



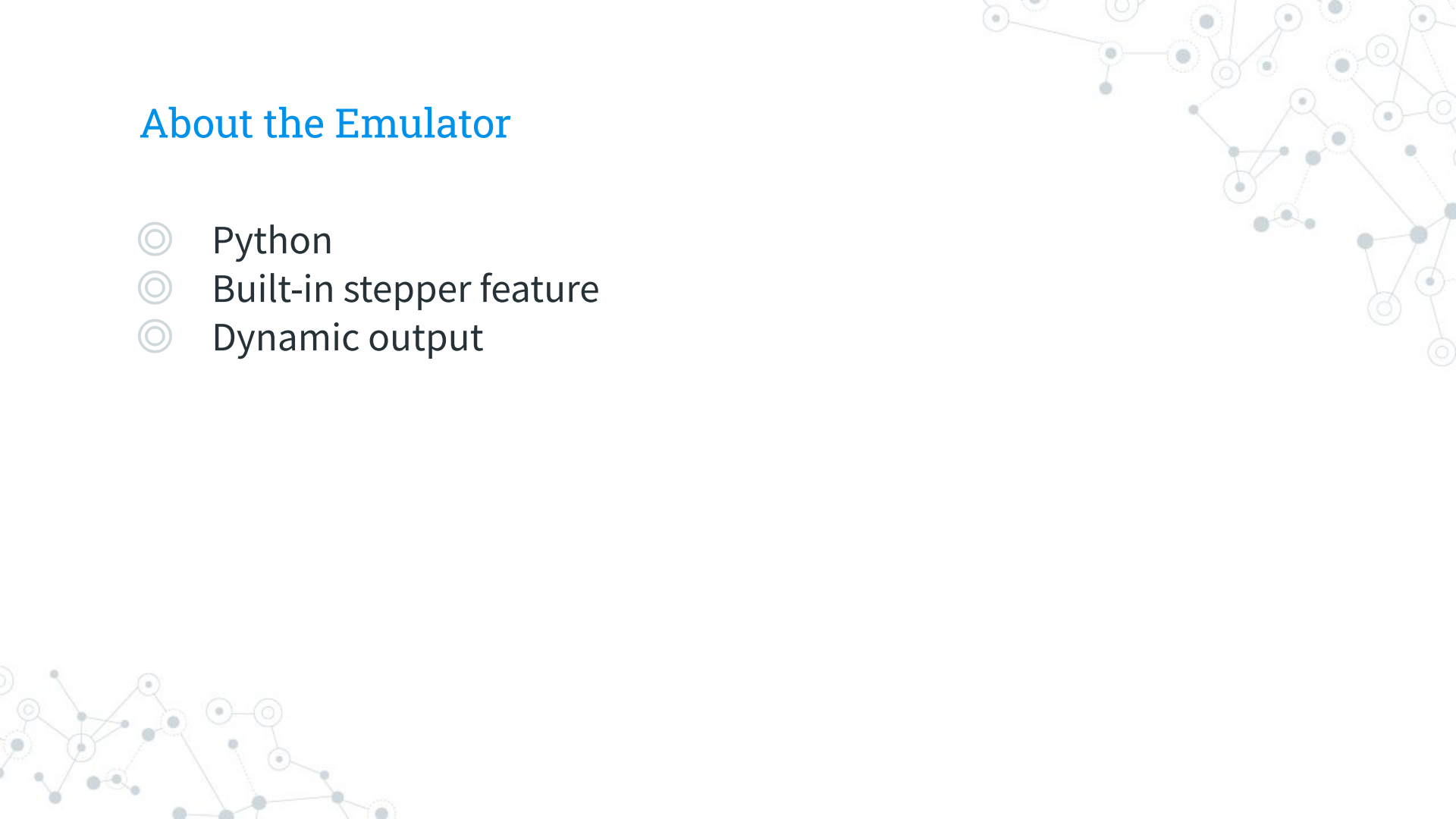
# ARM64 Emulator

William Turner and Omkar Ashish Pednekar



## About the Emulator

- ◎ Python
- ◎ Built-in stepper feature
- ◎ Dynamic output



## Instruction #1

Mnemonic: SUB  
Operand #1: SP  
Operand #2: SP  
Operand #3: #0X10

## Registers

X0: 0x0000000000000000 X11: 0x0000000000000000 X22: 0x0000000000000000  
X1: 0x0000000000000000 X12: 0x0000000000000000 X23: 0x0000000000000000  
X2: 0x0000000000000000 X13: 0x0000000000000000 X24: 0x0000000000000000  
X3: 0x0000000000000000 X14: 0x0000000000000000 X25: 0x0000000000000000  
X4: 0x0000000000000000 X15: 0x0000000000000000 X26: 0x0000000000000000  
X5: 0x0000000000000000 X16: 0x0000000000000000 X27: 0x0000000000000000  
X6: 0x0000000000000000 X17: 0x0000000000000000 X28: 0x0000000000000000  
X7: 0x0000000000000000 X18: 0x0000000000000000 X29: 0x0000000000000000  
X8: 0x0000000000000000 X19: 0x0000000000000000 X30: 0x0000000000000000  
X9: 0x0000000000000000 X20: 0x0000000000000000 SP: 0x00000000000000ff  
X10: 0x0000000000000000 X21: 0x0000000000000000 PC: 0x0000000000000000  
N bit: 0  
Z bit: 0

## Stack

00000000: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
00000010: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
00000020: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
00000030: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
00000040: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
00000050: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
00000060: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
00000070: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
00000080: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
00000090: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
000000A0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
000000B0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
000000C0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
000000D0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
000000E0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
000000F0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....

Press ENTER to continue:

## What We Learned

- ◎ Basics of ARM64 assembly
- ◎ Differences between ARM32 and ARM64
- ◎ Python debugging

## Features to Add

- ⊙ Disassembler
- ⊙ Interactive code editor
- ⊙ GUI
- ⊙ Optional printing switches

Navigation capability

## Resources

- ◎ <https://courses.cs.washington.edu/courses/cse469/18wi/Materials/arm64.pdf>
- ◎ <https://developer.arm.com/documentation/ddi0596/2021-12/Base-Instructions>
- ◎ [https://www.youtube.com/playlist?list=PLn\\_Ilt163He32Ujm-l\\_czgEBhbJjOUgFhg](https://www.youtube.com/playlist?list=PLn_Ilt163He32Ujm-l_czgEBhbJjOUgFhg)