SIGPwny

FA2023 Week 01 • 2023-09-03

Intro to Terminal and Setup

Pete and Emma

Announcements

- Fall CTF registration open!
  - sigpwny.com/register23
  - Event on September 23rd 12- 6 PM, register by September 7th for a free t-shirt!

- First group CTF of the year: PatriotCTF!
  - Play collaboratively with everyone (room TBD), get some free pizza, have a blast with us!
  - September 8th 4PM CST - 10th

- ACM Open House
  - Watch our cool demo and learn more about larger ACM (free pizza!)
  - Tuesday, September 5th 6:30PM CST

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

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**

ctf.sigpwny.com

sigpwny{starting_off_strong}

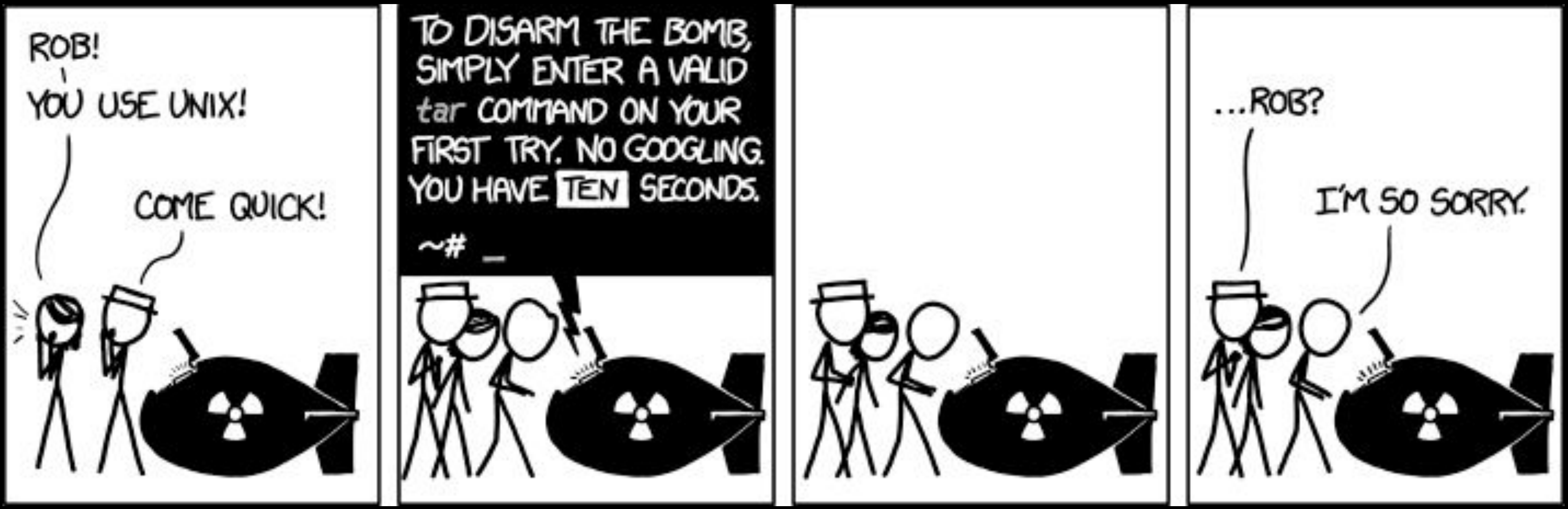
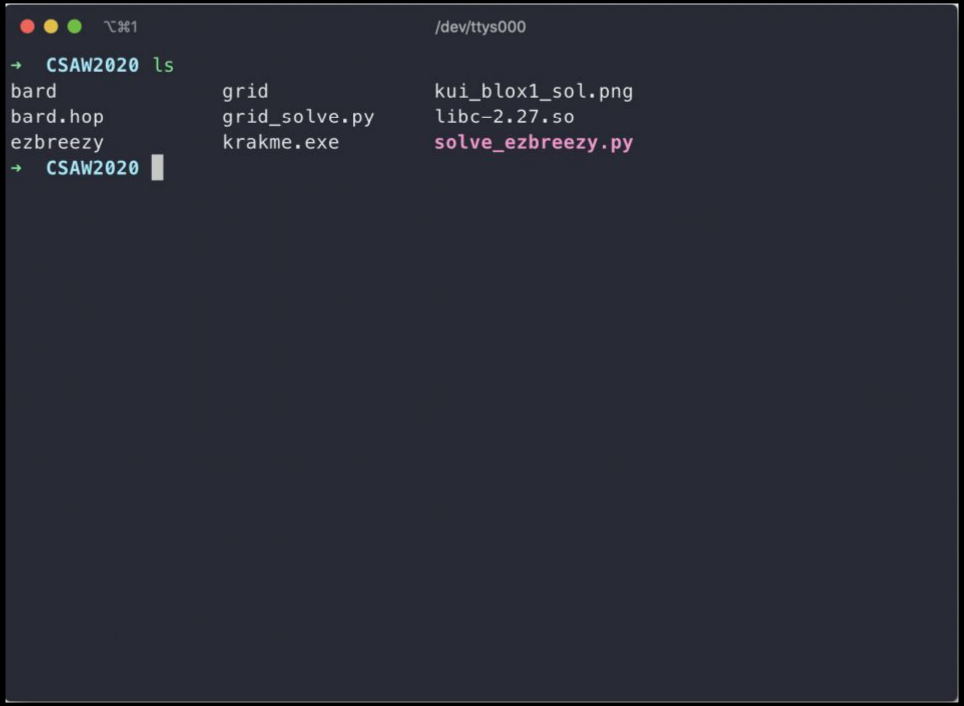

ROB!
YOU USE UNIX!
COME QUICK!
TO DISARM THE BOMB, SIMPLY ENTER A VALID tar COMMAND ON YOUR FIRST TRY. NO GOOGLING. YOU HAVE TEN SECONDS.
~# _
...ROB?
I'M SO SORRY.

Table of Contents

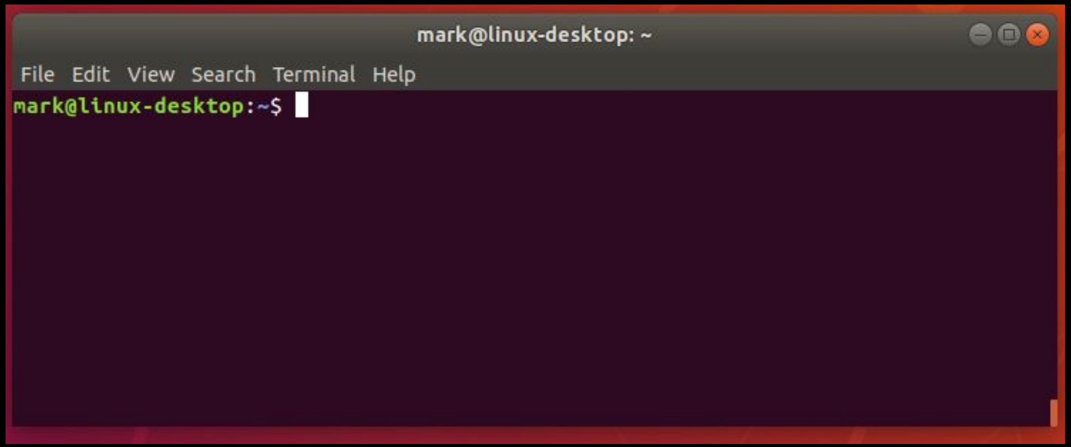
- What is a shell
    - I want one
- Getting into the shell
    - OS Differences + Different Shells
    - WSL or Virtual Machines?
    - Installing WSL
- Starter commands
- Tools to install

> The Terminal

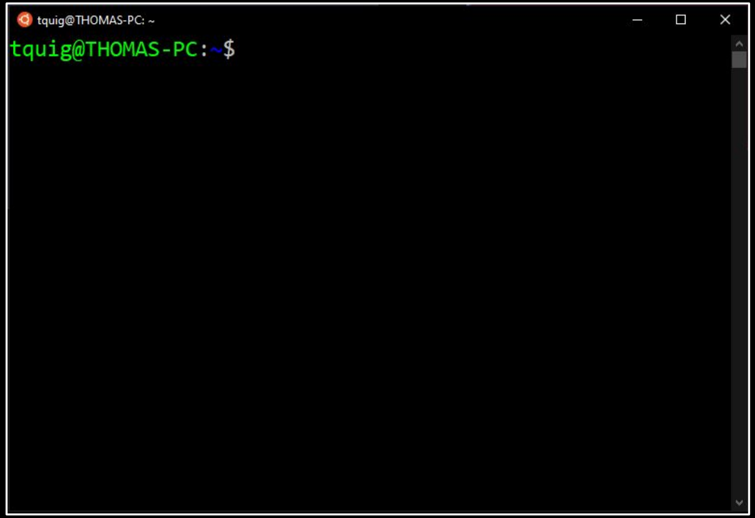
"It’s where things happen" - Ravi



```
➜  CSAW2020 ls
bard              grid              kui_blox1_sol.png
bard.hop          grid_solve.py     libc-2.27.so
ezbreezy          krakme.exe        solve_ezbreezy.py
➜  CSAW2020
```



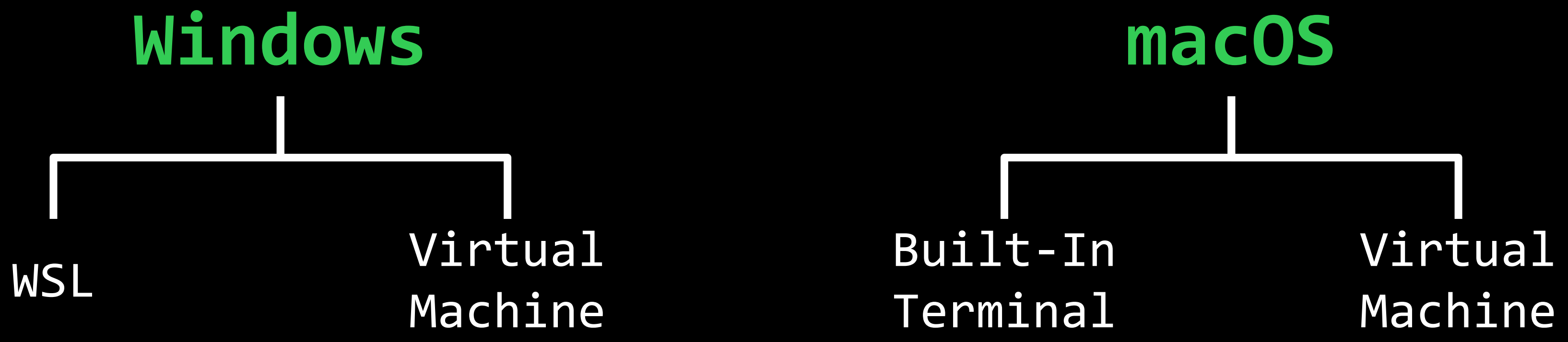
```
mark@linux-desktop:~$
```



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

Linux

You’re good to go!



Windows

WSL

Virtual Machine

macOS

Built-In Terminal

Virtual Machine

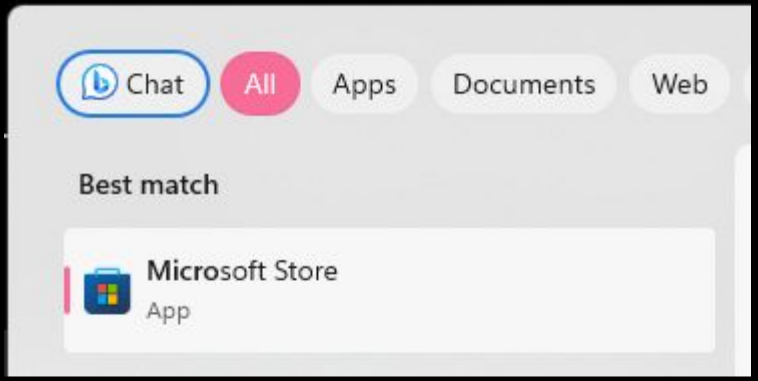
PowerShell? Command Prompt?

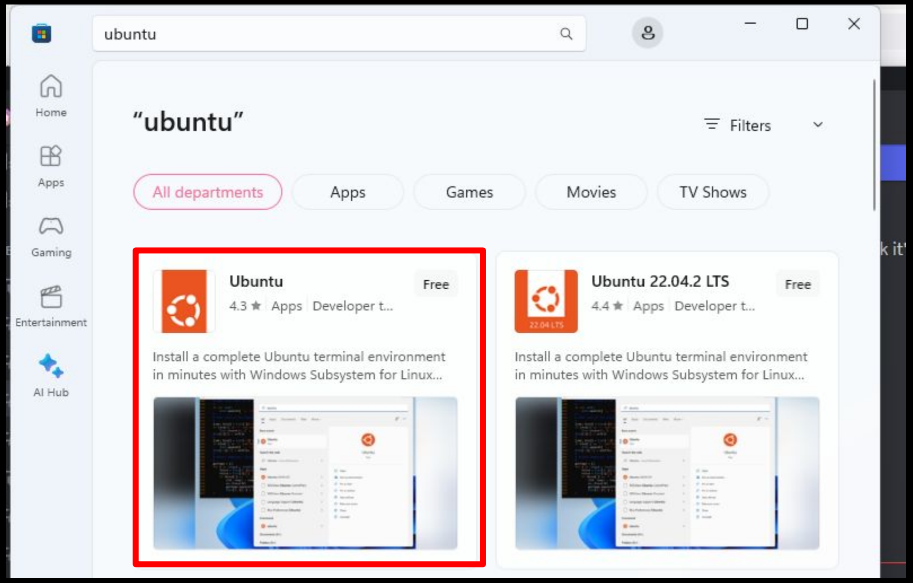
- Those are shells too!
- However, the Windows terminal is built differently than the Mac and Linux terminals (which are both UNIX based)
  - Different command structure/rules
  - Less support for CTF relevant applications

Windows Subsystem for Linux

Getting A Terminal

Open the Microsoft Store → Search “Ubuntu” →





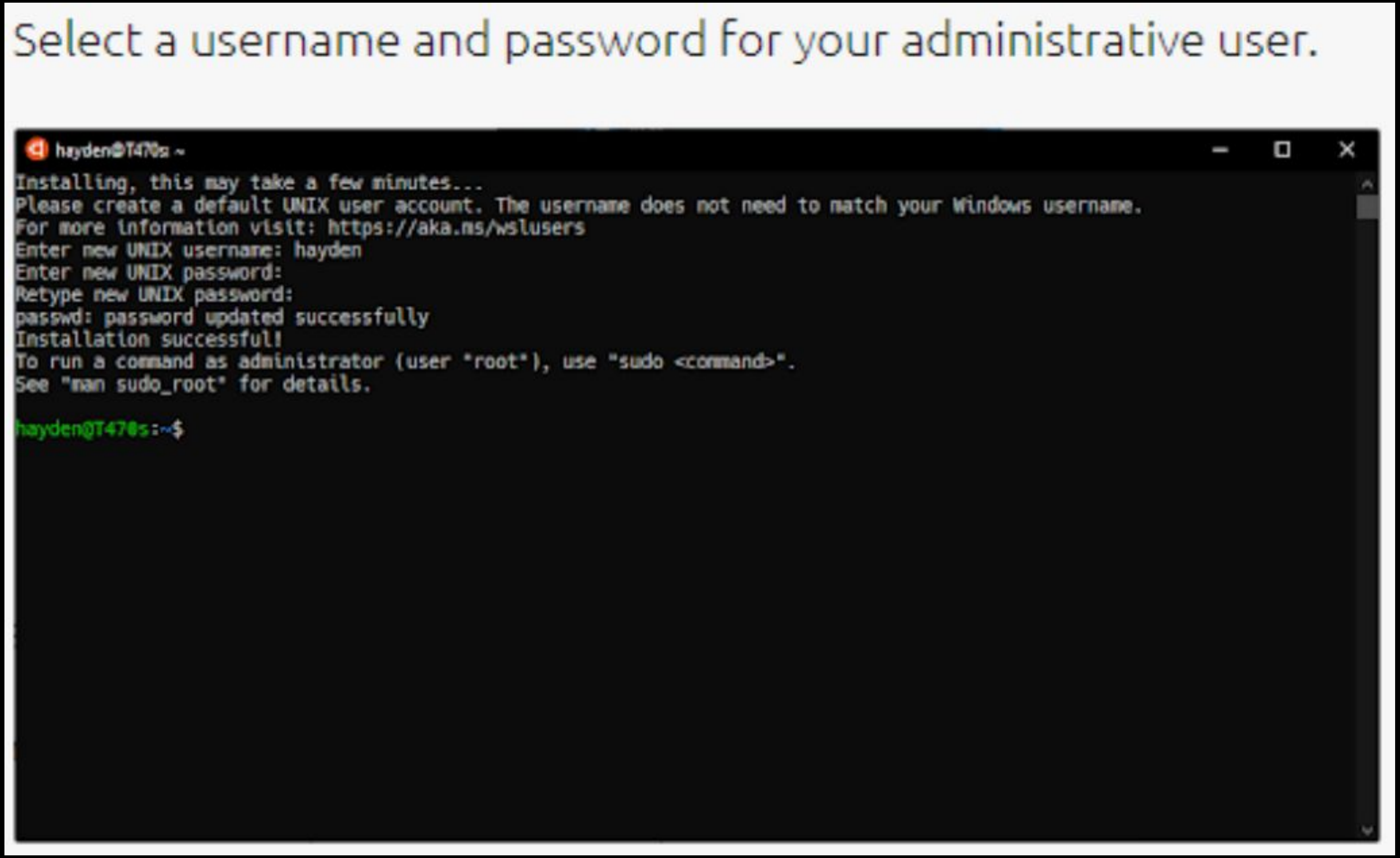
Ubuntu 4.3 ★ Apps Developer t... Free

Install a complete Ubuntu terminal environment in minutes with Windows Subsystem for Linux...

Ubuntu 22.04.2 LTS 4.4 ★ Apps Developer t... Free

Install a complete Ubuntu terminal environment in minutes with Windows Subsystem for Linux...

Set a "root" user



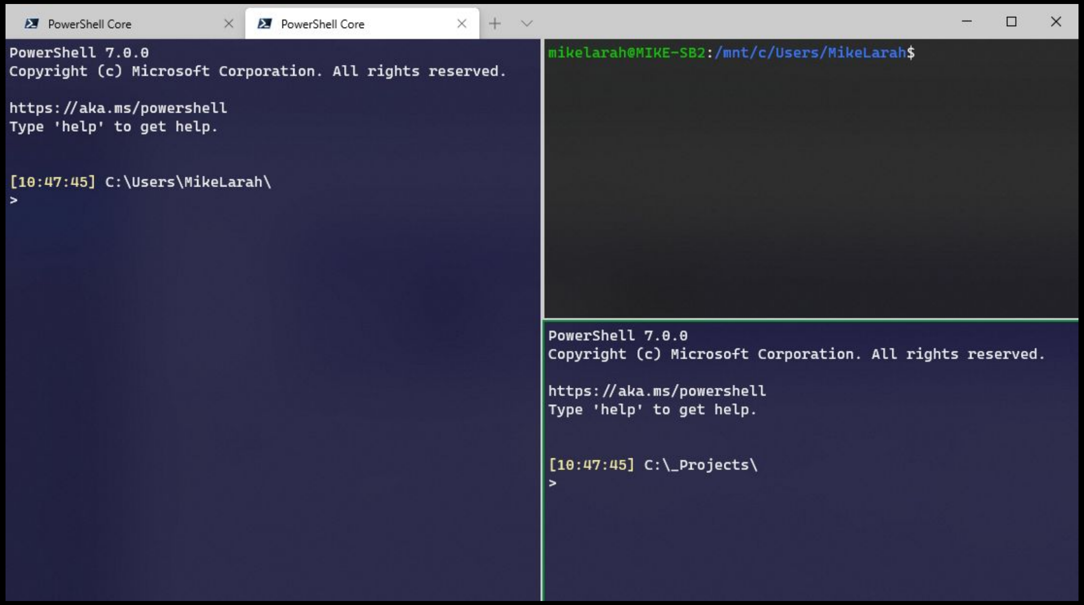
Select a username and password for your administrative user.

```
Installing, this may take a few minutes...
Please create a default UNIX user account. The username does not need to match your Windows username.
For more information visit: https://aka.ms/wslusers
Enter new UNIX username: hayden
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
Installation successful!
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

hayden@T470s:~$
```

Windows Terminal (Optional)

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



```
PowerShell 7.0.0
Copyright (c) Microsoft Corporation. All rights reserved.

https://aka.ms/powershell
Type 'help' to get help.


[10:47:45] C:\Users\MikeLarah\
>
```

```
mikelarah@MIKE-SB2:/mnt/c/Users/MikeLarah$
```

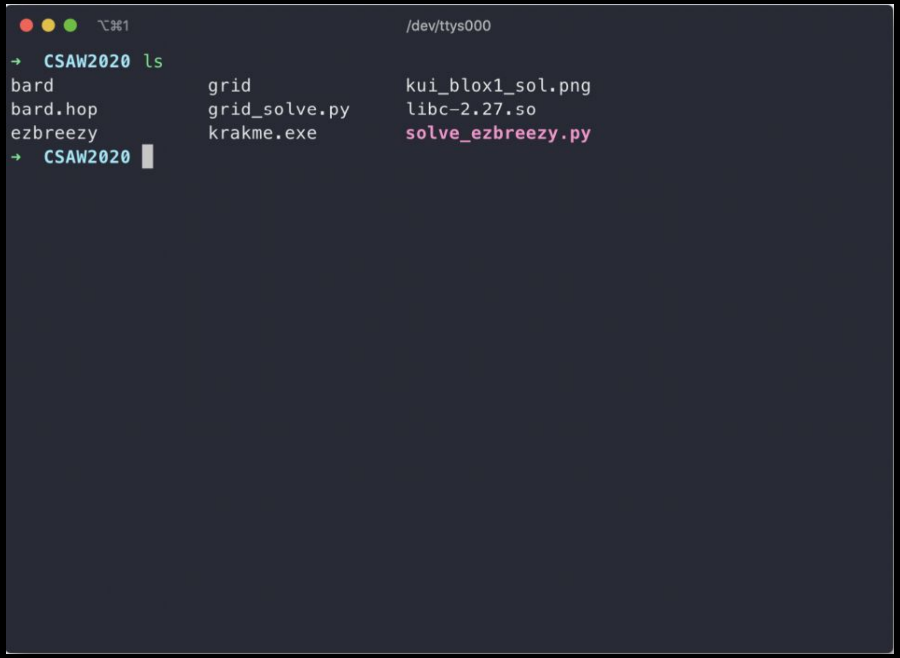
```
PowerShell 7.0.0
Copyright (c) Microsoft Corporation. All rights reserved.

https://aka.ms/powershell
Type 'help' to get help.


[10:47:45] C:\_Projects\
>
```

macOS Terminal

Command
+ Space → Search “Terminal” →



```
➜  CSAW2020 ls
bard                 grid                 kui_blox1_sol.png
bard.hop             grid_solve.py        libc-2.27.so
ezbreezy             krakme.exe           solve_ezbreezy.py
➜  CSAW2020 
```

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`

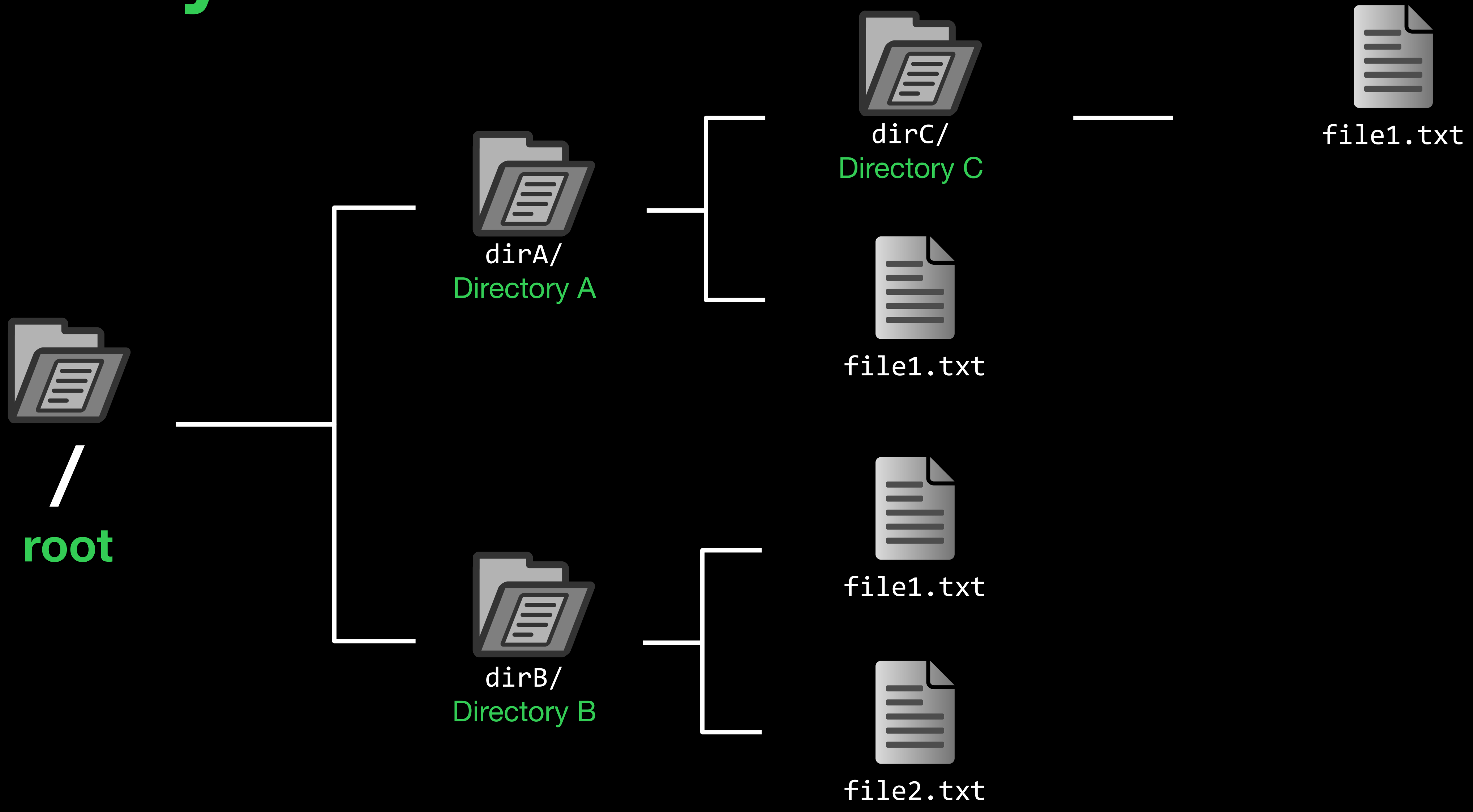
iTerm2 (Optional)

iTerm2

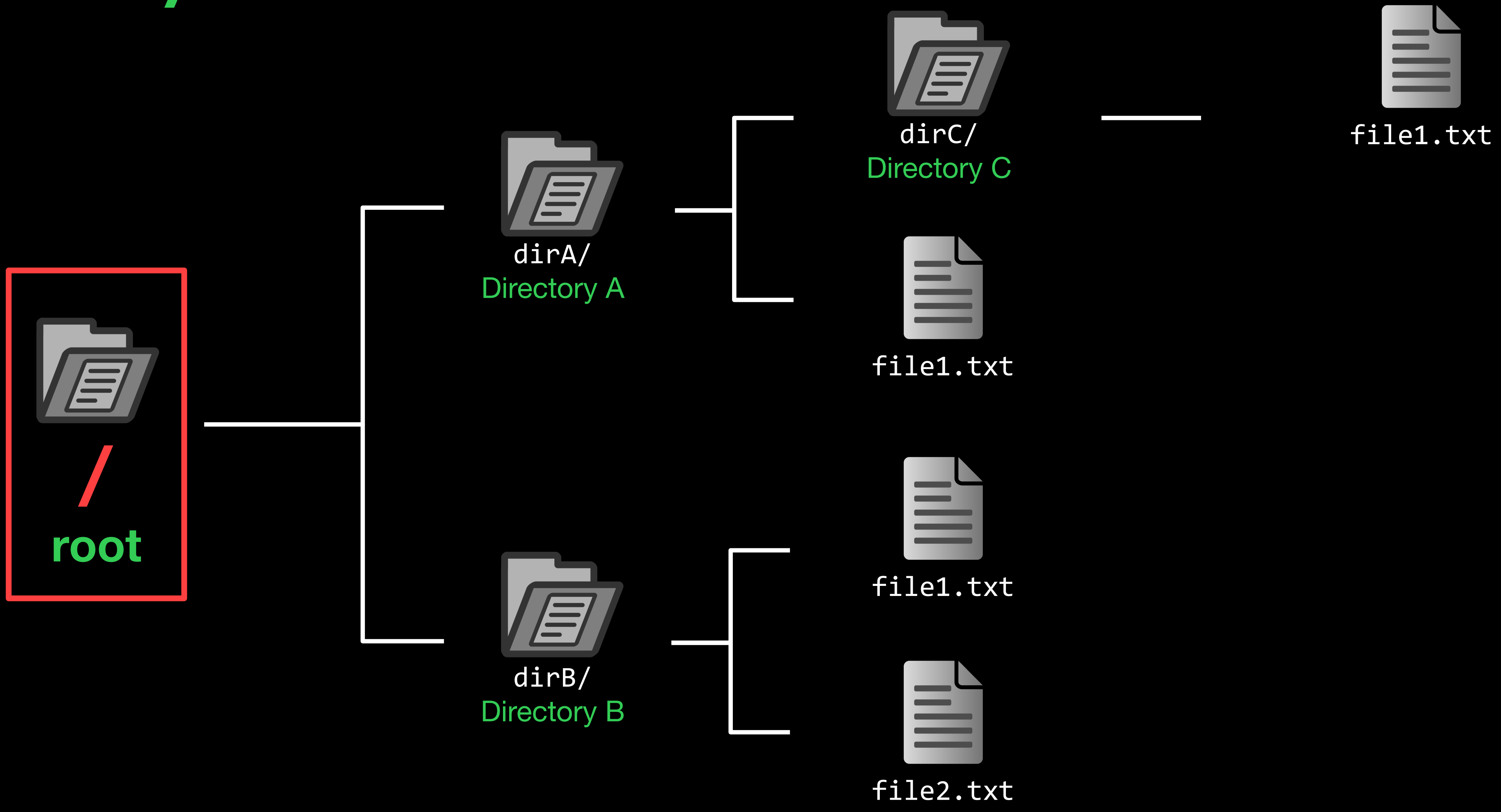
iTerm2 is a terminal emulator for macOS that does amazing things.

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

Filesystems

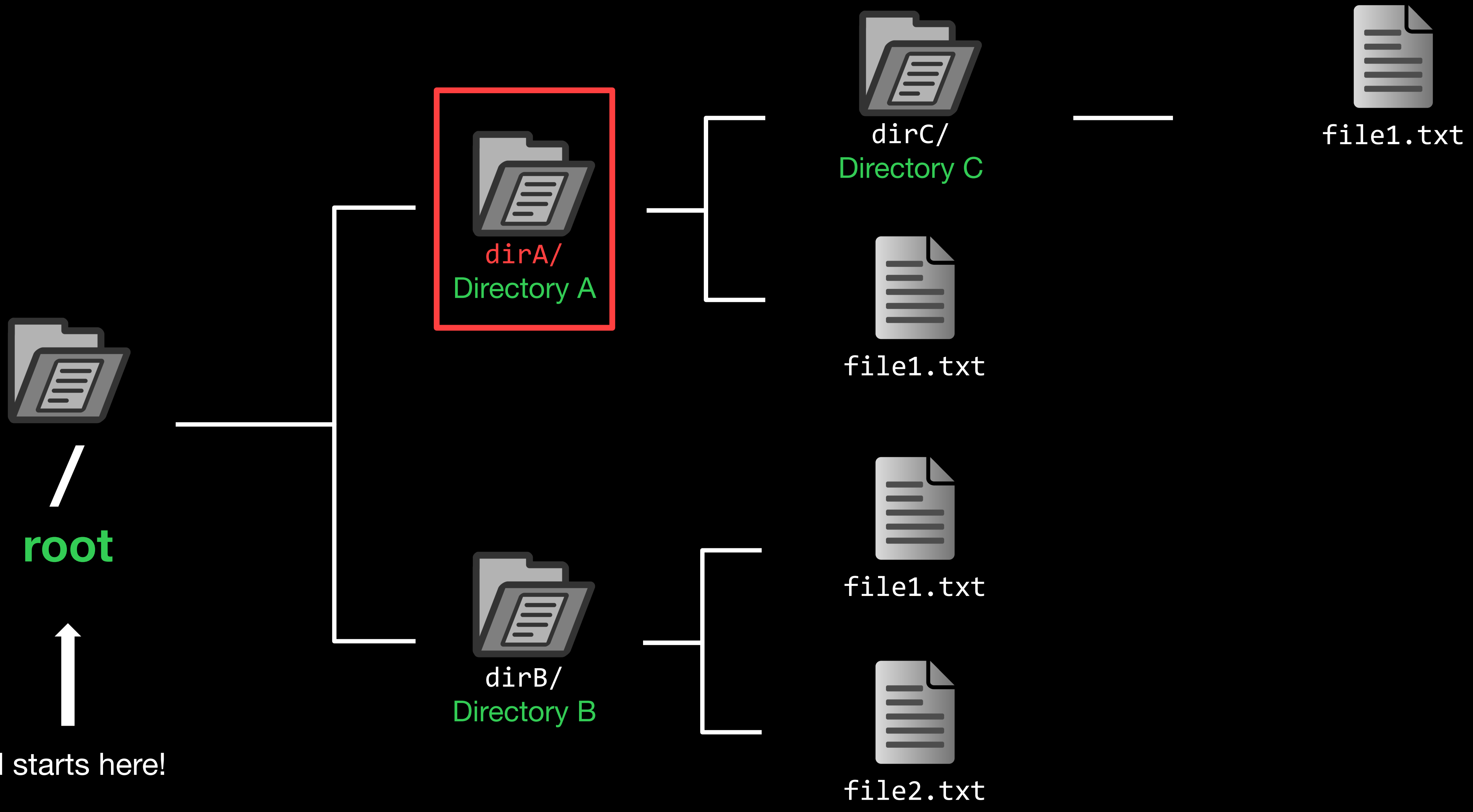


```
cd /
```



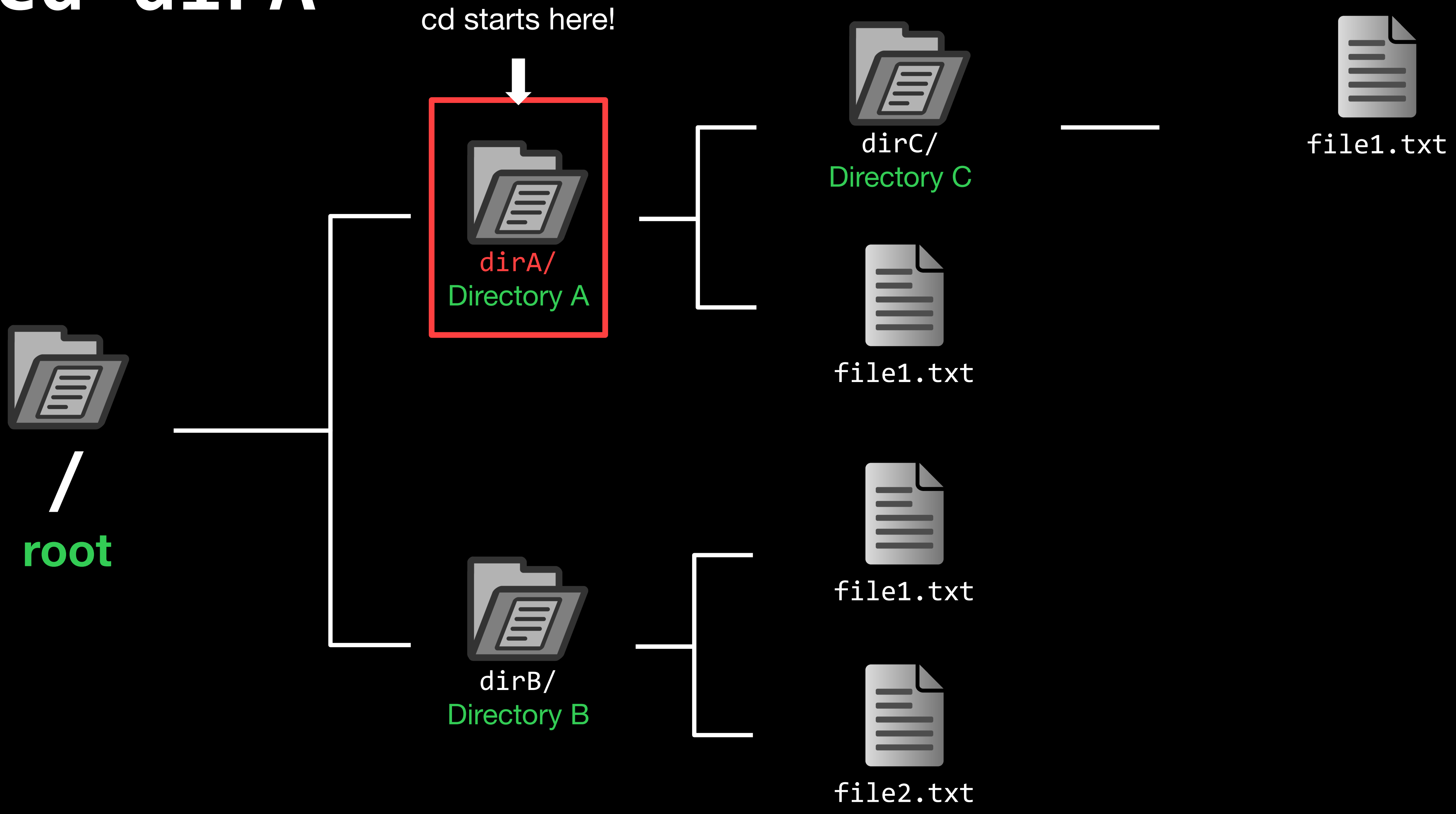
/
root
dirA/
Directory A
dirB/
Directory B
dirC/
Directory C
file1.txt
file1.txt
file1.txt
file2.txt

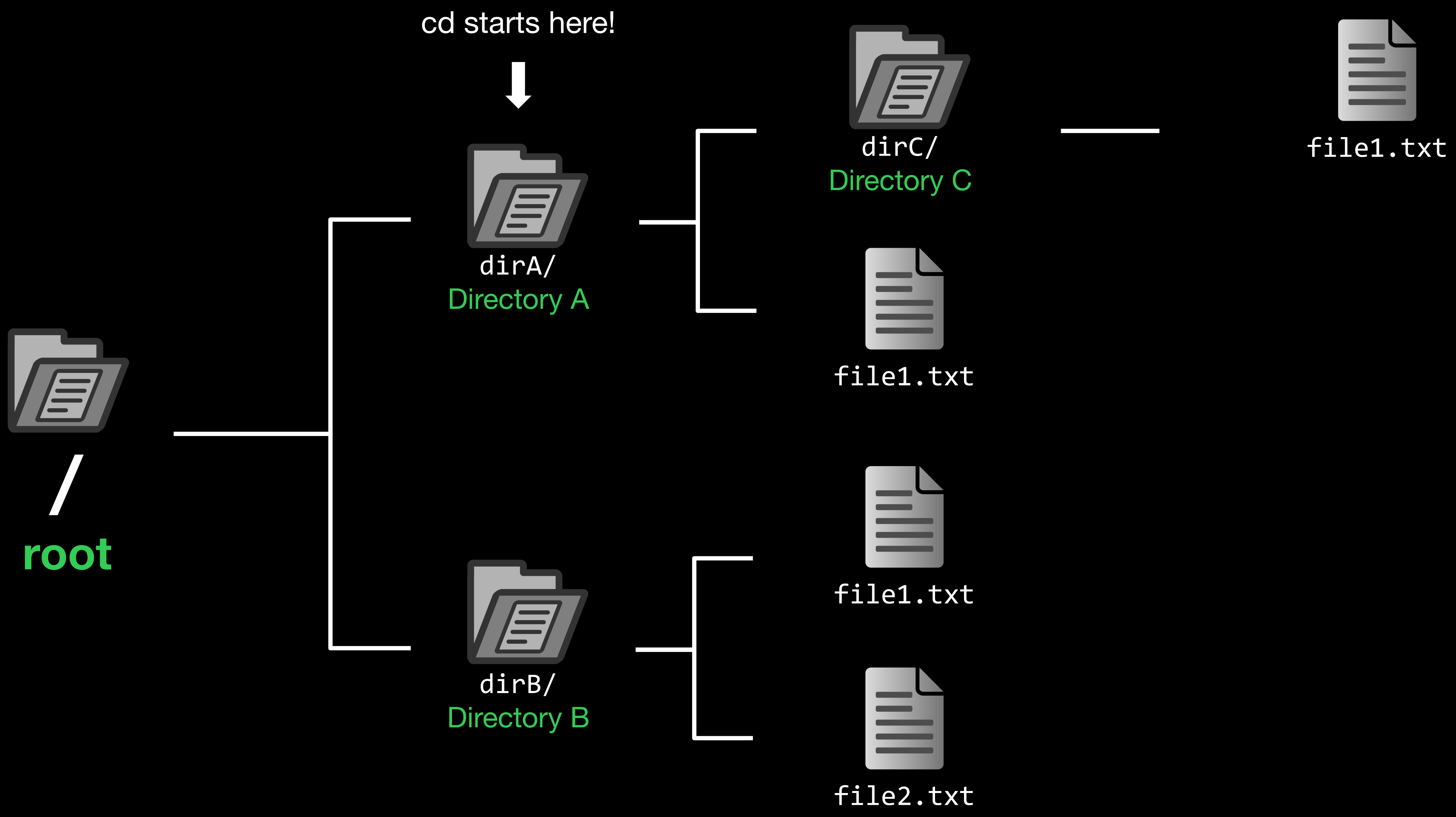
cd dirA



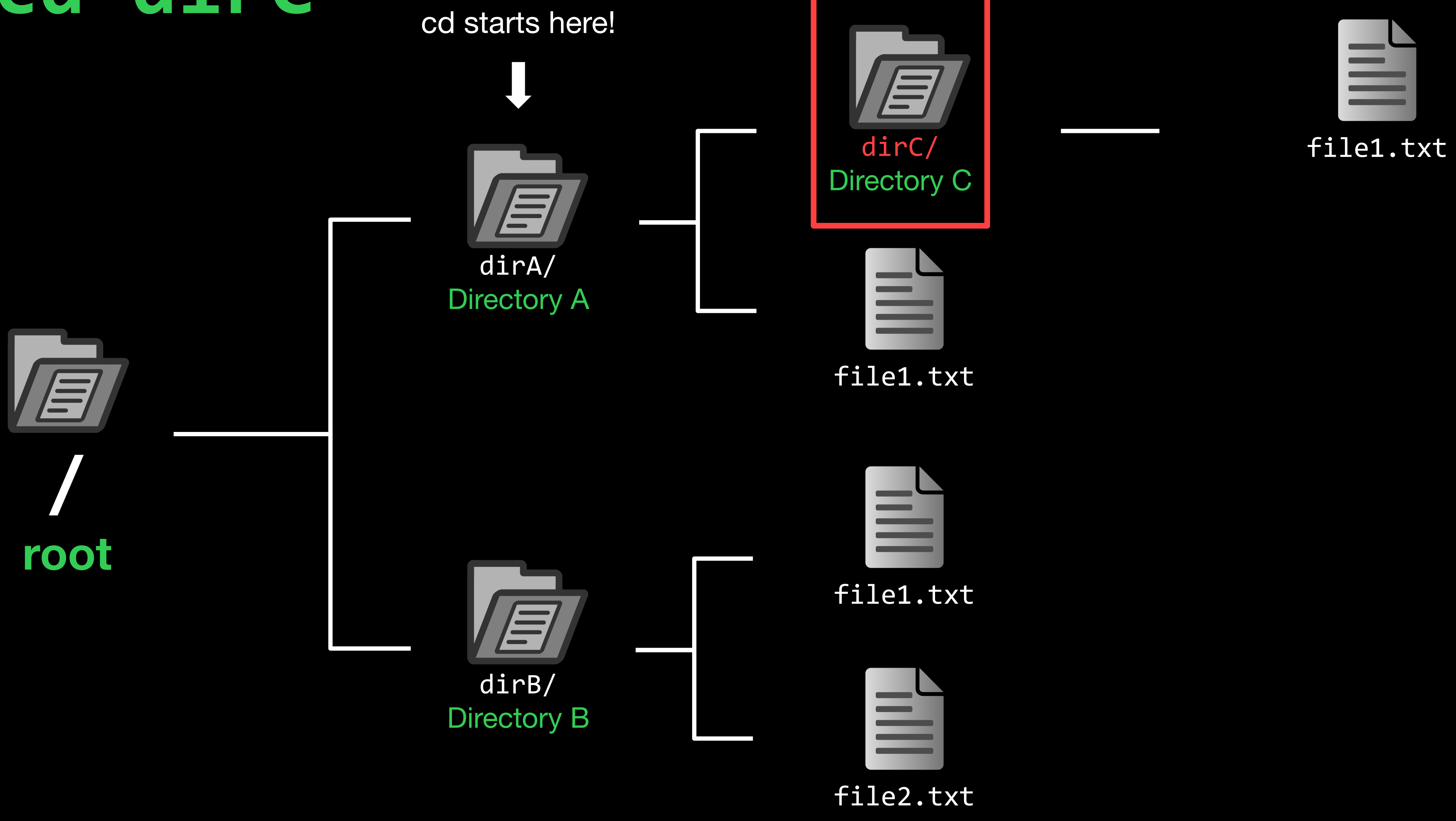
cd starts here!

cd dirA

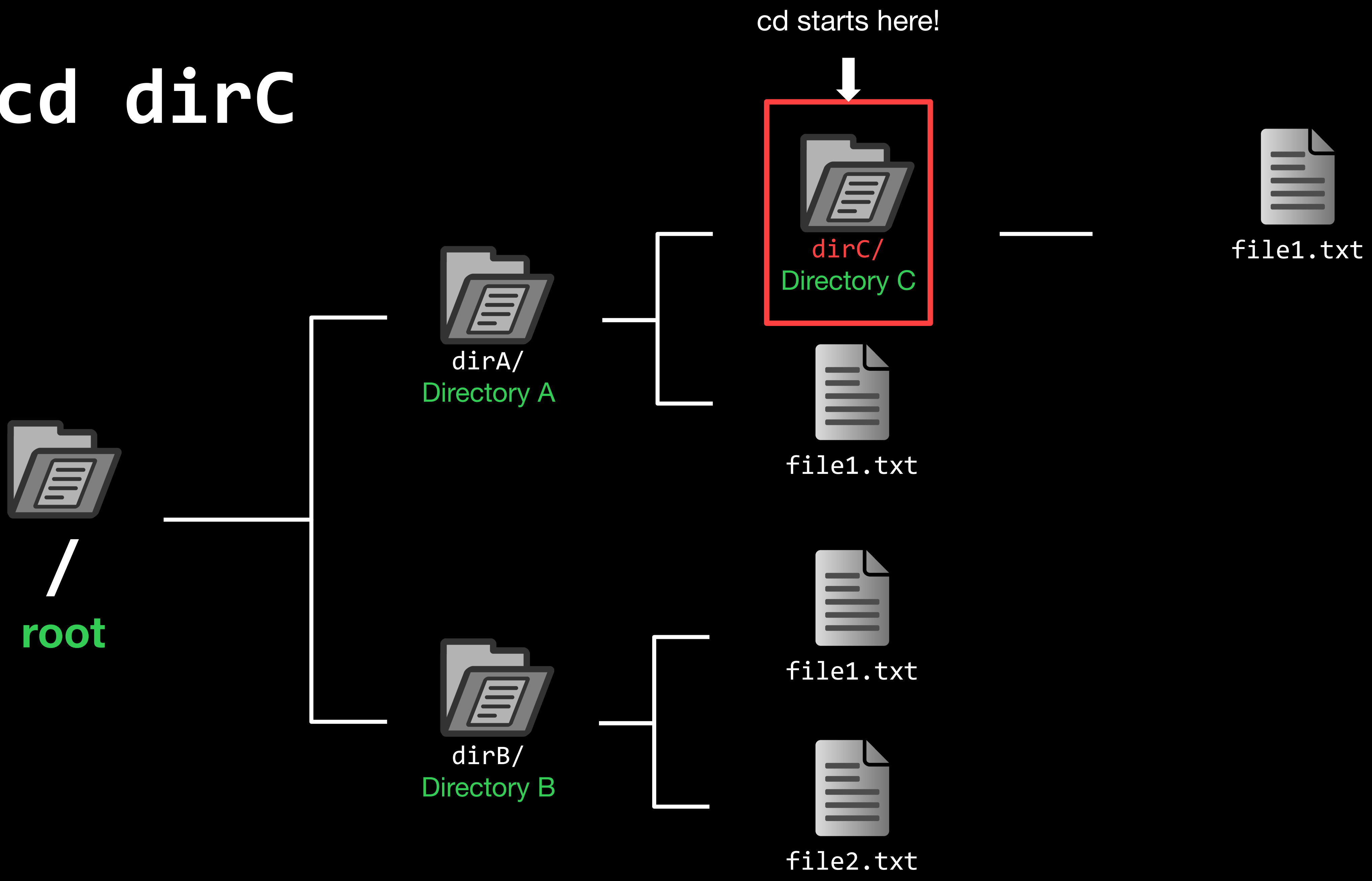

cd starts here!
dirA/
Directory A
/
root
dirB/
Directory B
dirC/
Directory C
file1.txt
file1.txt
file2.txt
file1.txt


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

cd dirC

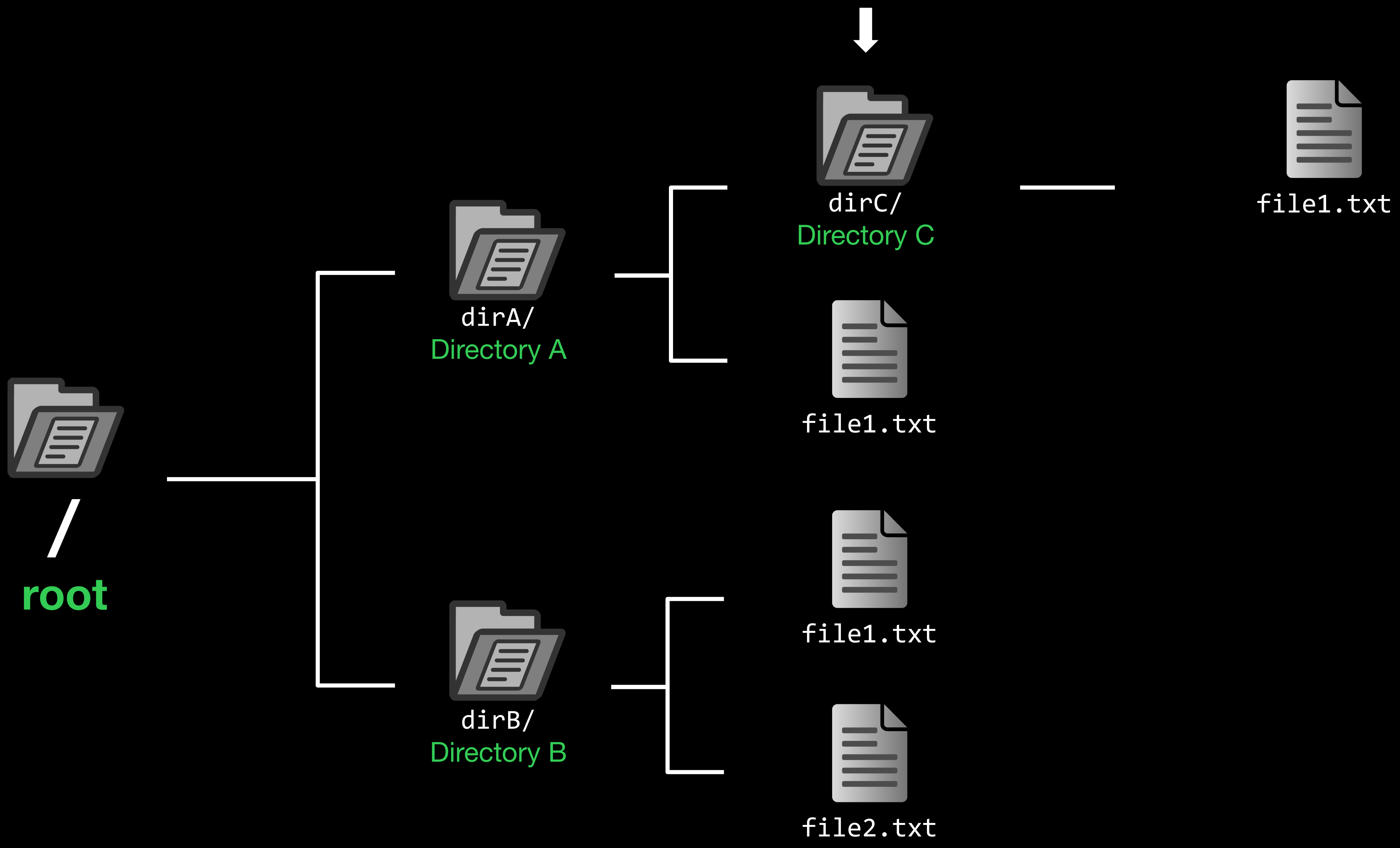

cd starts here!
dirA/
Directory A
dirC/
Directory C
file1.txt
file1.txt
/
root
dirB/
Directory B
file1.txt
file2.txt

cd dirC



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

cd starts here!



/
root

dirA/
Directory A

dirB/
Directory B

dirC/
Directory C

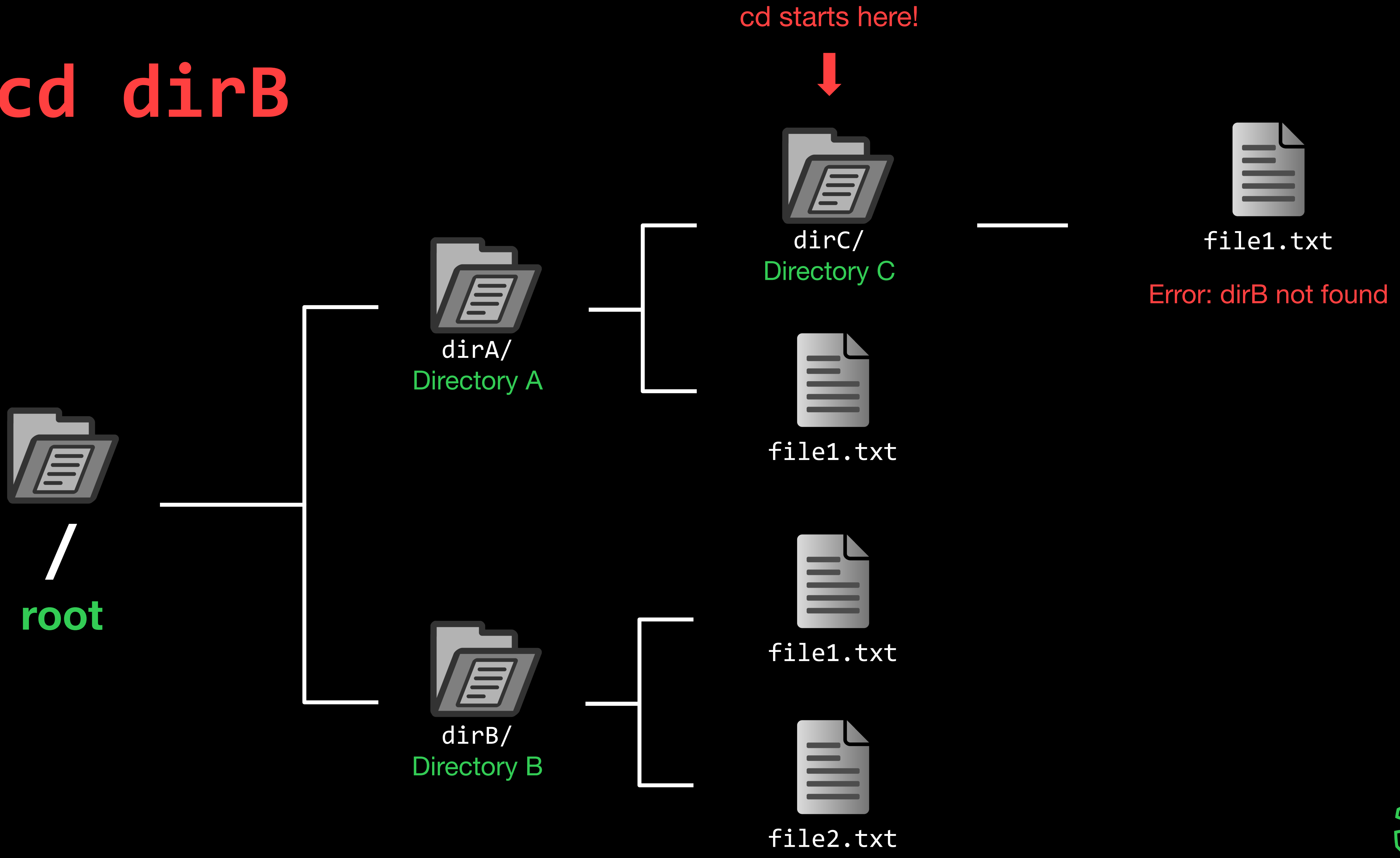
file1.txt

file1.txt

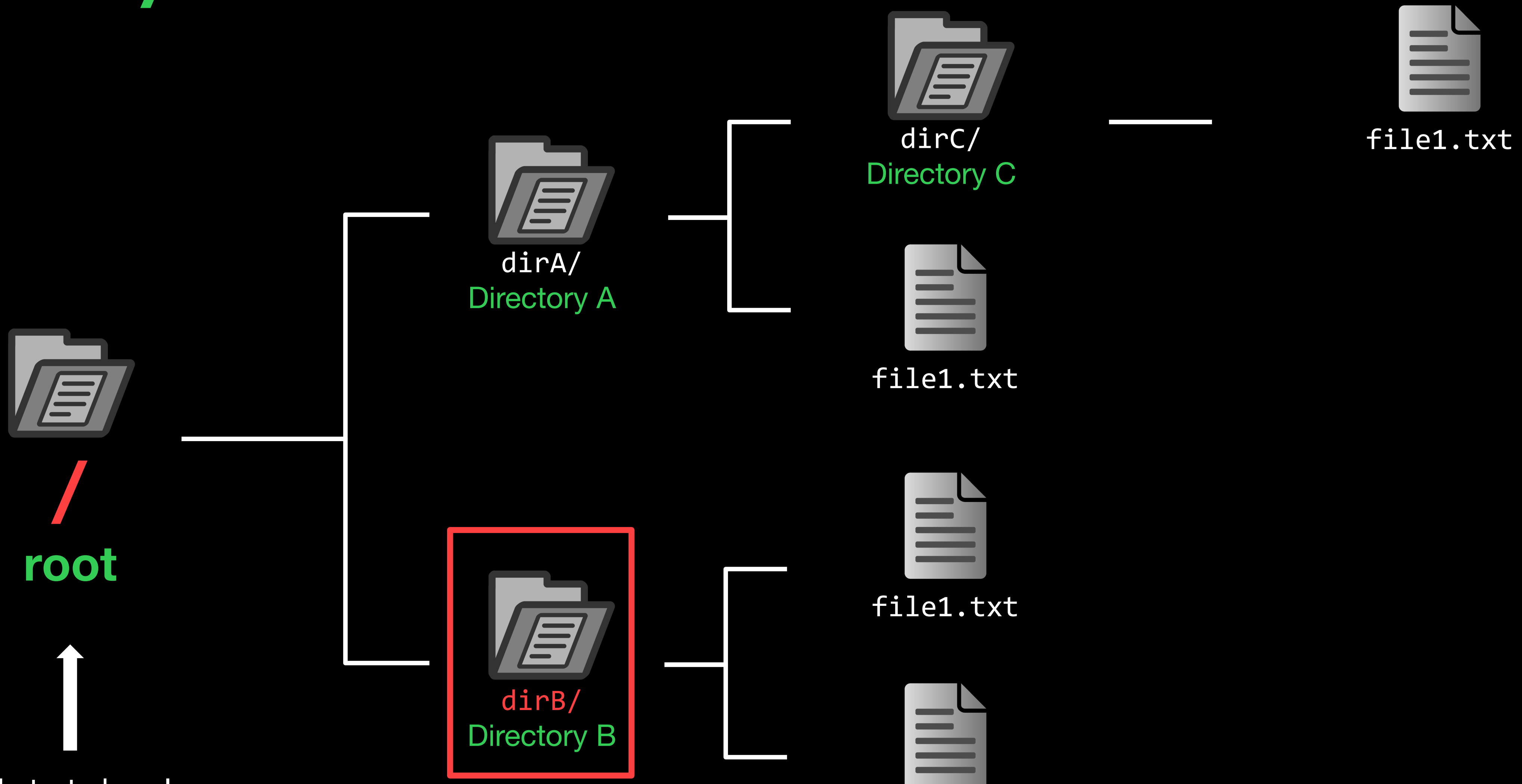
file1.txt

file2.txt

```
cd dirB
```

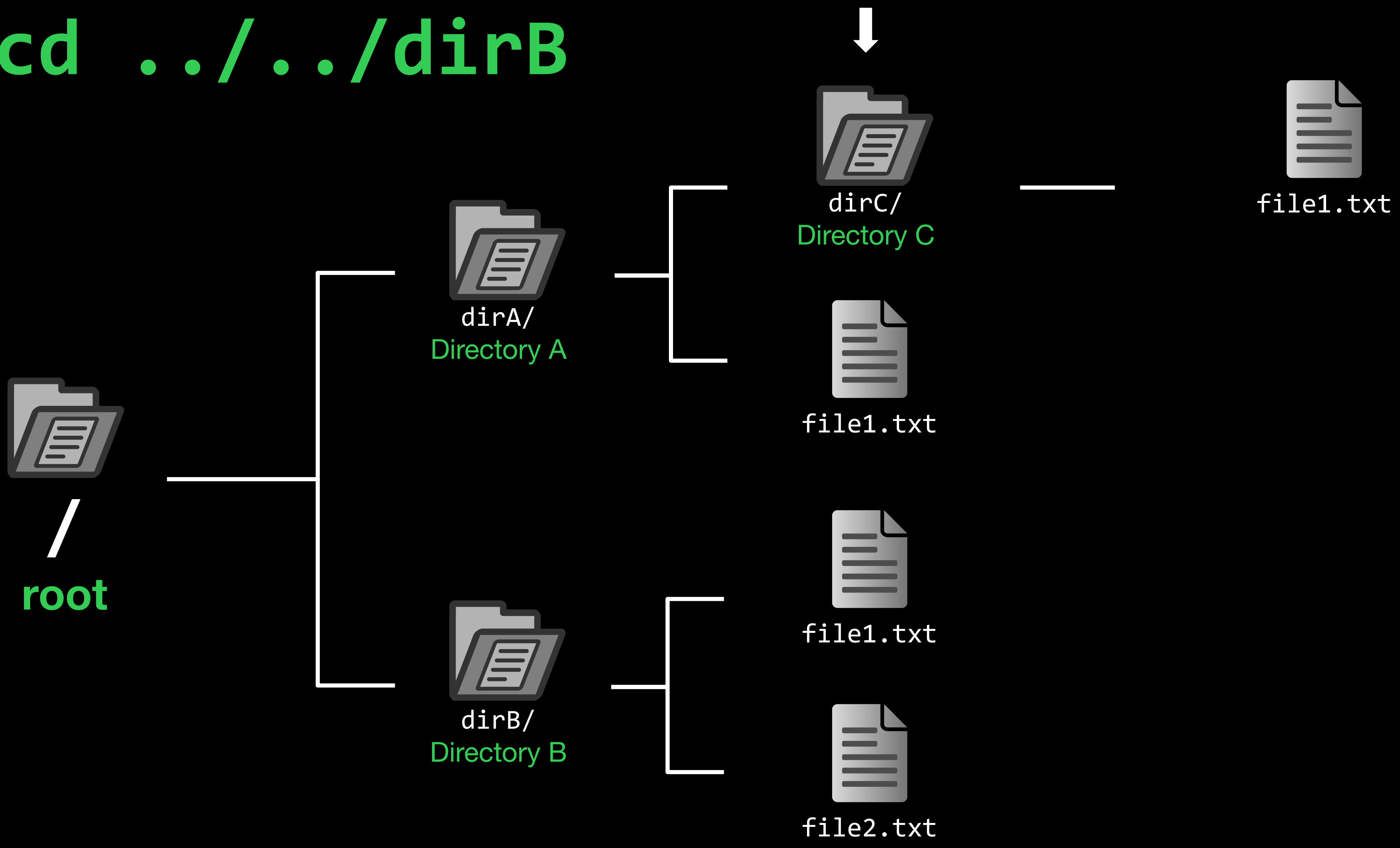

cd starts here!
dirC/
Directory C
file1.txt
Error: dirB not found
dirA/
Directory A
file1.txt
/
root
file1.txt
dirB/
Directory B
file2.txt

cd /dirB



cd starts here!

```
cd ../../dirB
```



cd starts here!

/
root

dirA/
Directory A

dirC/
Directory C

file1.txt

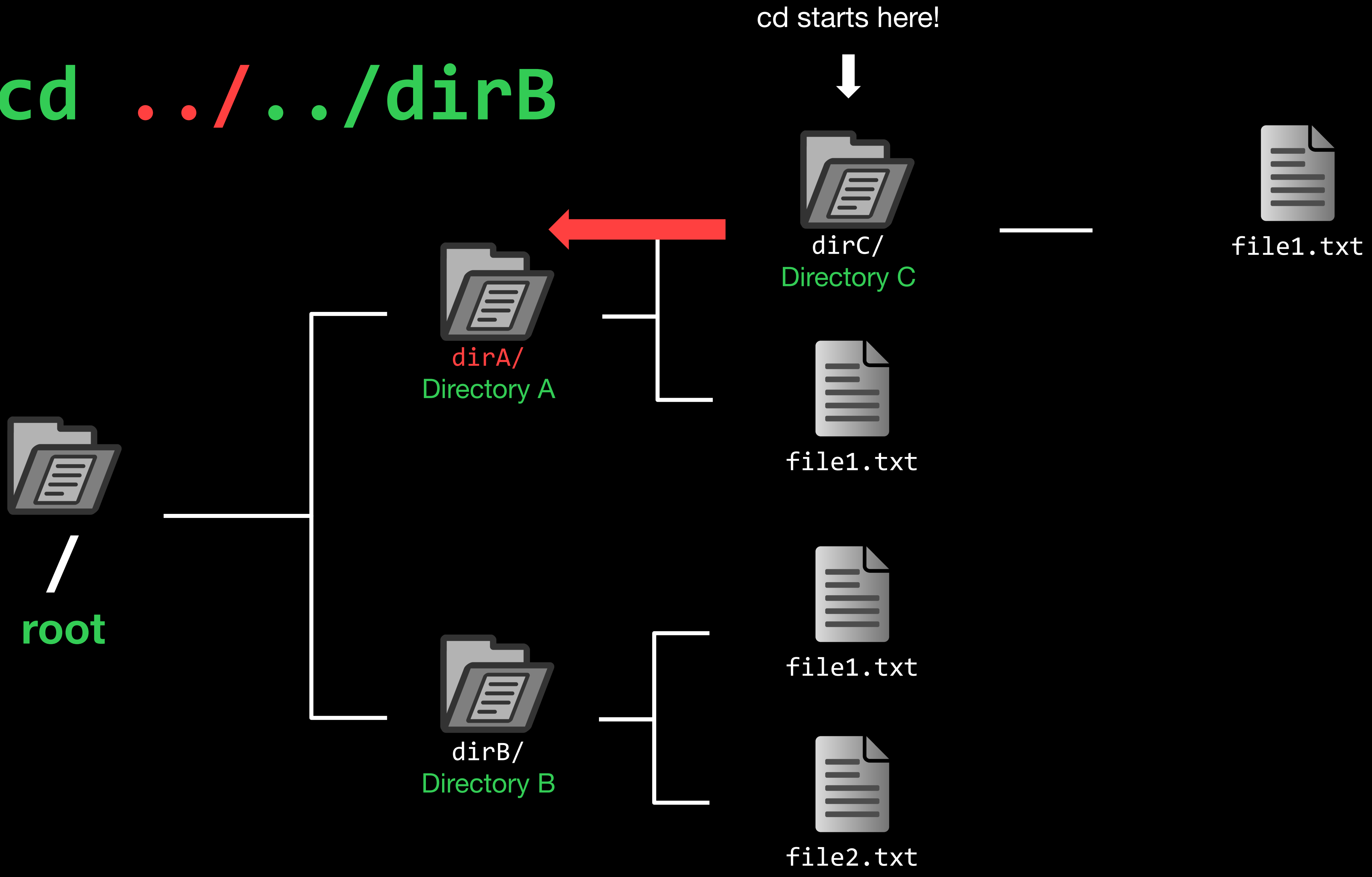
file1.txt

dirB/
Directory B

file1.txt

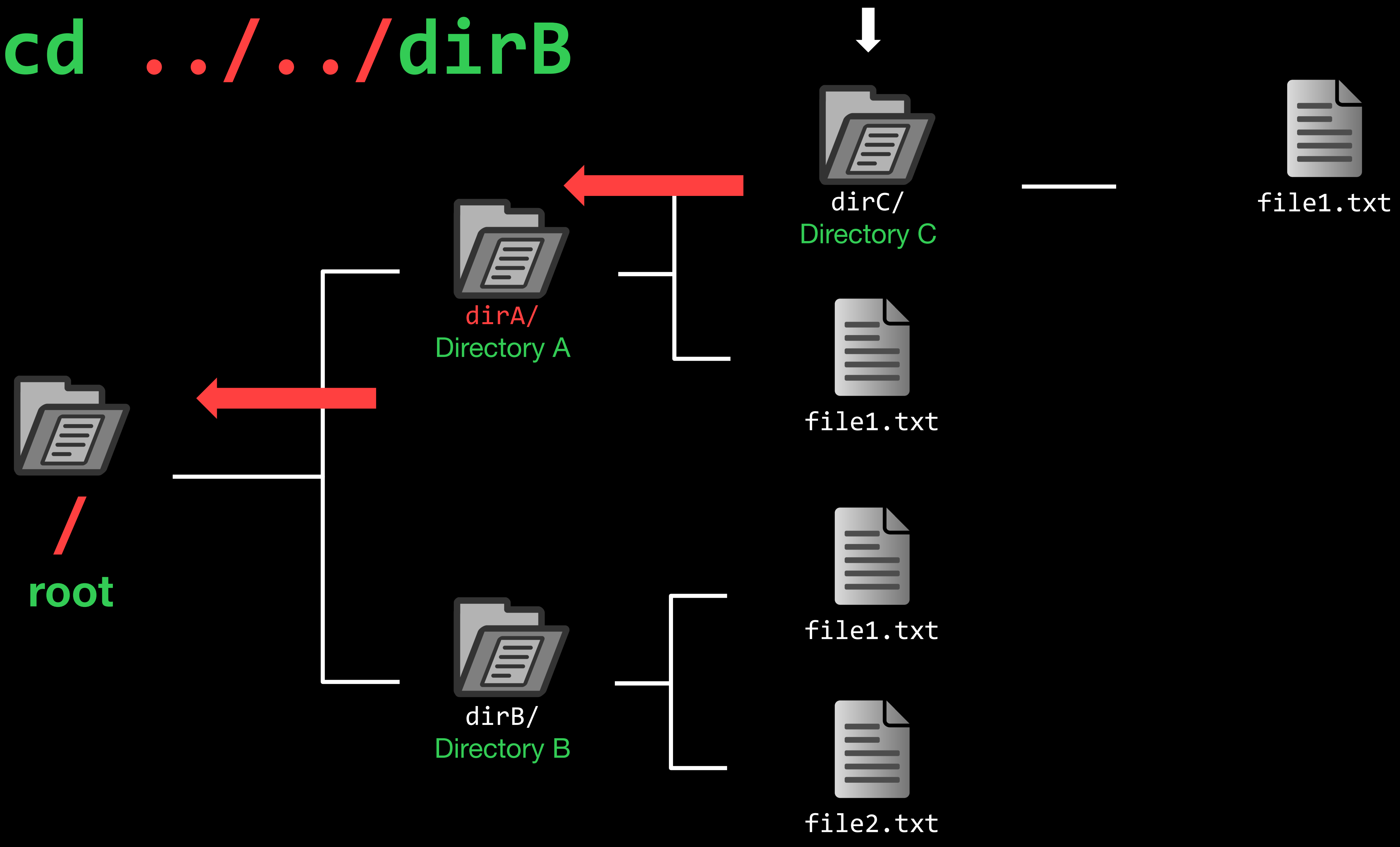
file2.txt

```
cd ../../dirB
```

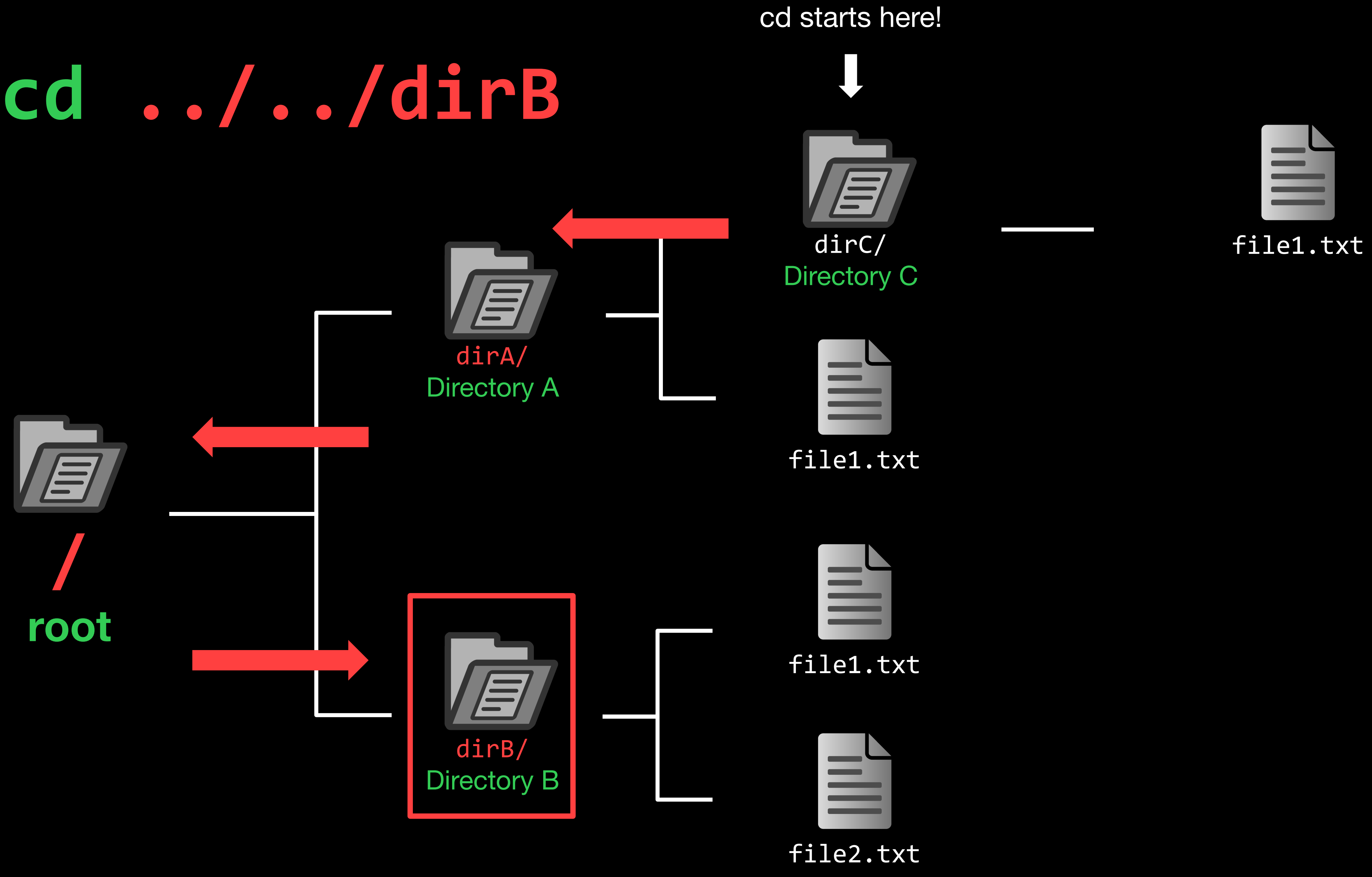

cd starts here!
dirC/
Directory C
file1.txt
dirA/
Directory A
file1.txt
/
root
file1.txt
dirB/
Directory B
file2.txt

```
cd ../../dirB
```

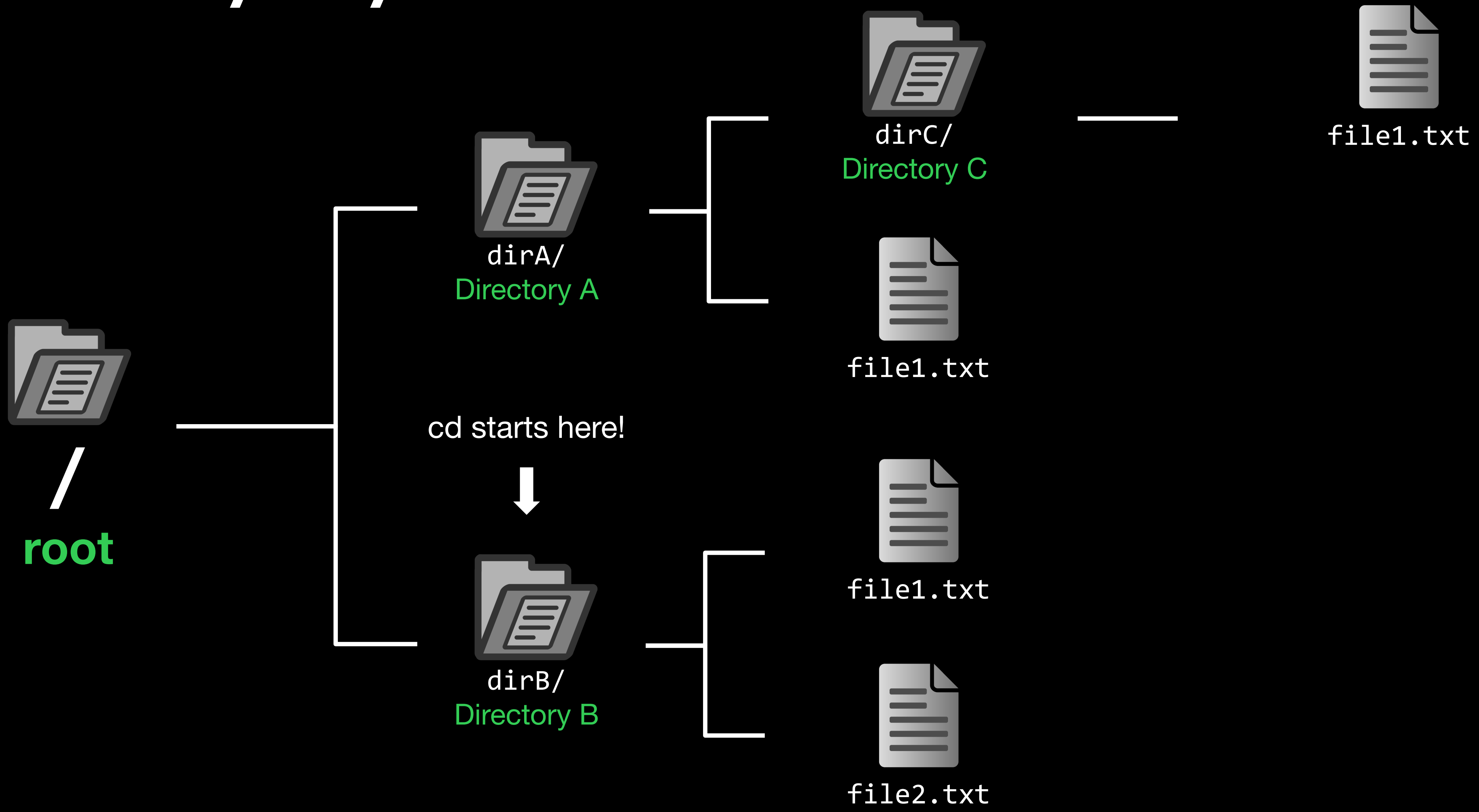
cd starts here!



```
cd ../../dirB
```

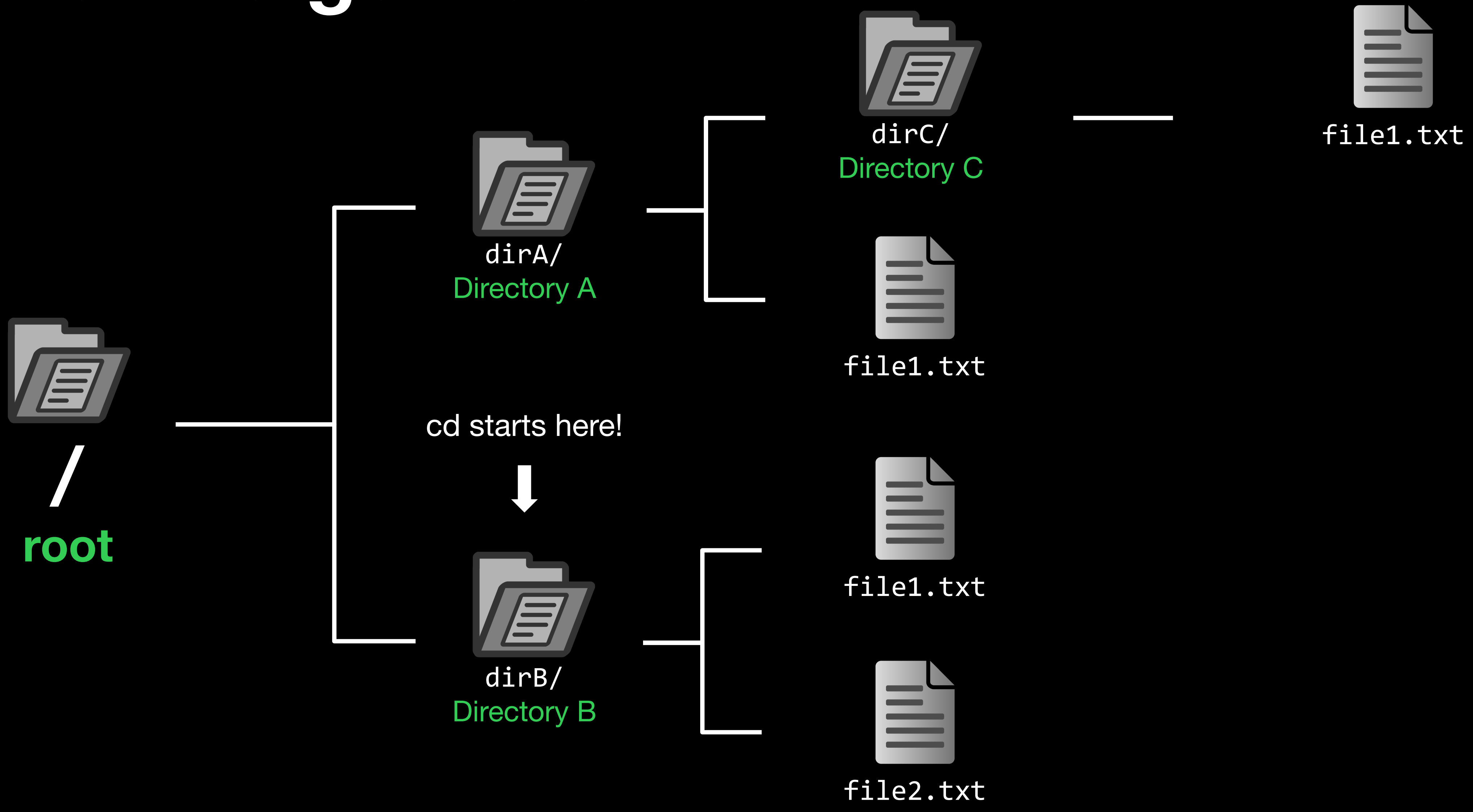

cd starts here!
dirC/
Directory C
file1.txt
dirA/
Directory A
file1.txt
/
root
file1.txt
dirB/
Directory B
file2.txt

cd ../../dirB

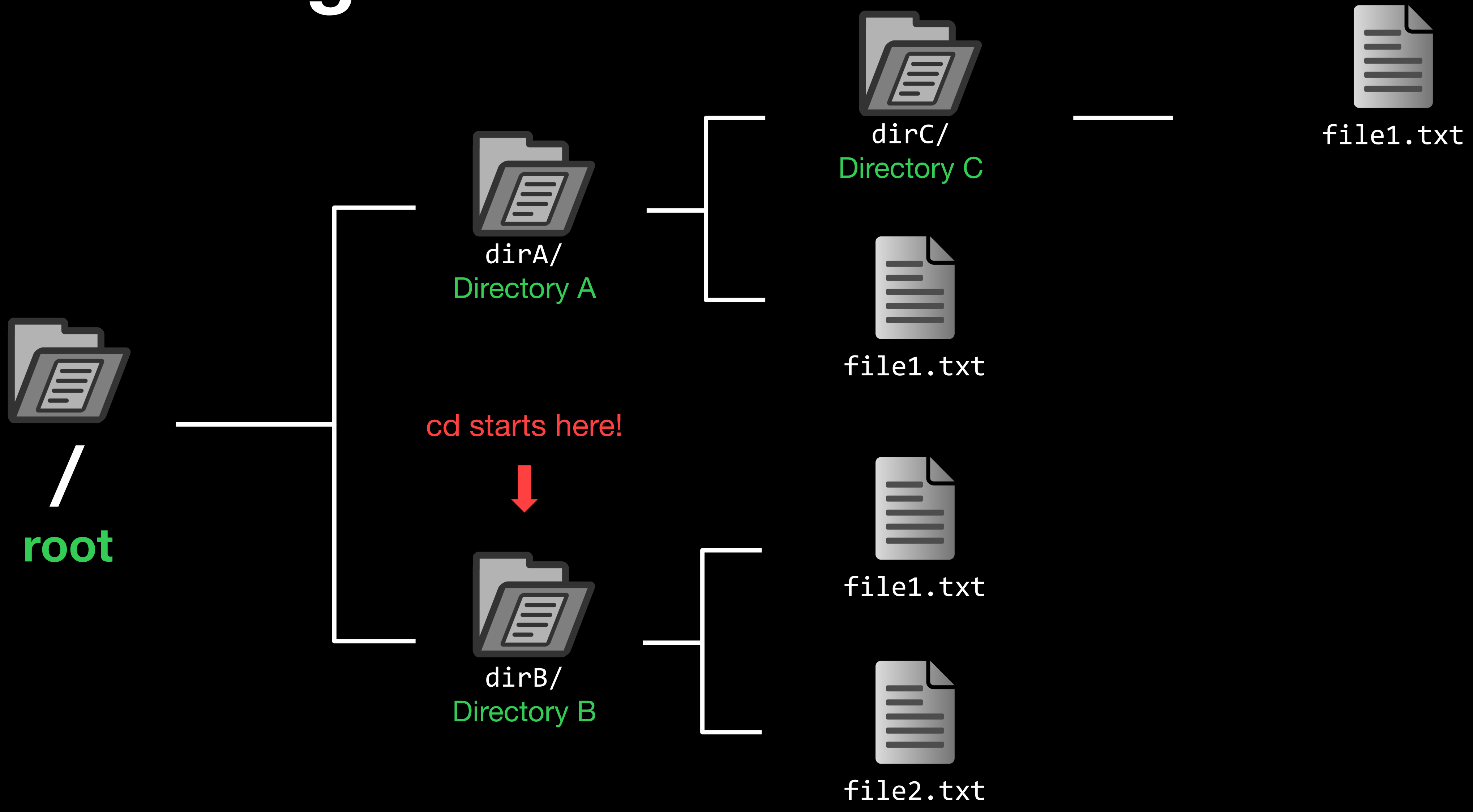


/
root
dirA/
Directory A
dirC/
Directory C
file1.txt
file1.txt
cd starts here!
dirB/
Directory B
file1.txt
file2.txt

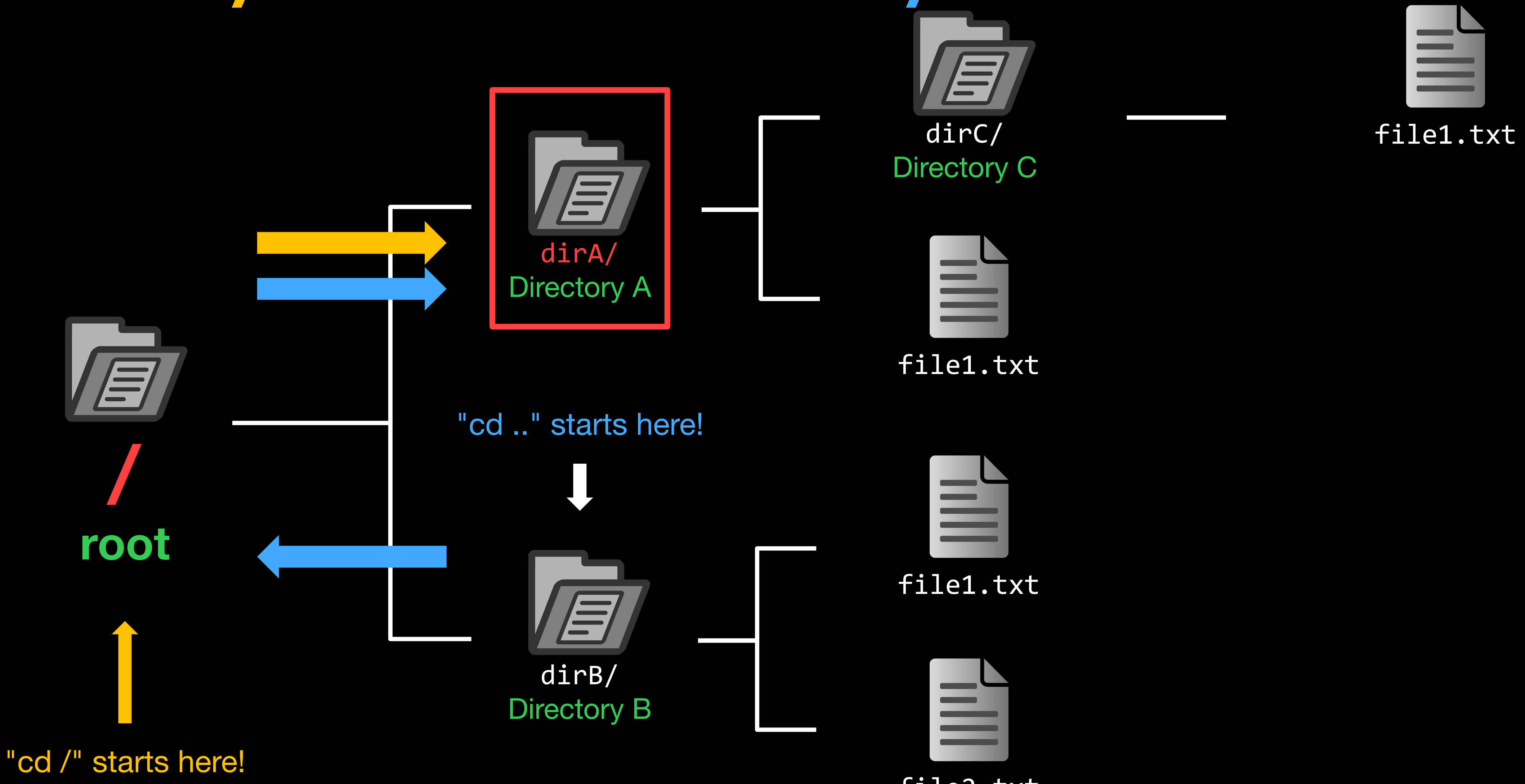
How to get to dirA?



How to get to dirA?



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



Paths

Relative Path

The full path that always starts at root (/)

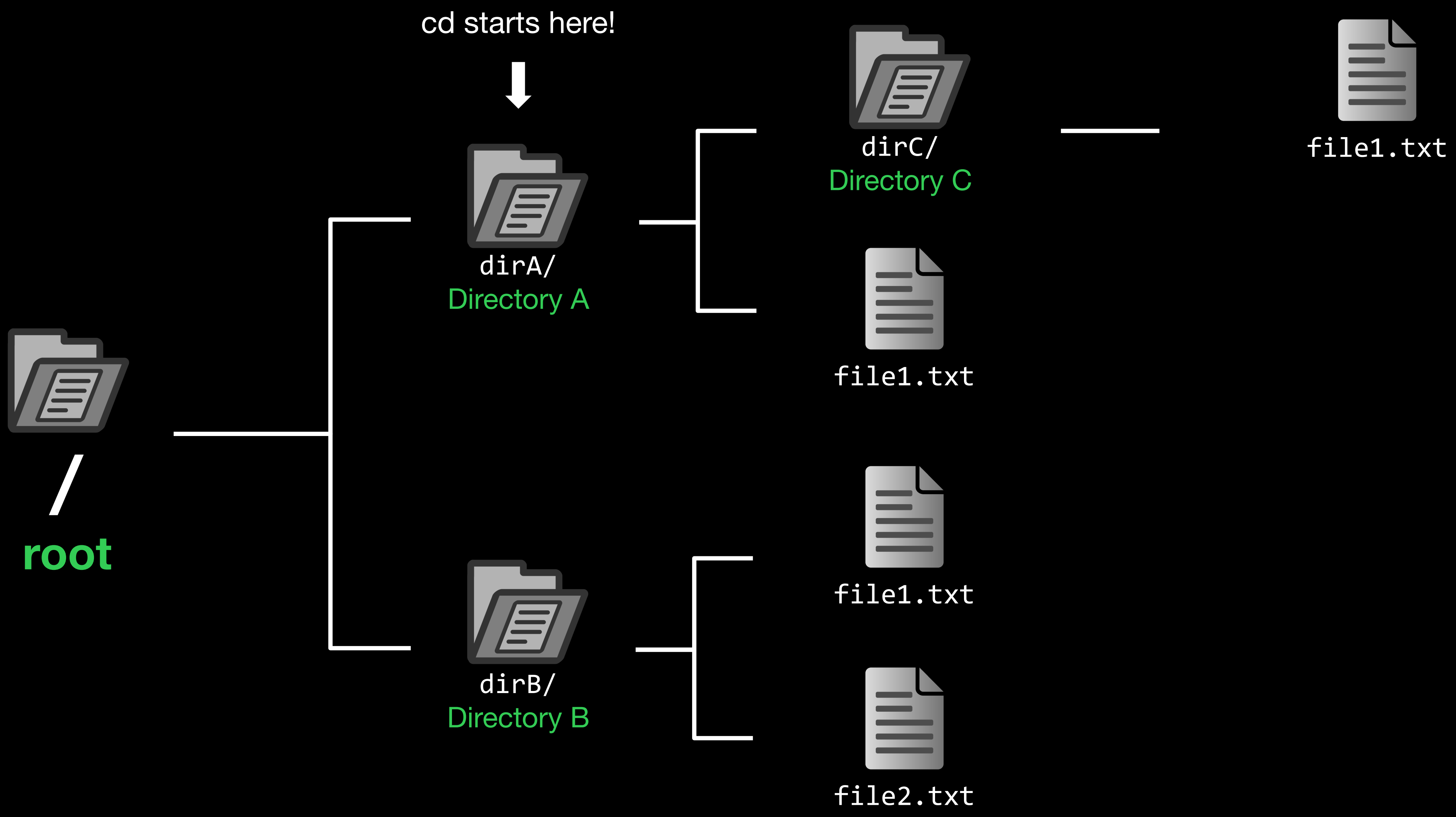
```
/dirA/file1.txt
/dirA/dirC/file1.txt
```

Absolute Path

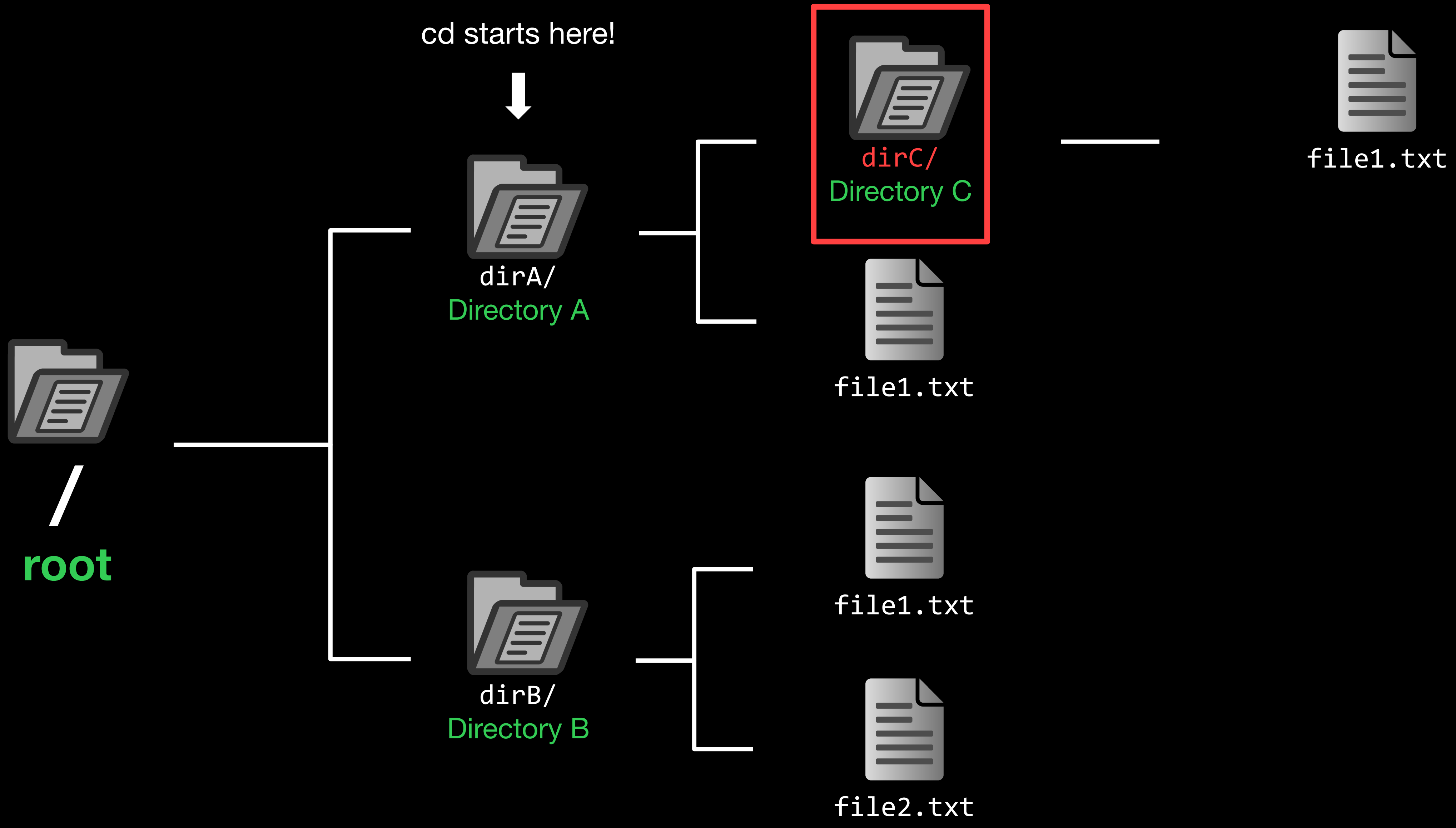
The partial path relative to where you are currently in the terminal

(Relative to dirA)

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


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

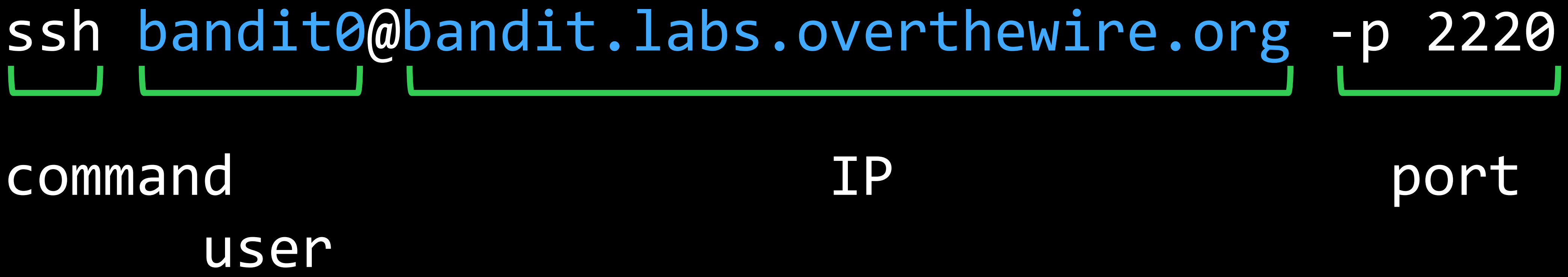
`nc <ip> <port>`: open a connection to the specified IP and port

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

2023-09-07 • **This Thursday**

- Web Hacking I with Pomona
- Learn introductory knowledge on web hacking

2023-09-10 • **Next Sunday**

- Terminal Session 2
- Same terminal setup content as today, tell your friends!

2023-09-08 • **Next Friday 4PM CST - Sunday 4PM CST**

- Playing **PatriotCTF** together
- Play our first CTF of the year with us! Free pizza, location TBD

ctf.sigpwny.com

`sigpwny{starting_off_strong}`

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

SIGPwny