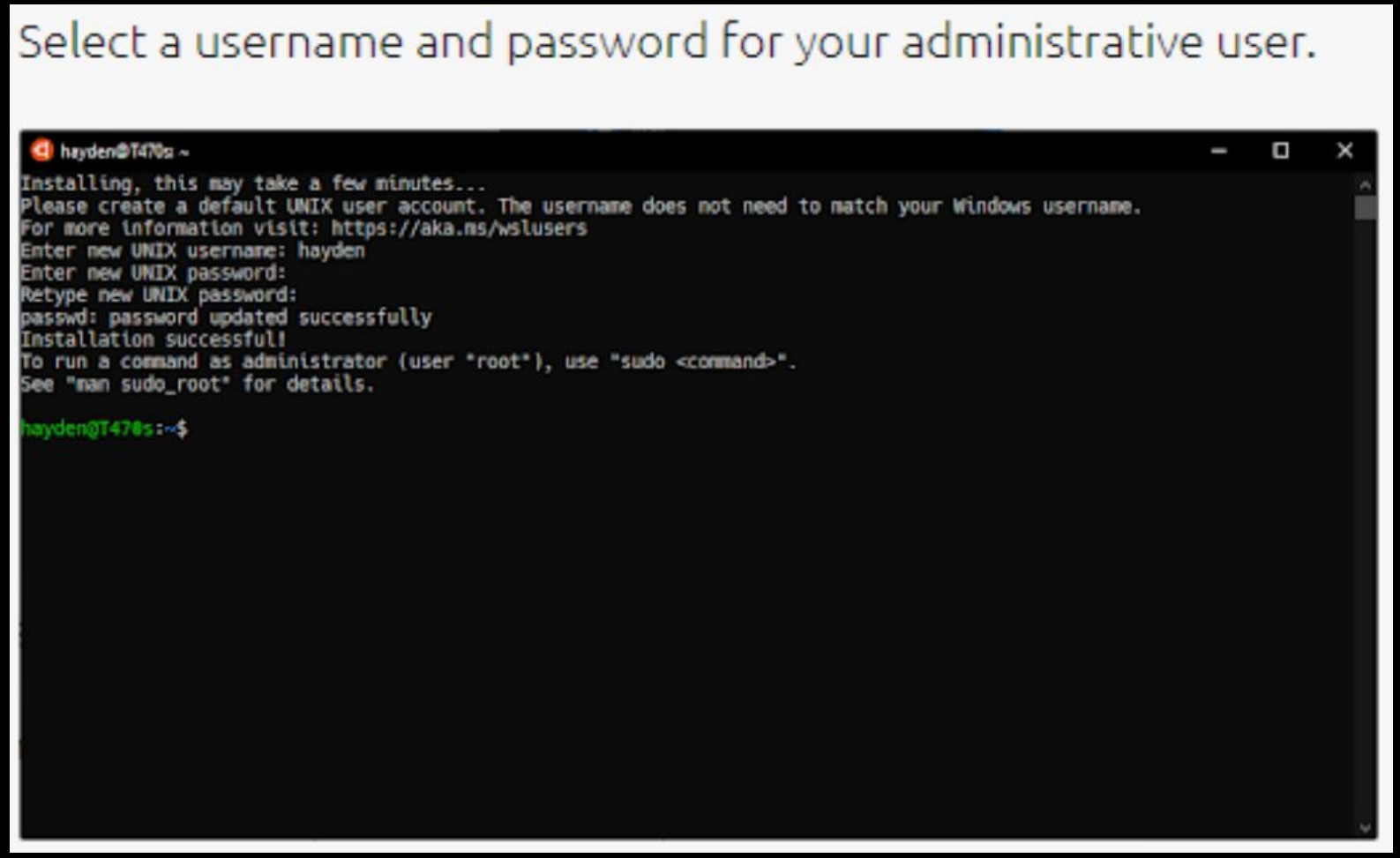
If you already have Docker for Windows installed or are taking CS 128 or 225, you may run into an issue when running wsl.exe.

The below commands should be run in **PowerShell** or **Command Prompt**!

Docker also uses WSL and creates a minified WSL installation to work. If you run `wsl --list`, you may see that docker-desktop-data is set as the default.

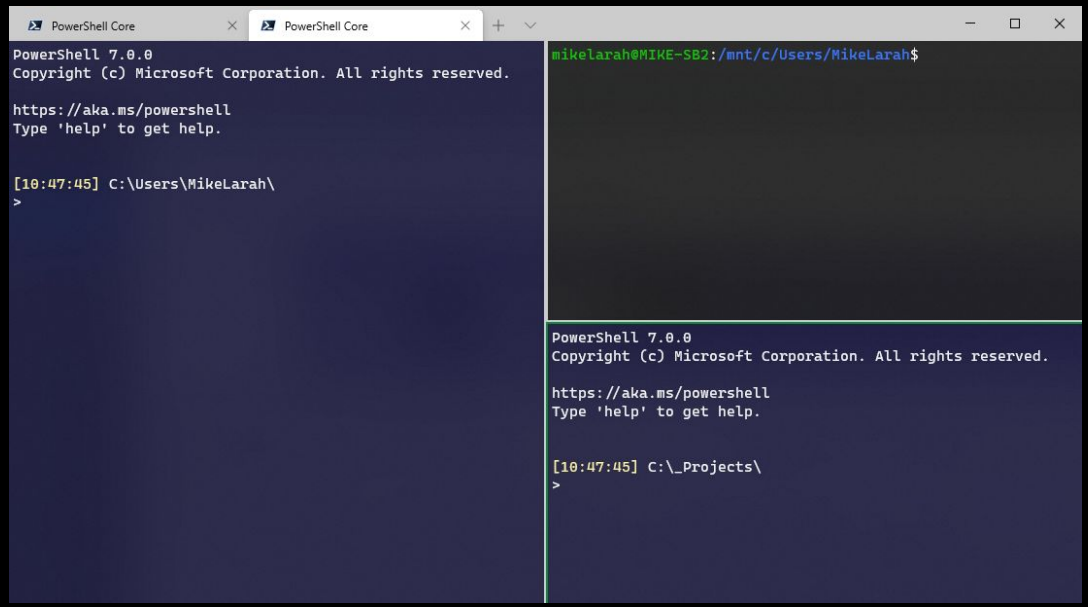
Run `wsl --set-default Ubuntu` to set Ubuntu as your default WSL installation. This will not affect Docker.

Set a "root" user



Windows Terminal (Optional)

- Nice for managing multiple types of command line on Windows machines
- Download from the Microsoft Store



macOS Terminal

Command
+ Space → Search “Terminal” →

Homebrew (Optional)

- AKA "brew"
- Popular package installation tool on MacOS
- https://brew.sh
- To install tools with brew, use `brew install <package>`
- Example: `brew install wget`

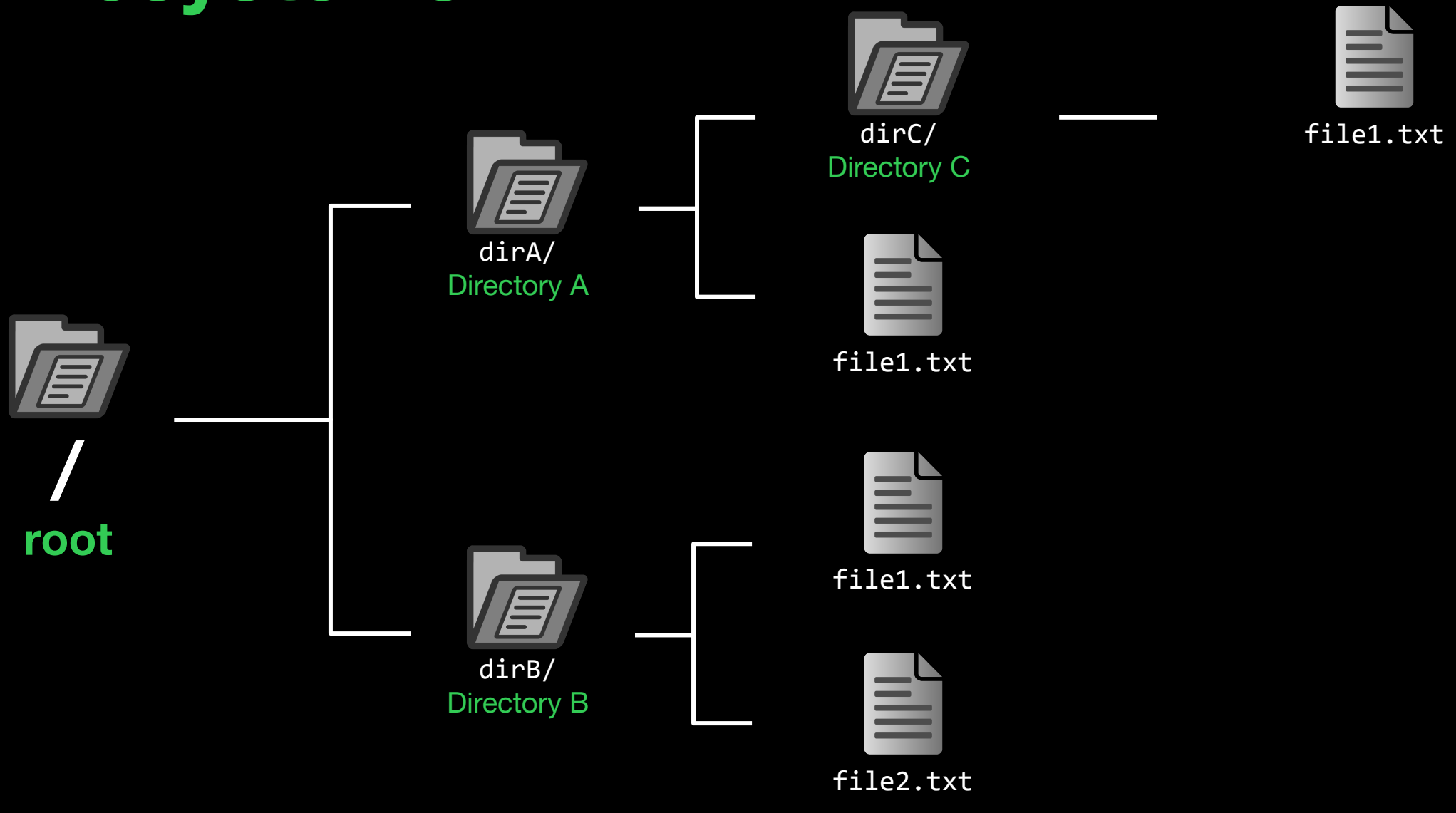
iTerm2 (Optional)

iTerm2

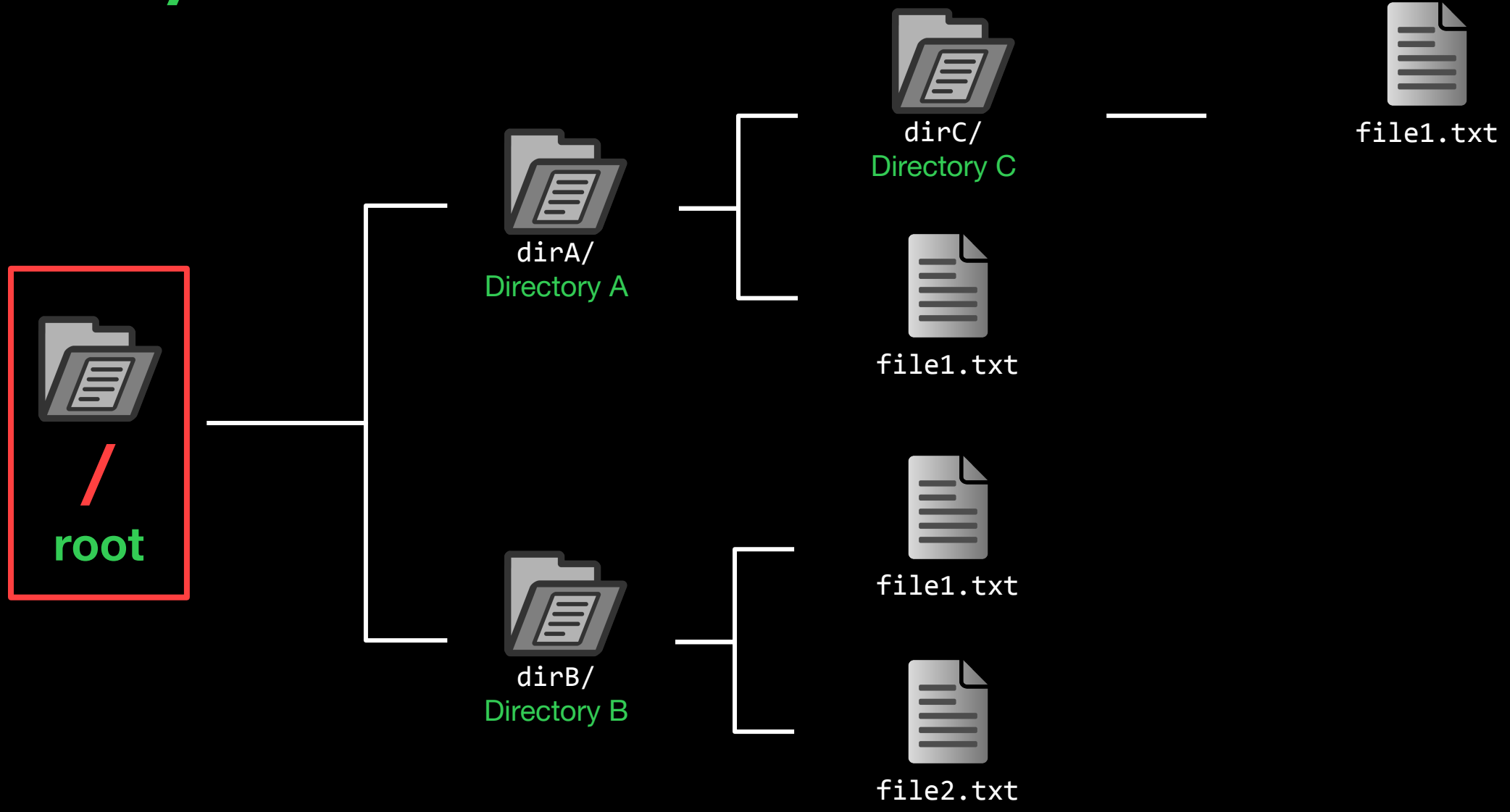
iTerm2 is a terminal emulator for macOS that does amazing things.

- Modern replacement for the basic macOS Terminal
- https://iterm2.com

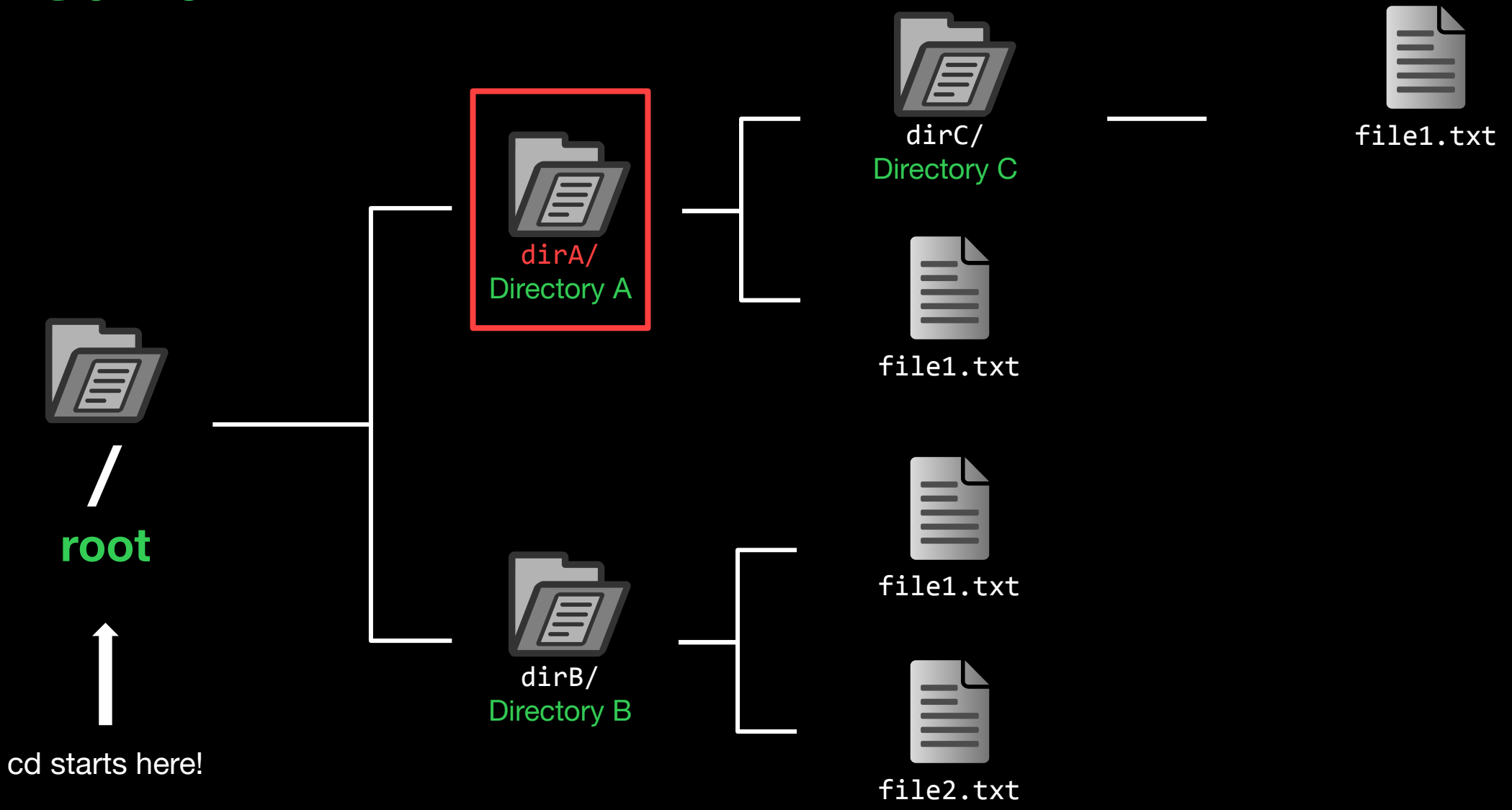
Filesystems



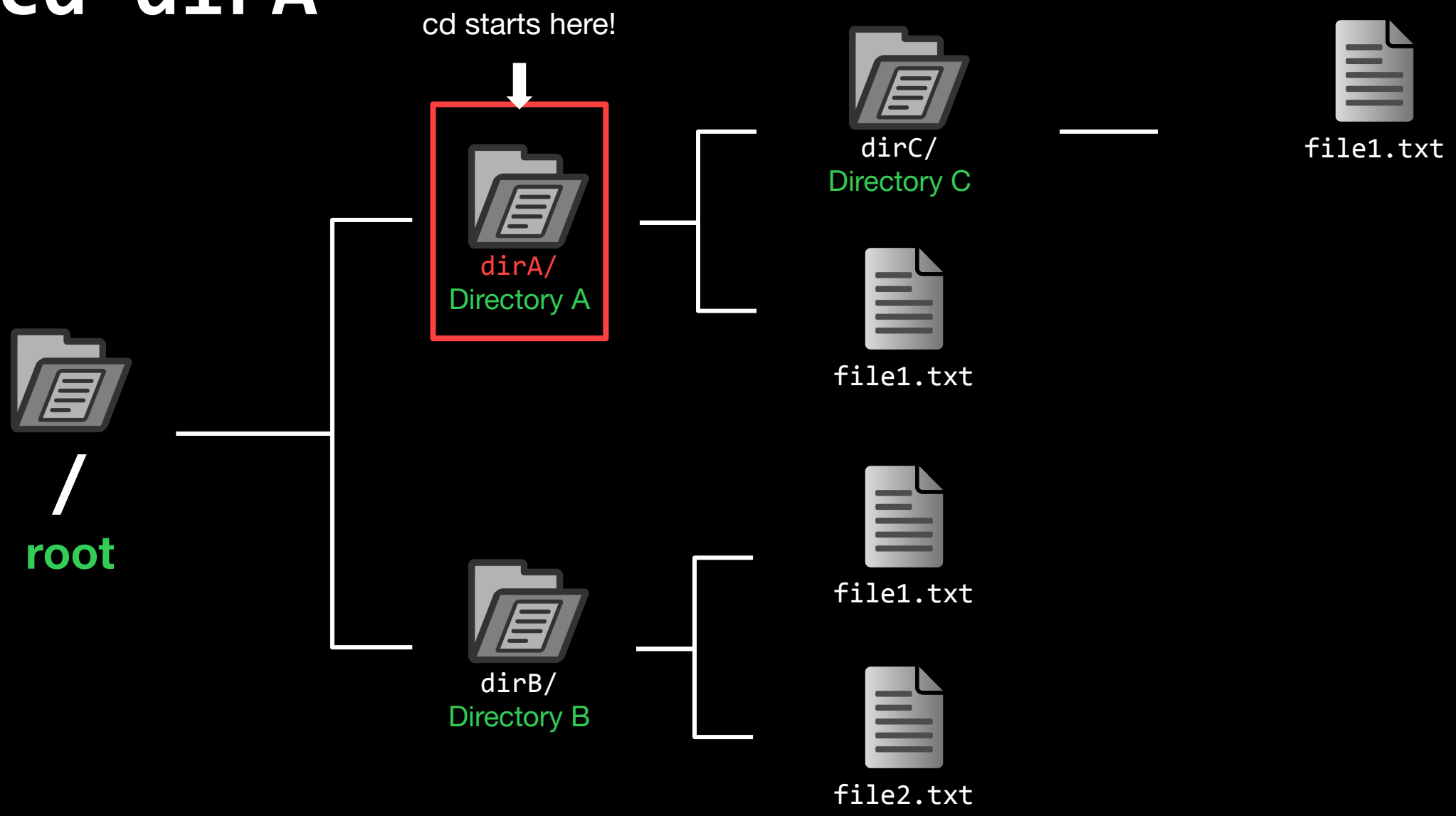
cd /

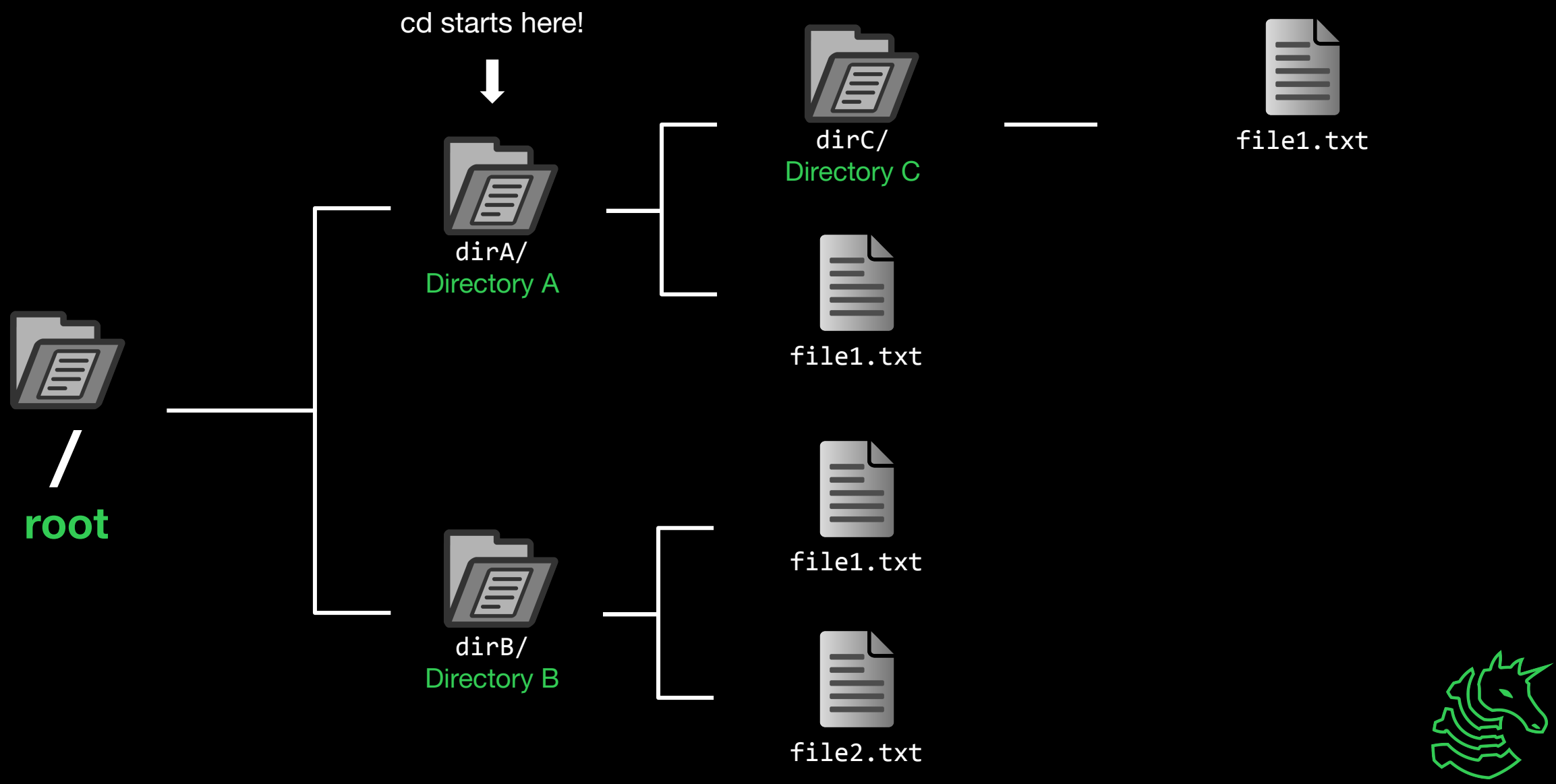

/
root
dirA/
Directory A
dirB/
Directory B
dirC/
Directory C
file1.txt
file1.txt
file1.txt
file2.txt
file1.txt

cd dirA

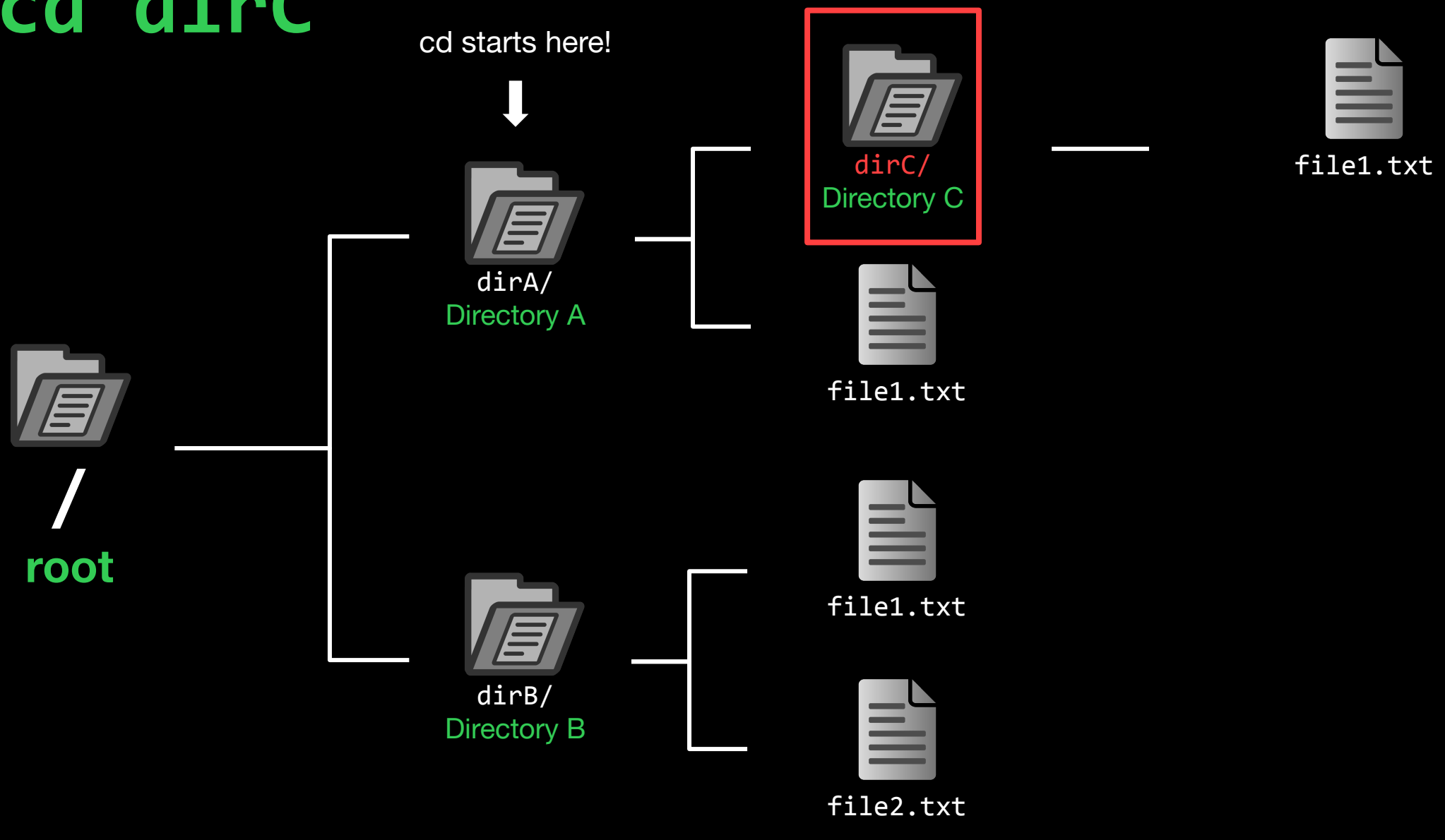

/
root
cd starts here!
dirA/
Directory A
dirB/
Directory B
dirC/
Directory C
file1.txt
file1.txt
file1.txt
file2.txt

cd dirA

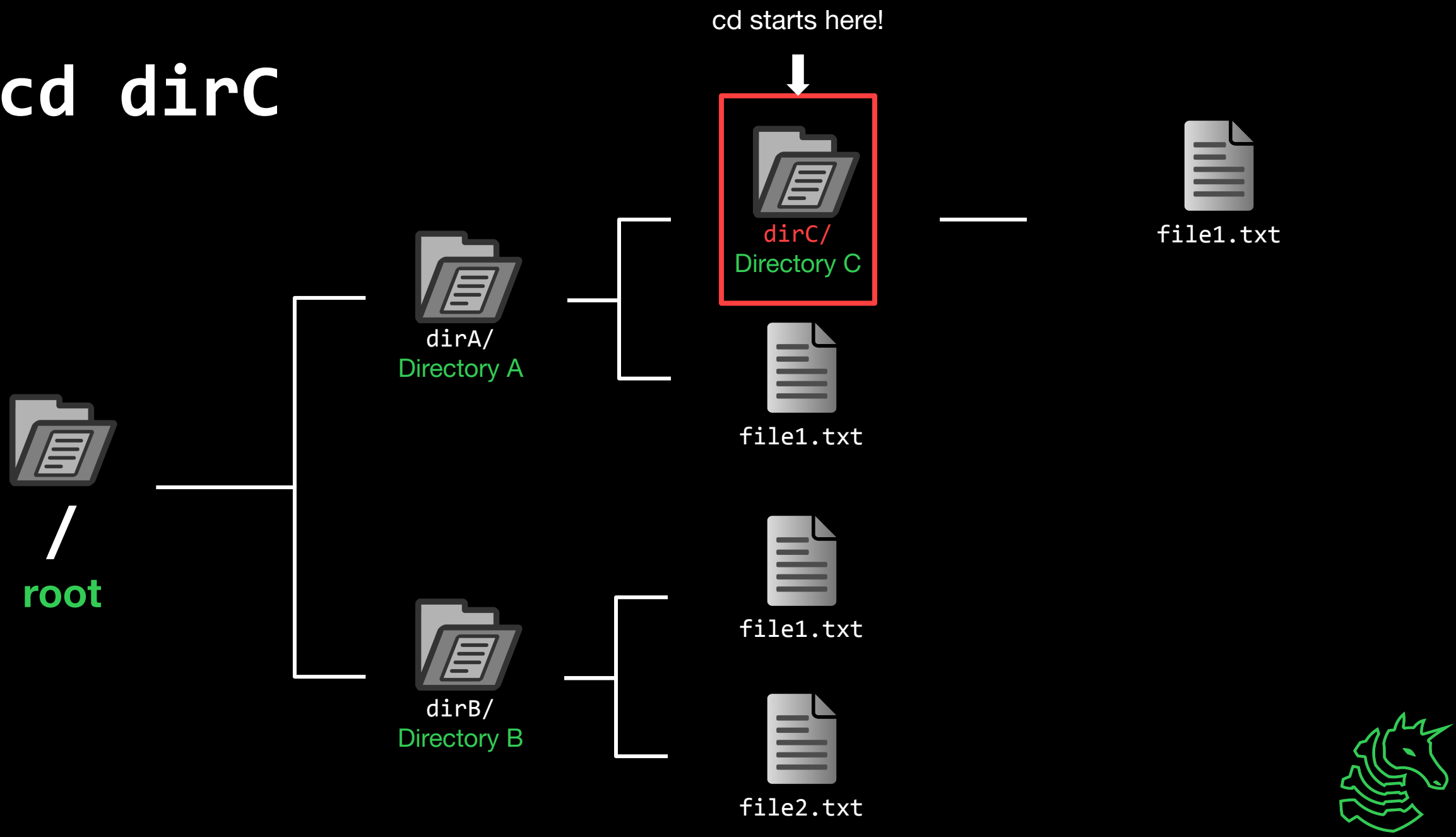

cd starts here!
/
root
dirA/
Directory A
dirB/
Directory B
dirC/
Directory C
file1.txt
file1.txt
file1.txt
file2.txt

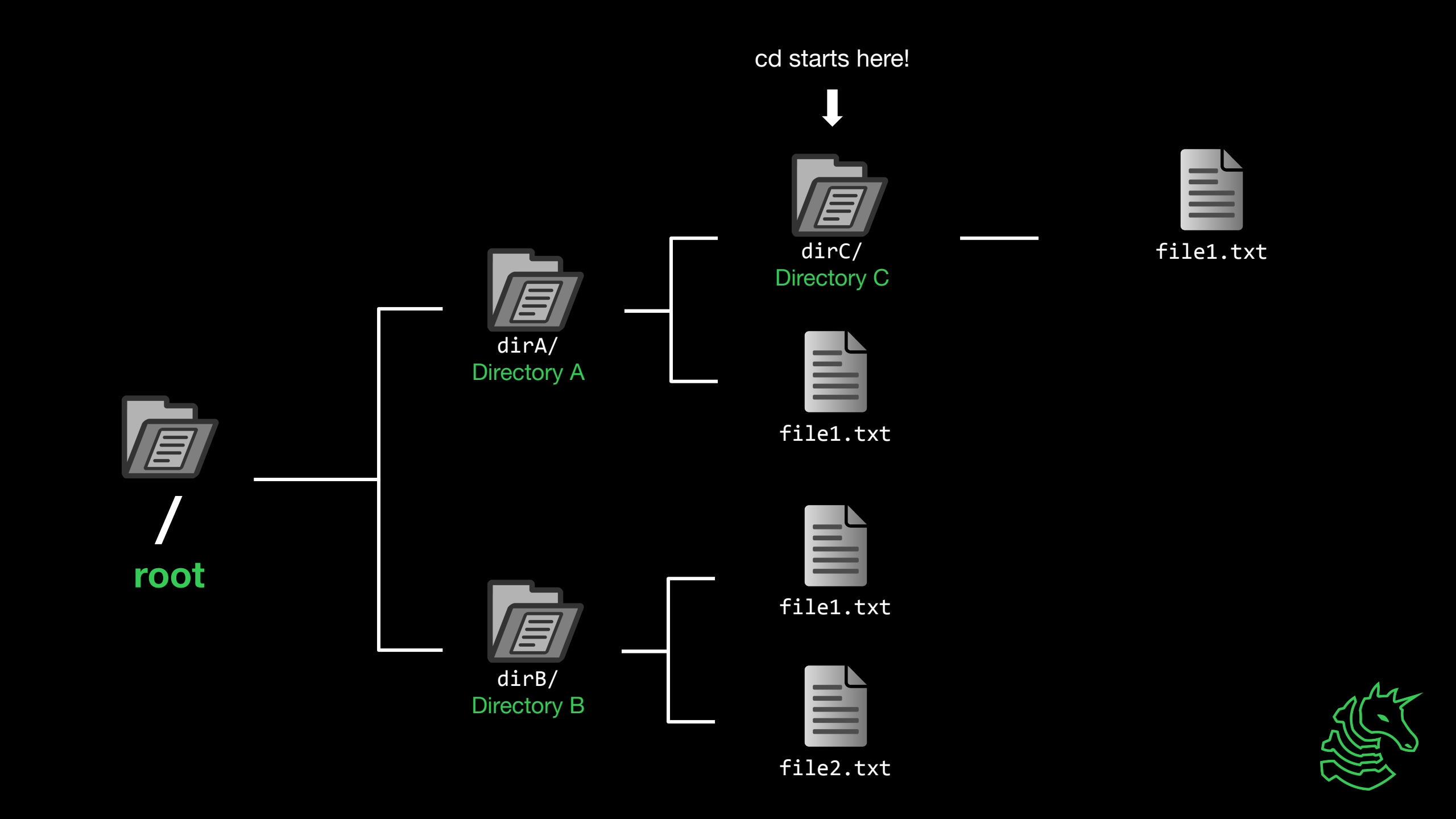

cd starts here!
/
root
dirA/
Directory A
dirB/
Directory B
dirC/
Directory C
file1.txt
file1.txt
file1.txt
file2.txt
file1.txt

cd dirC

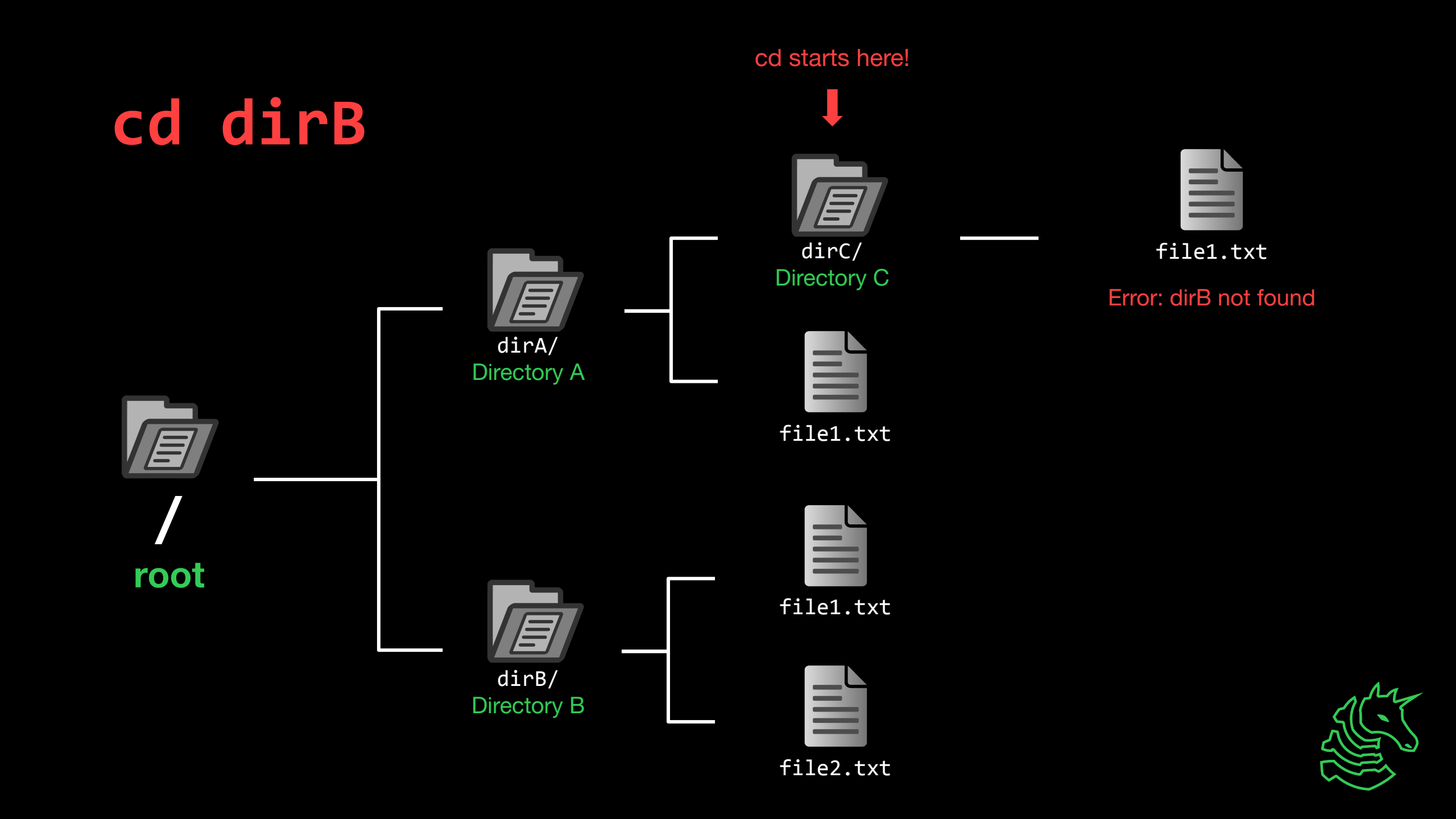

cd starts here!
/
root
dirA/
Directory A
dirB/
Directory B
dirC/
Directory C
file1.txt
file1.txt
file1.txt
file2.txt

cd dirC

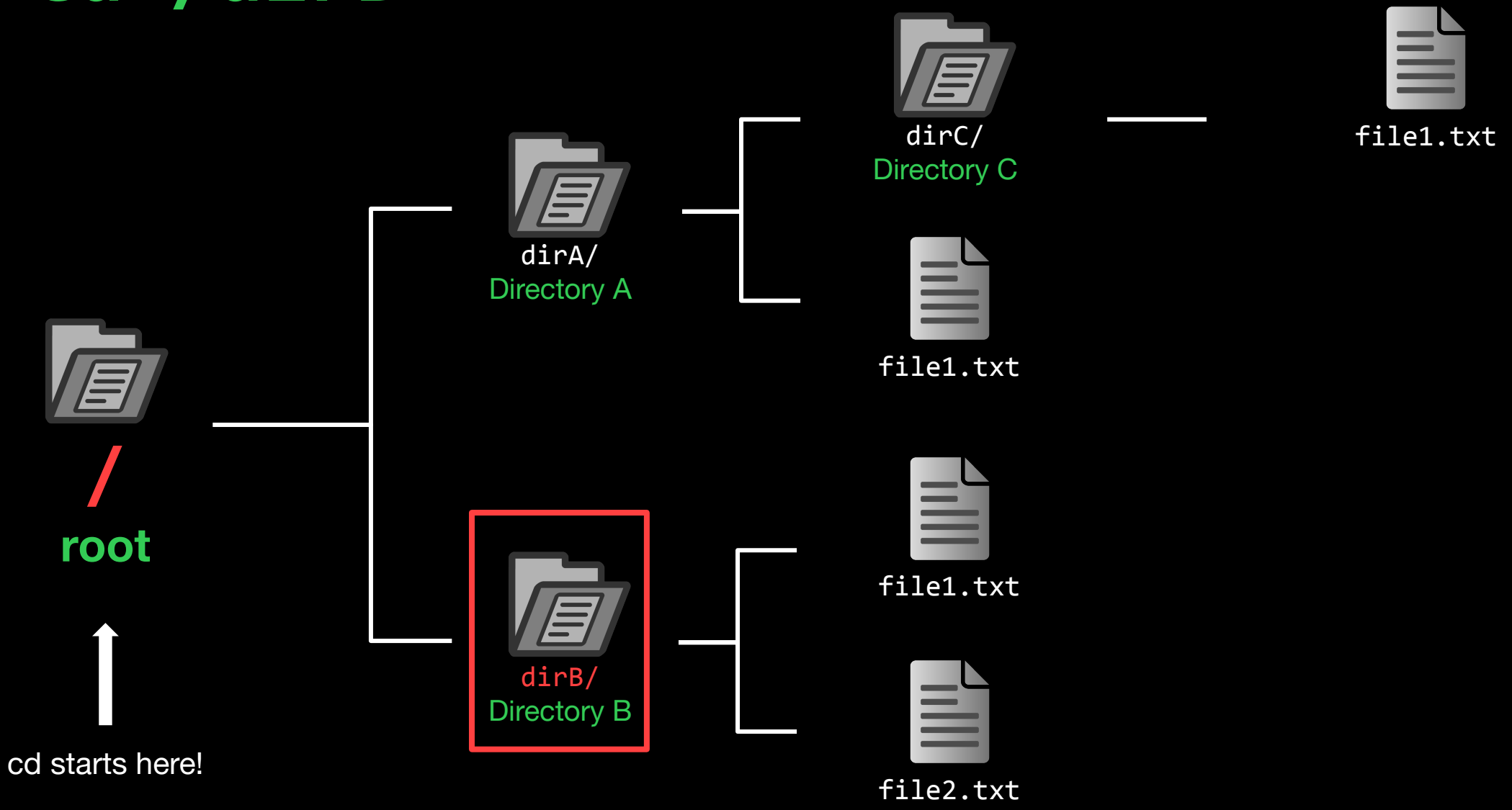

cd starts here!
/
root
dirA/
Directory A
dirB/
Directory B
dirC/
Directory C
file1.txt
file1.txt
file1.txt
file2.txt


cd starts here!
/
root
dirA/
Directory A
dirB/
Directory B
dirC/
Directory C
file1.txt
file1.txt
file1.txt
file2.txt

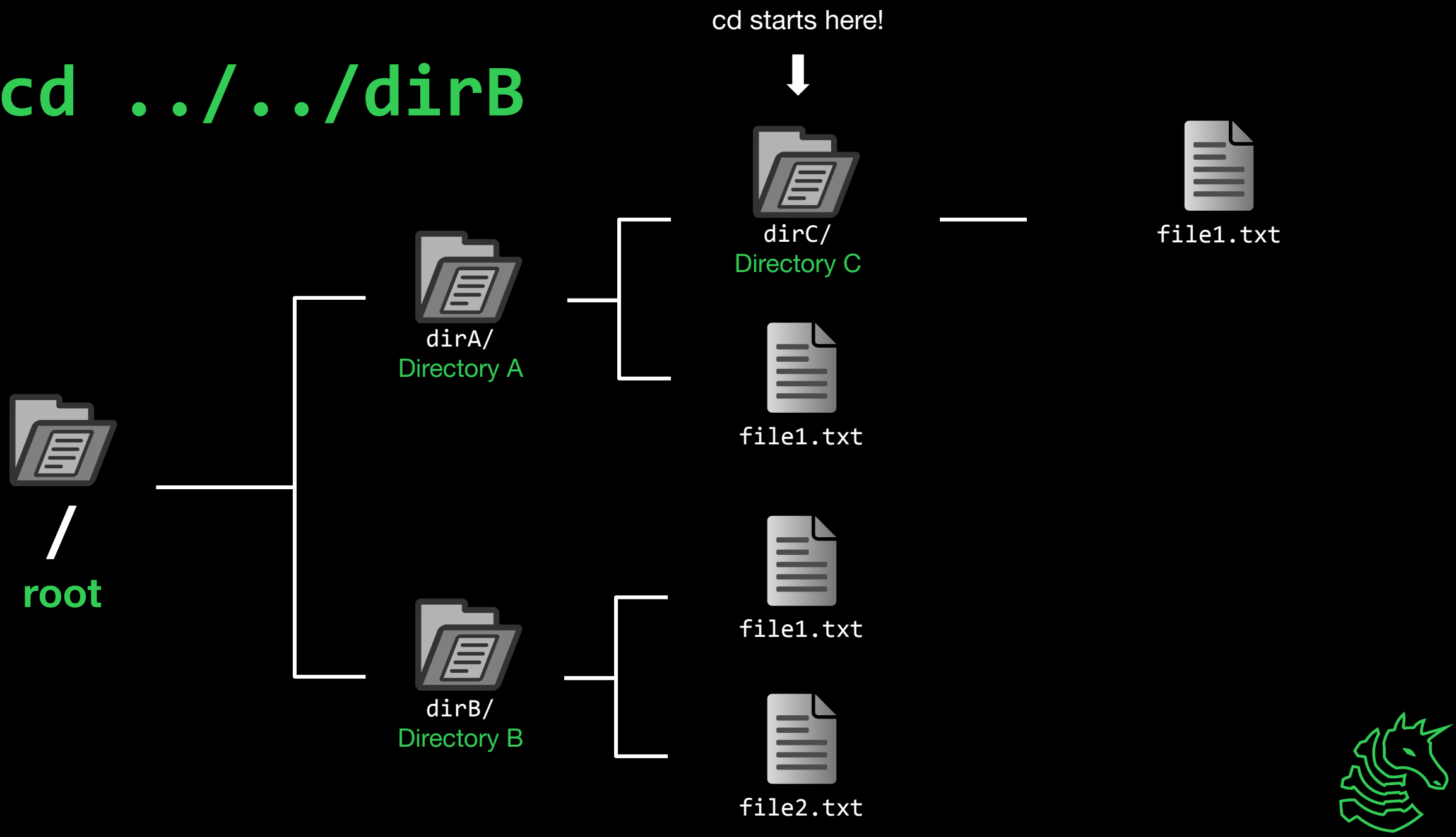
cd dirB


cd starts here!
dirC/
Directory C
file1.txt
Error: dirB not found
dirA/
Directory A
file1.txt
/
root
file1.txt
dirB/
Directory B
file2.txt

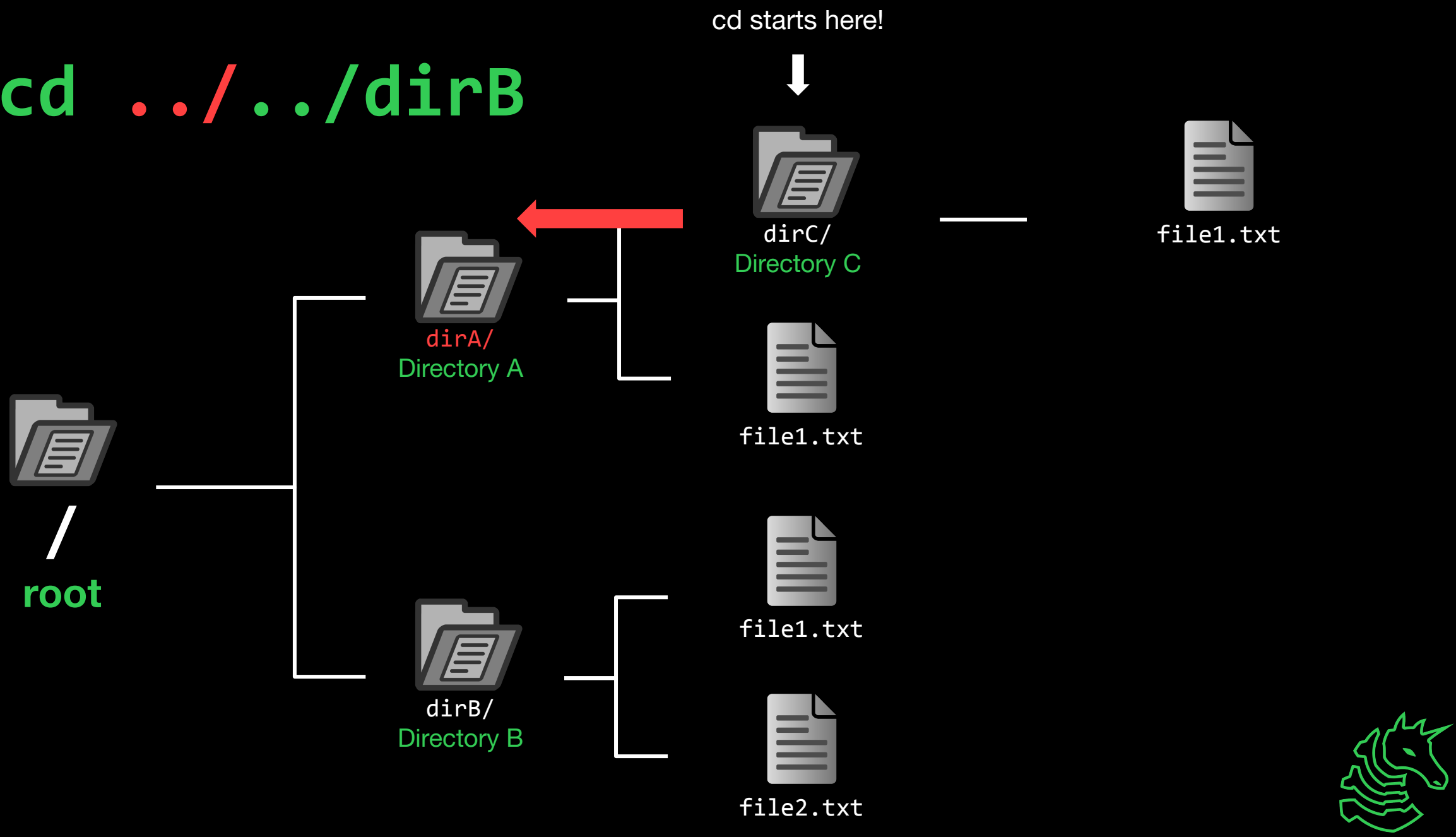
cd /dirB

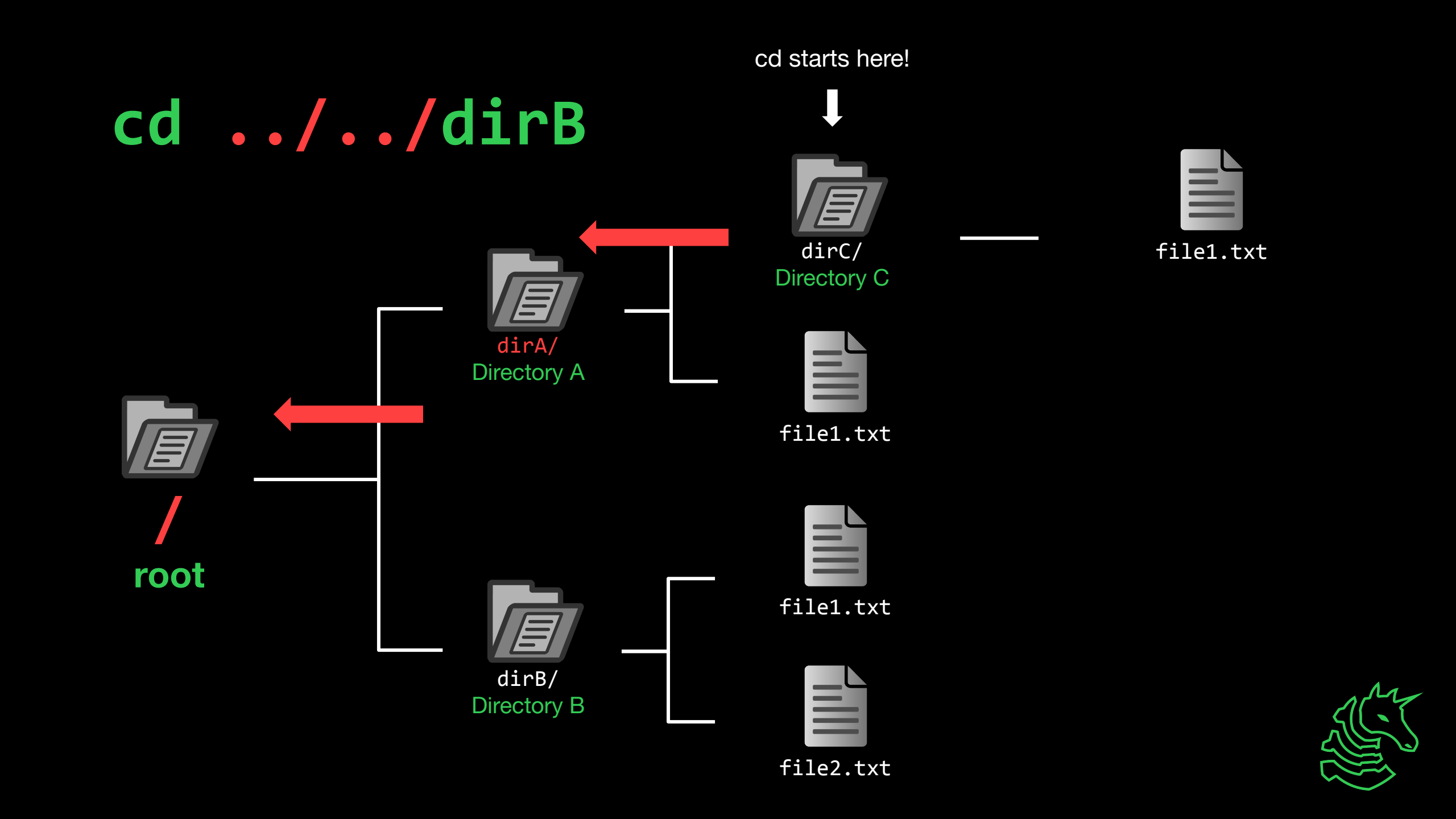

/
root
cd starts here!
dirA/
Directory A
dirB/
Directory B
dirC/
Directory C
file1.txt
file1.txt
file1.txt
file2.txt
file1.txt

cd ../../dirB

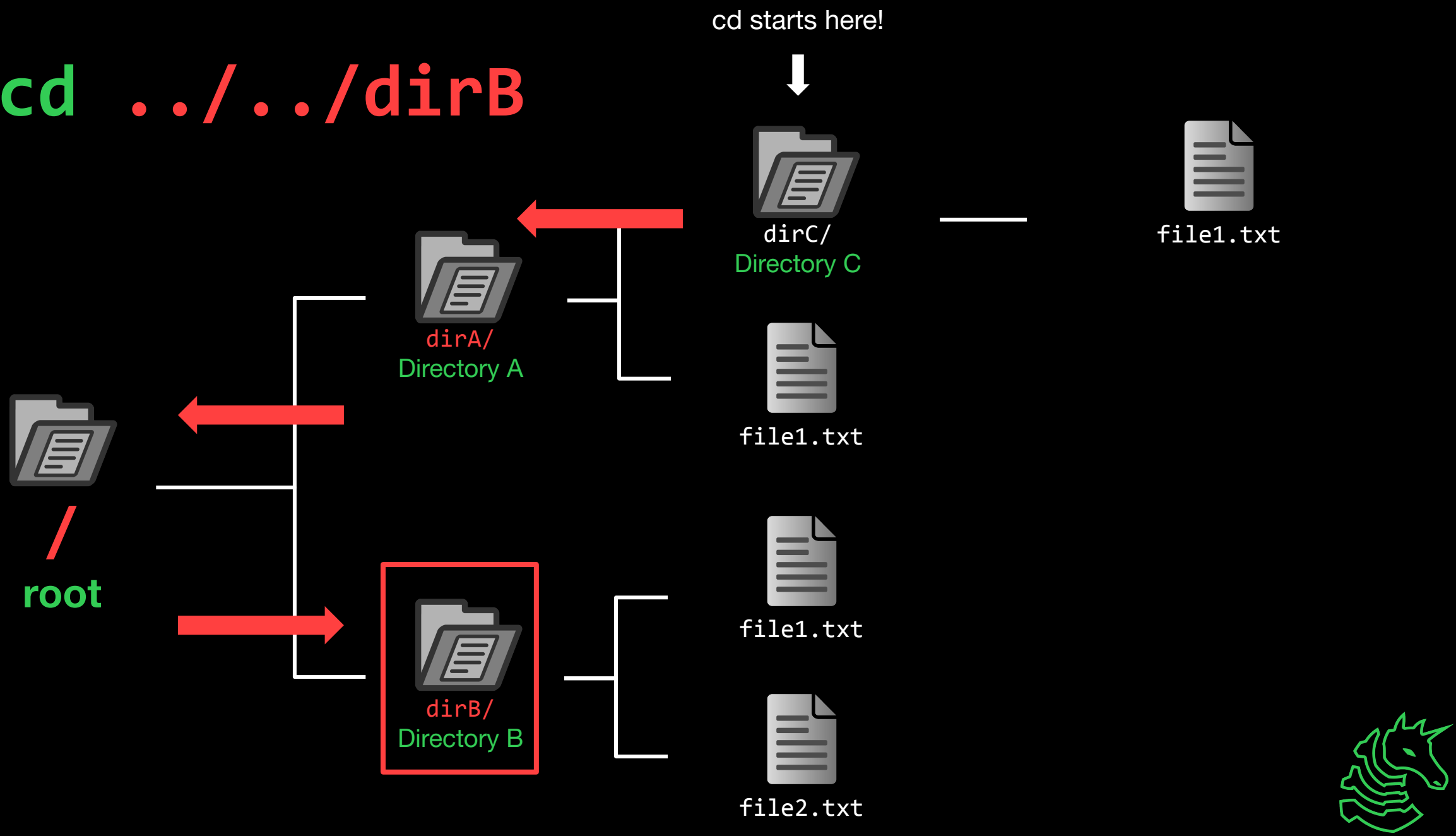

cd starts here!
dirC/
Directory C
file1.txt
dirA/
Directory A
file1.txt
/
root
file1.txt
dirB/
Directory B
file2.txt

cd ../../dirB

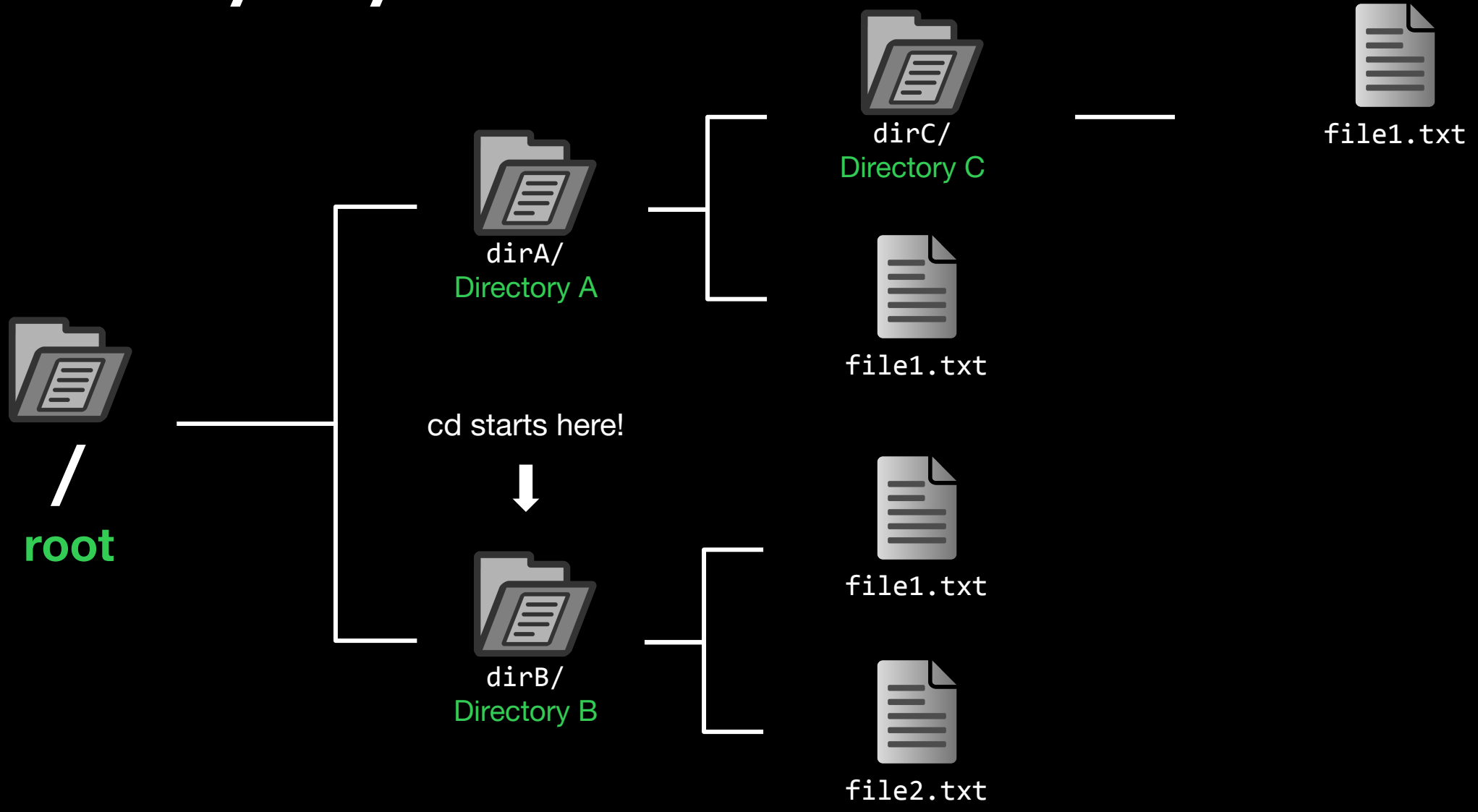

cd starts here!
dirC/
Directory C
file1.txt
dirA/
Directory A
file1.txt
/
root
file1.txt
dirB/
Directory B
file2.txt


cd ../../dirB
cd starts here!
dirC/
Directory C
file1.txt
dirA/
Directory A
file1.txt
/
root
file1.txt
dirB/
Directory B
file2.txt

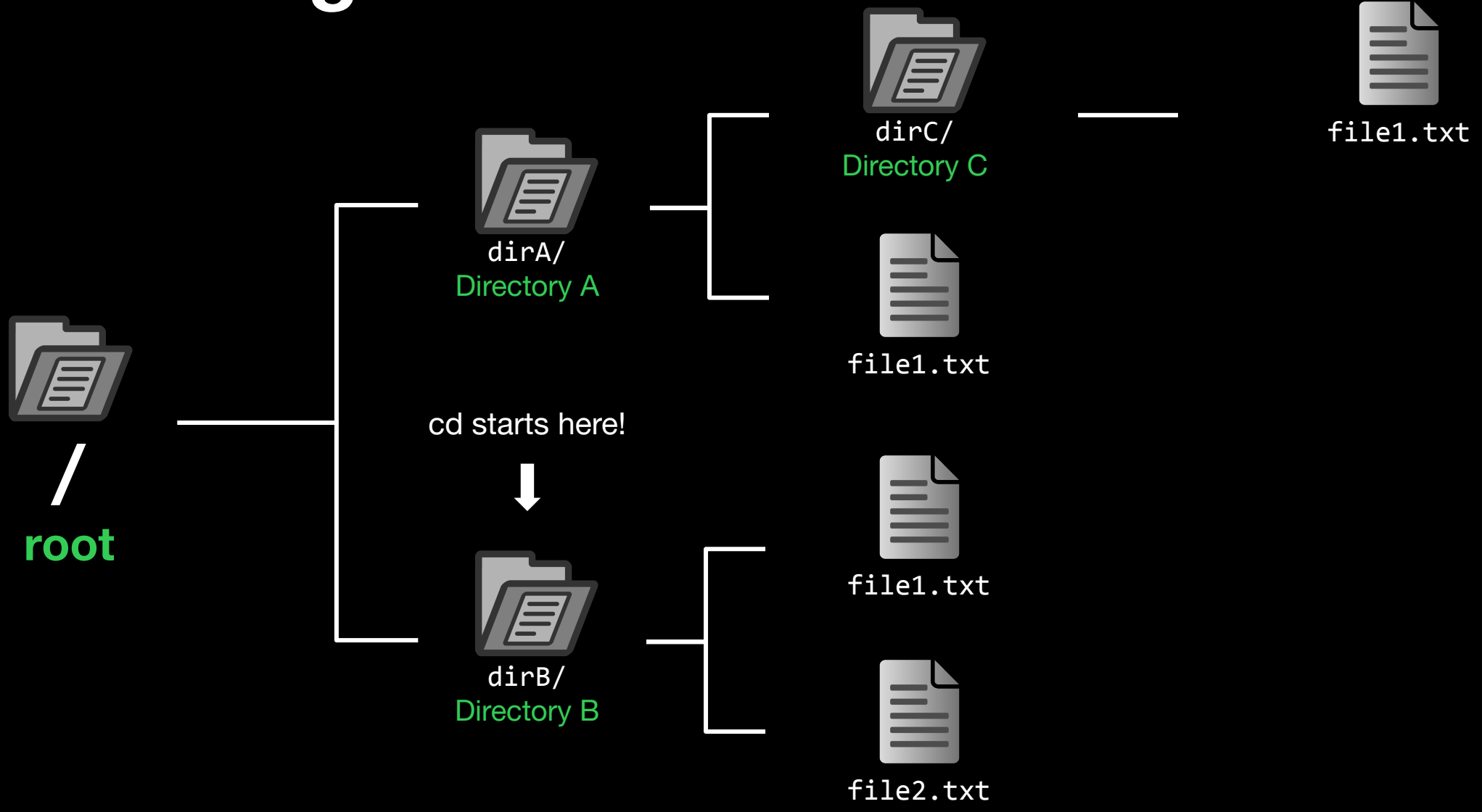
cd ../../dirB


cd starts here!
dirC/
Directory C
file1.txt
dirA/
Directory A
file1.txt
/
root
file1.txt
dirB/
Directory B
file2.txt

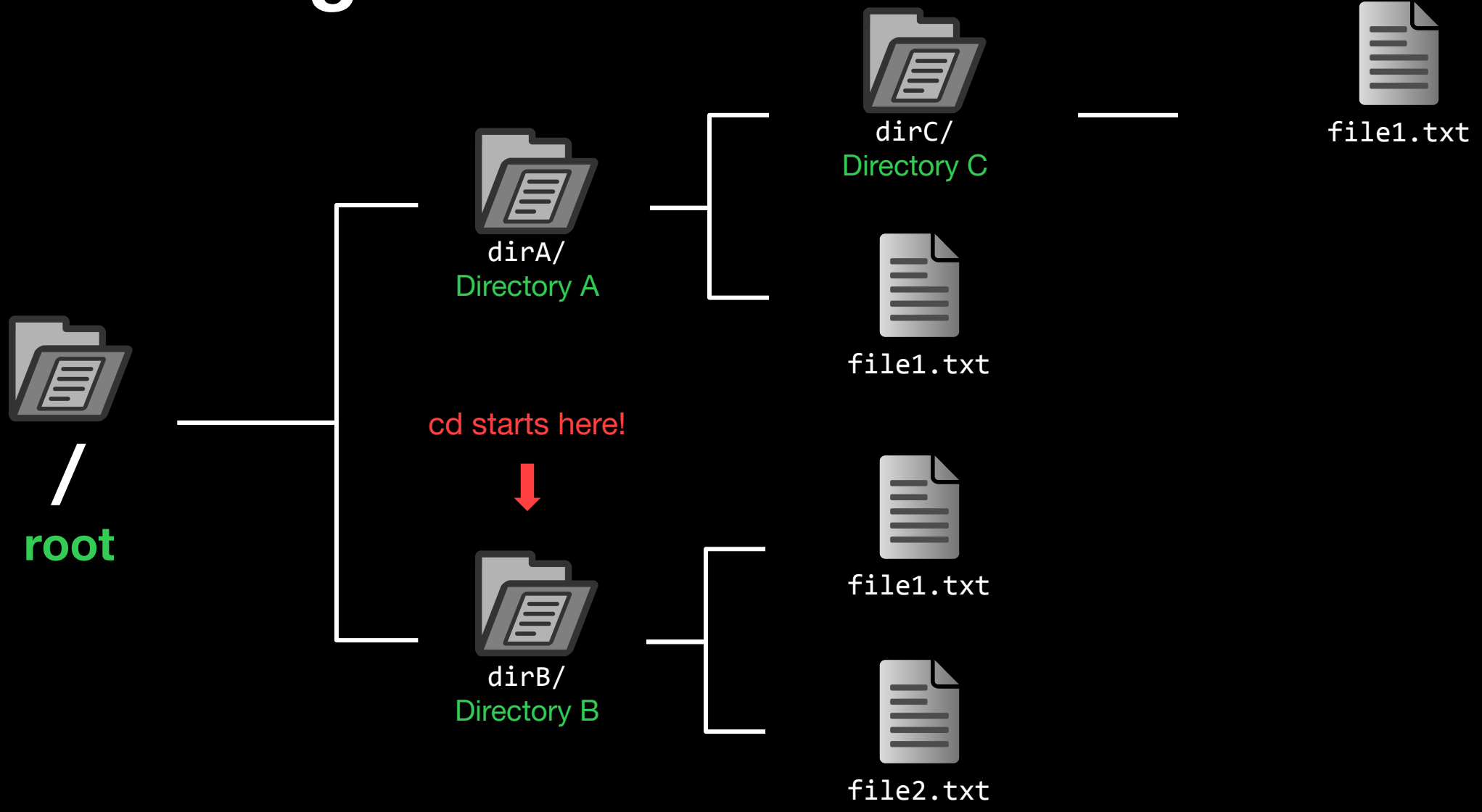
cd ../../dirB


/
root
dirA/
Directory A
dirC/
Directory C
file1.txt
file1.txt
cd starts here!
dirB/
Directory B
file1.txt
file2.txt

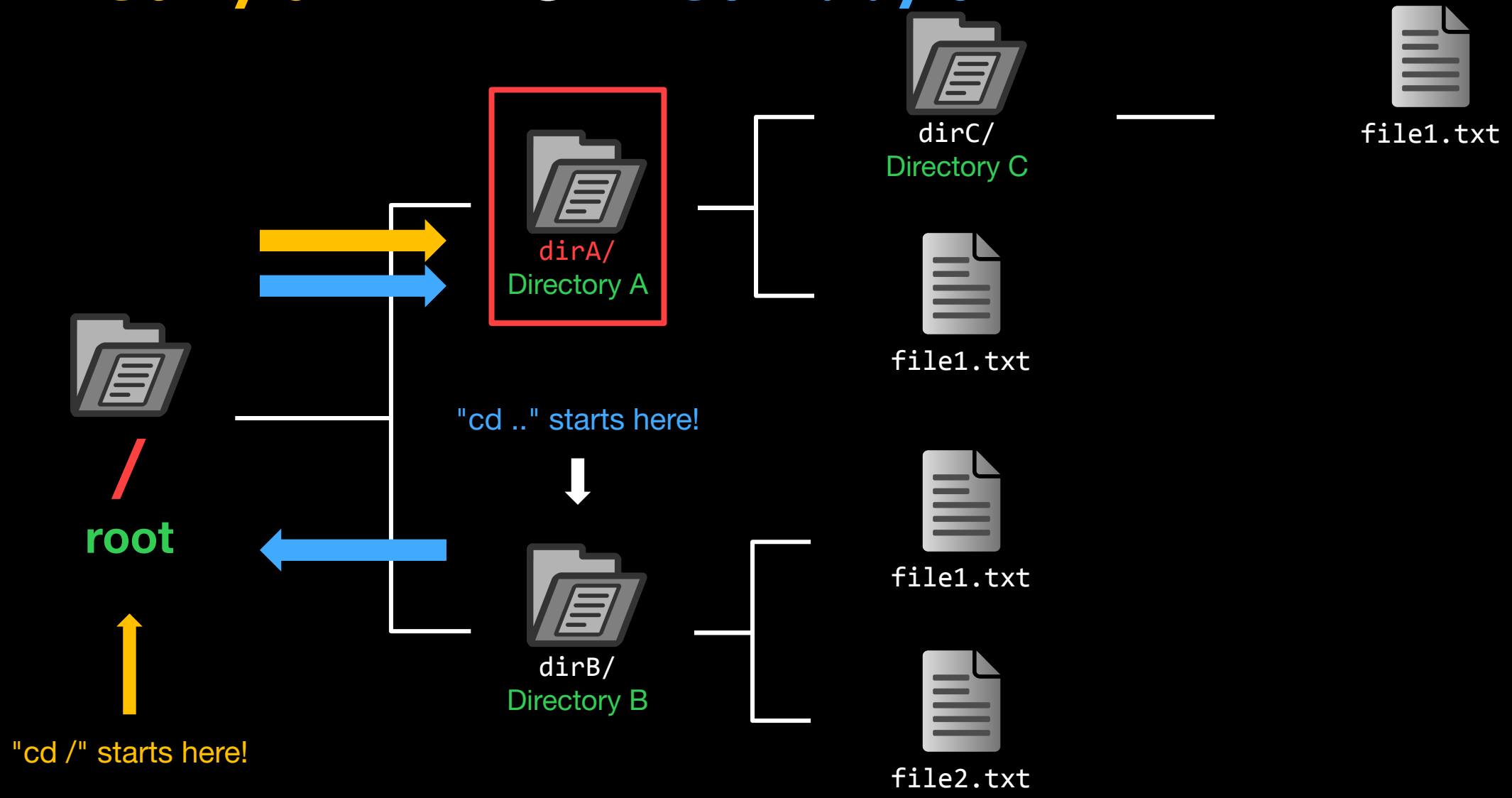
How to get to dirA?



How to get to dirA?



"cd /dirA" or "cd ../dirA"



Paths

Absolute Path

The full path that always starts at root (/)

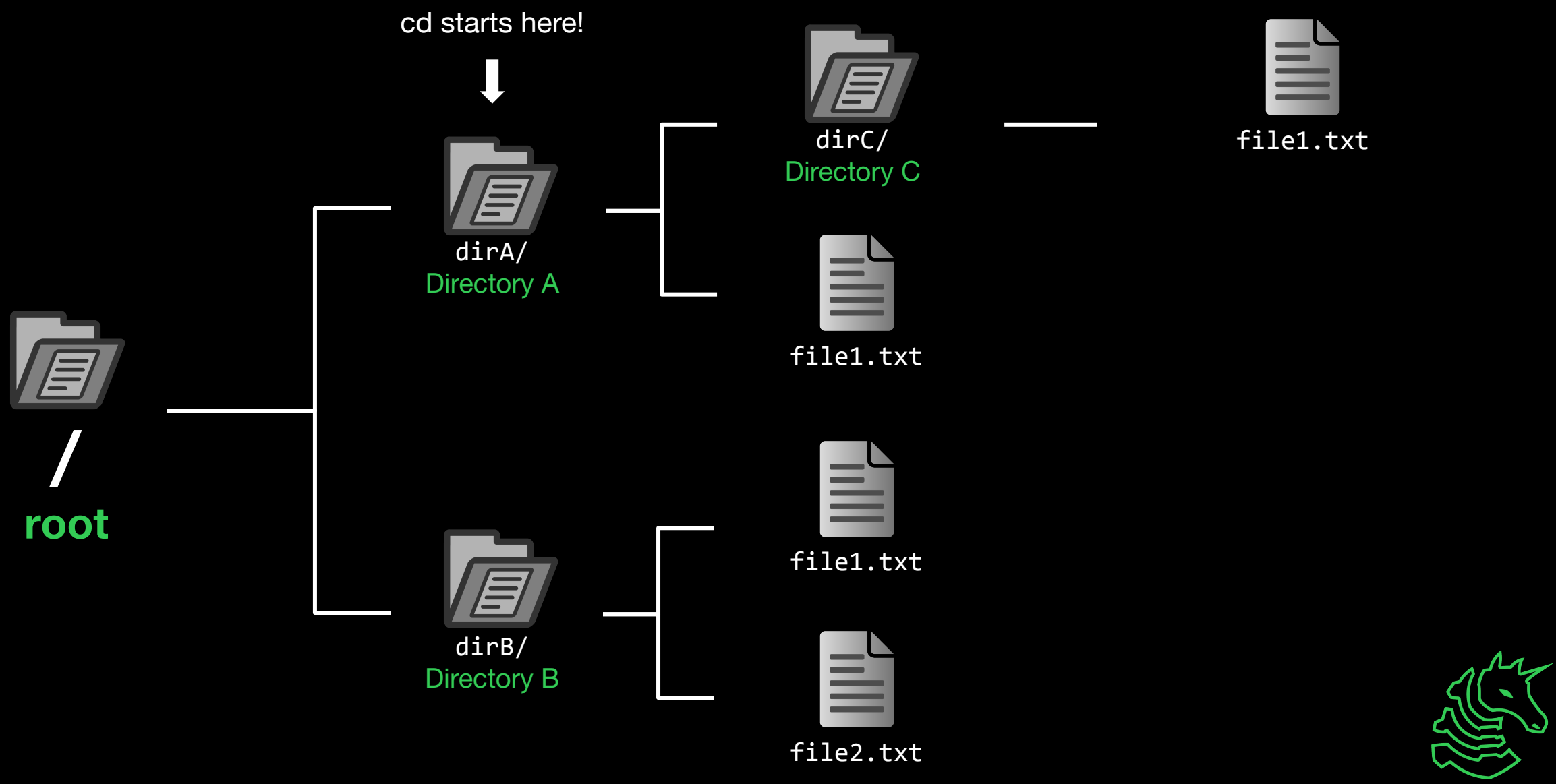
```
/dirA/file1.txt
/dirA/dirC/file1.txt
```

Relative Path

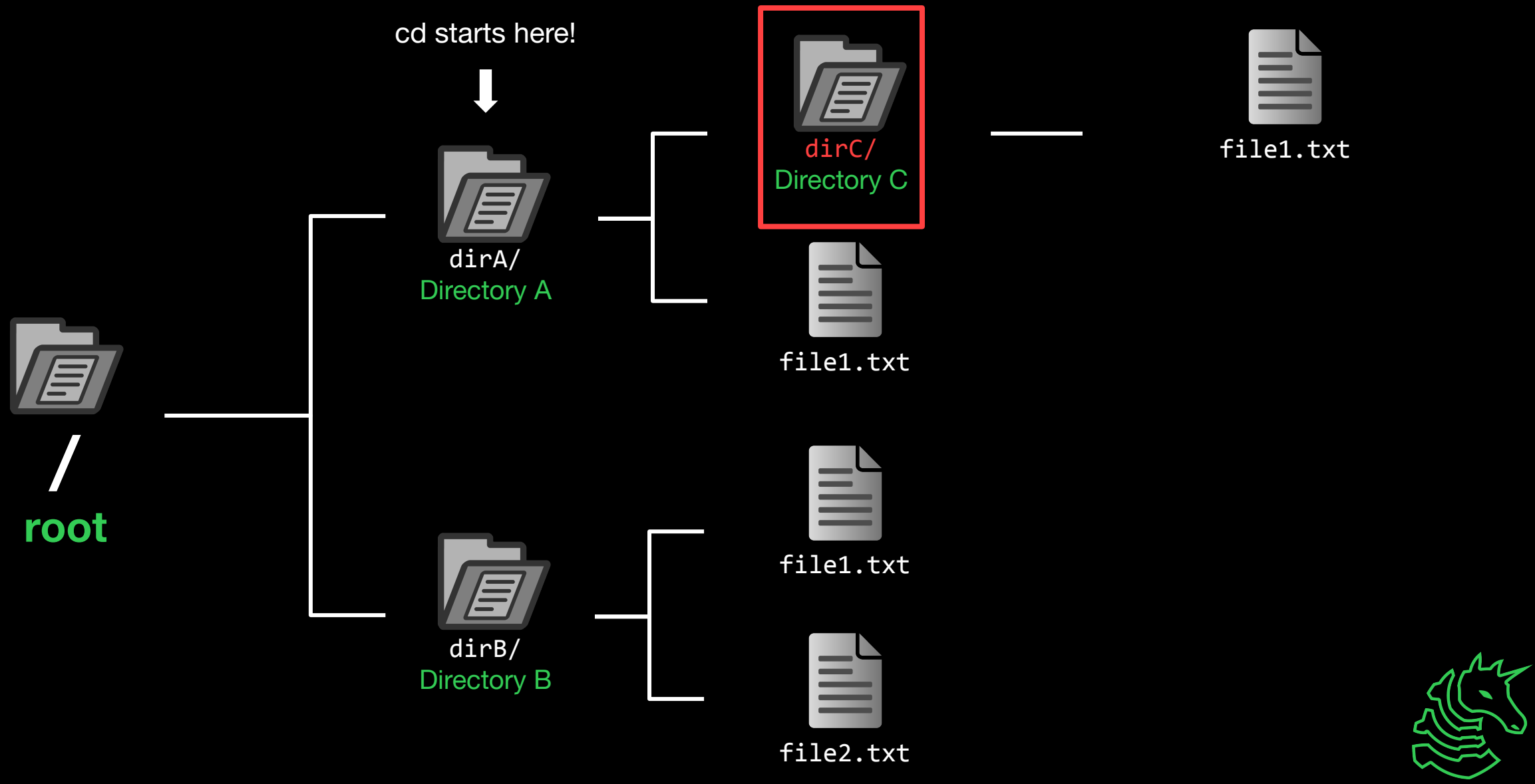
The partial path relative to where you are currently in the terminal

(Relative to dirA)

```
file1.txt
dirC/file1.txt
```


cd starts here!
/
root
dirA/
Directory A
dirB/
Directory B
dirC/
Directory C
file1.txt
file1.txt
file1.txt
file2.txt
file1.txt

"cd dirC" or "cd ./dirC" or "cd dirC/"



`./dirC == dirC == dirC/`

Also `./../dirC` and `./../../dirC` and `./../../../dirC` and...

These are just conventions!

Useful Commands - Filesystem

`ls <directory>`: lists files in your current directory or specified directory

`cd <directory>`: changes your current directory to specified directory

`mv <source> <dest>`: moves file from source to dest (rename), if dest is a directory, move source

`rm <file>`: removes file (**NOT REVERSIBLE**)

`cat <file>`: prints the contents of file (sometimes it prints gibberish, think why that might happen)

`./file`: executes whatever is at file

`man <command>`: lets you see info about a command and all of its parameters/options

`<parameter>` means it's a required parameter

`[parameter]` means it's an optional parameter

Useful Commands - Networking

`nc <ip> <port>`: netcat, connect to ip on port port. (first command - netcat)

`ssh <user@ip> [port]`: secure remote shell, run an instance of a shell as user at the IP address

`ping <ip>`: see if an IP address is up using ICMP (usually blocked by firewalls)

`curl <url>`: network access tool that is mainly used to access websites from the terminal

`wget <url>`: Simplified/modern curl that downloads the file with relevant name

Networking Fundamentals

`nc -l <port>`: open a network socket to listen on specified port

`nc <ip> <port>`: open a connection to the specified IP and port

Ports - communication endpoints on your computer (1-65535)

Next Steps - Bandit

```
ssh bandit0@bandit.labs.overthewire.org -p 2220
```

Next Steps - Bandit

```
ssh bandit0@bandit.labs.overthewire.org -p 2220
```

command user IP port

Next Steps - Terminal Challenges

- **netcat**
  - Refer back to the slides!
- **Shell Basics**
  - Learn the ins and outs of using the terminal
- **A Very Special Character**
  - Intro to the ASCII table and Netcat

Next Meetings

2023-09-14 • This Thursday

- Web Hacking II
- Learn the power of malicious user inputs!

2023-09-17 • Next Sunday

- Reverse Engineering I
- Dig into unknown programs and learn what they do

2023-09-21 • Next Thursday

- Open Source Intelligence (OSINT)
- Master the art of public information gathering

ctf.sigpwny.com

`sigpwny{starting_off_strong}`

Meeting content can be found at sigpwny.com/meetings.

SIGPwny