SIGPwny @ UIUC

Fall 2017

Announcements

- UIUCTF Took 4th at CSAW Finals
  - Congratulations to Ankur, Ben, Matt, and Paul
- Trail of Bits Winter Internships
- Nadia Heninger Talk @ 10am Tomorrow
- SIG-ICPC Visit

Illinois Programming League

- Hone your algorithmic skills
- Ace your coding challenges
- Breeze through coding interviews

- It’s never too late to get on board!
- Students of all levels are welcomed to show up and solve problems

- ON: **Mondays 7-9pm**
- AT: **Siebel 0218**

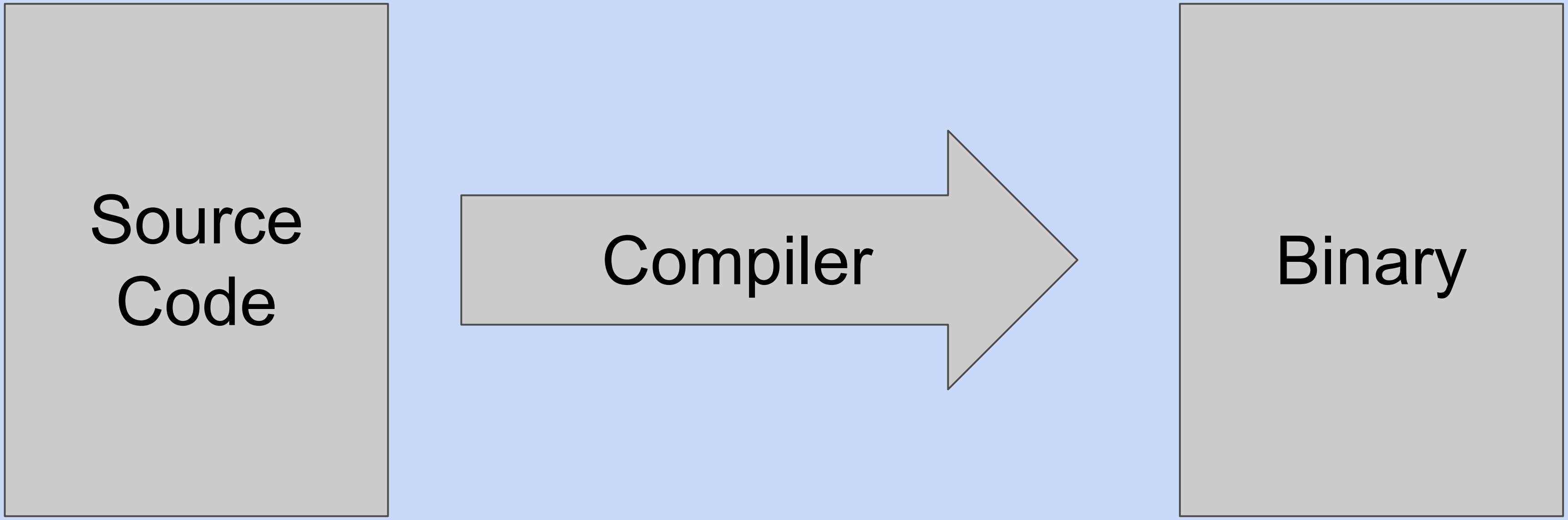
- Brought to you by the Illinois competitive programming team (ACM SIG-ICPC)

News of the Week

- Accepted CCS Papers
- FaceID Security Under Suspicion
- Shadow Brokers Impacts
- 757 Audit
- OnePlus Backdoor

Modern Binary Exploitation

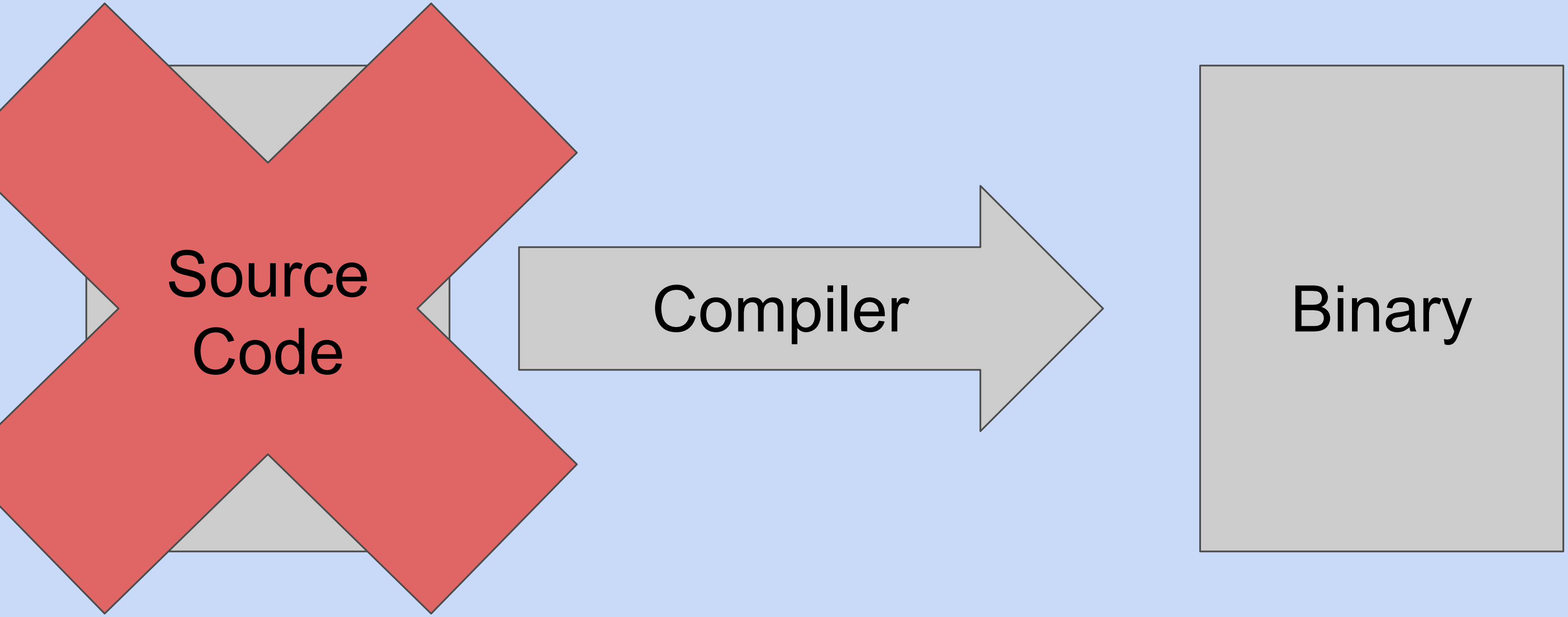
- Ran at RPI last two springs
- “how2pwn” the class
- everything’s on github.com/RPISEC/MBE
- I’m learning it for funsies



Source Code

Compiler

Binary



Source Code
Compiler
Binary

Analysis Types

Static

“stare at disassembly
until your eyes bleed”

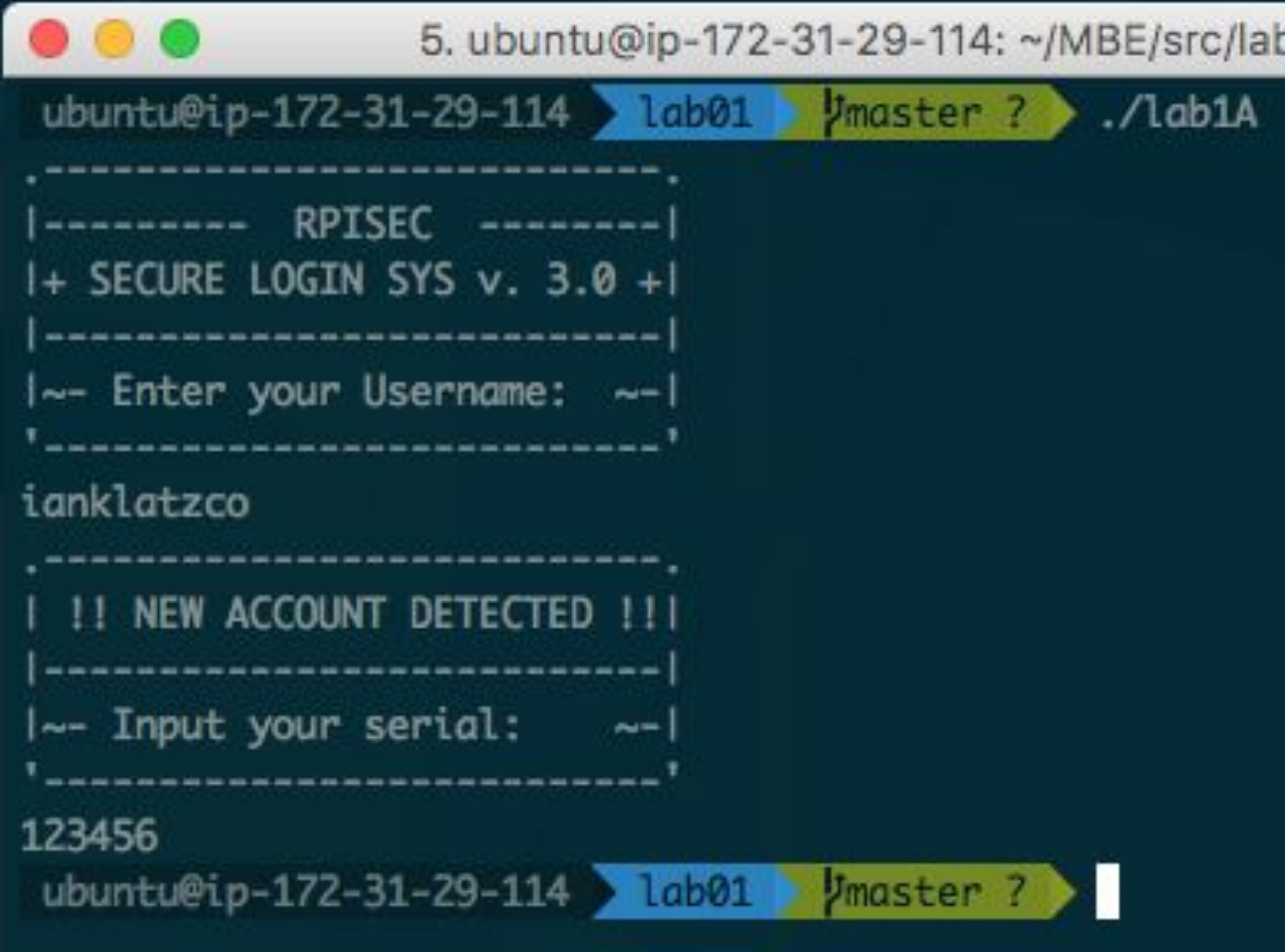
```
r2 lab1A
```

or
open it in binja

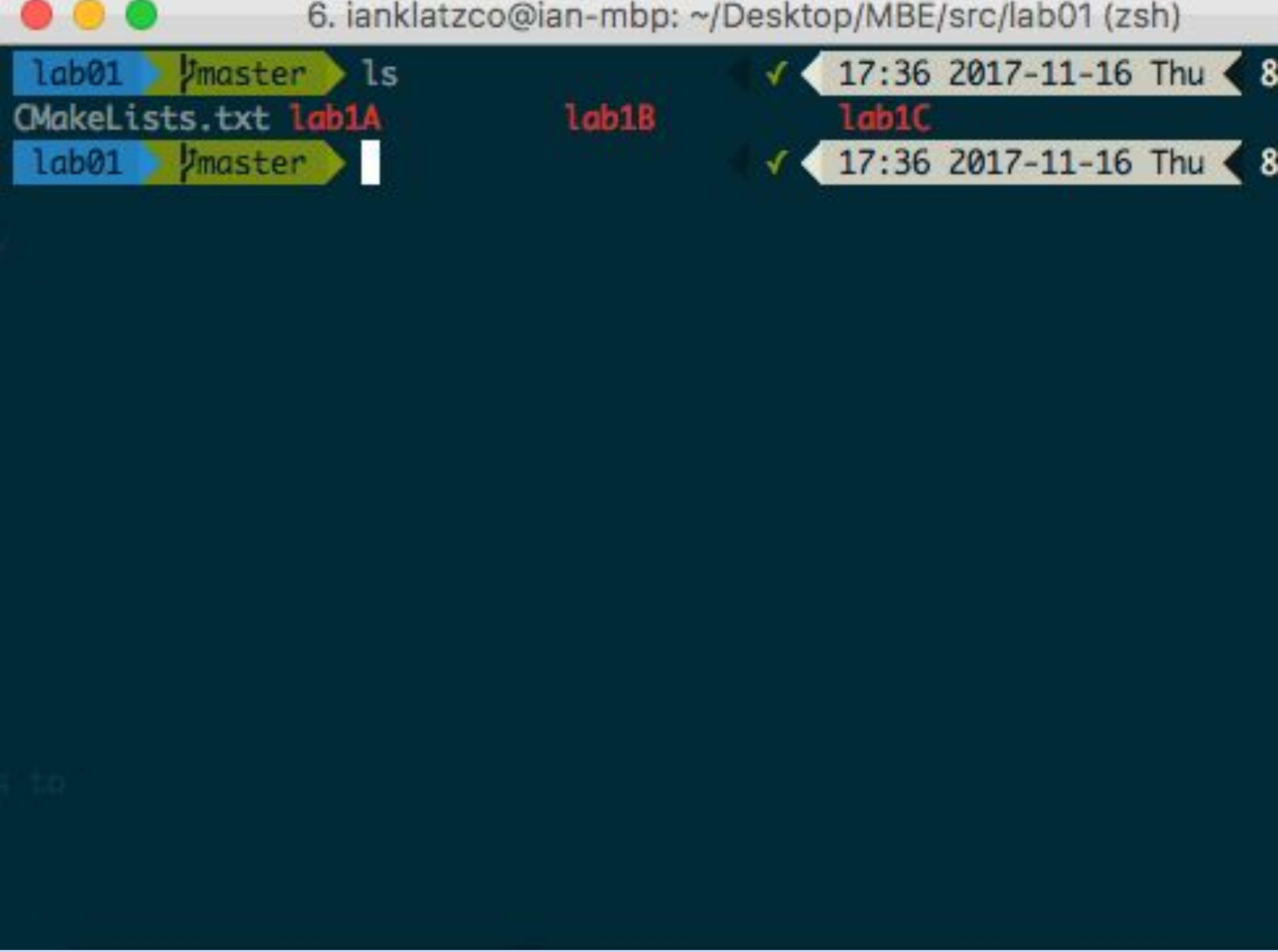
Dynamic

“run the program”

```
./lab1A
```



```
ubuntu@ip-172-31-29-114  lab01  master ?  ./lab1A
.---------------------------.
|---------  RPISEC  --------|
|+ SECURE LOGIN SYS v. 3.0 +|
|---------------------------|
|~- Enter your Username:  ~-|
'---------------------------'
ianklatzco
.---------------------------.
| !! NEW ACCOUNT DETECTED !!|
|---------------------------|
|~- Input your serial:    ~-|
'---------------------------'
123456
ubuntu@ip-172-31-29-114  lab01  master ?
```



6. ianklatzco@ian-mbp: ~/Desktop/MBE/src/lab01 (zsh)

```
lab01  master  ls                            ✓  17:36 2017-11-16 Thu  8
CMakeLists.txt lab1A          lab1B          lab1C
lab01  master                                ✓  17:36 2017-11-16 Thu  8
```

your turn!

- what does it do?
- figure it out!
- get shell

klatz.co/sigpwny/mbe-day1.tar.gz
klatz.co/sigpwny/mbe-day1.zip