

# Reverse Engineering Workshop



terrynini38514



terrynini





提供

台灣駭客協會

Hacks In Taiwan





# 快速複習一下

<https://speakerdeck.com/terrynini/ni-ni-ren-shu-f5-xiao-shi-zhi-shu>

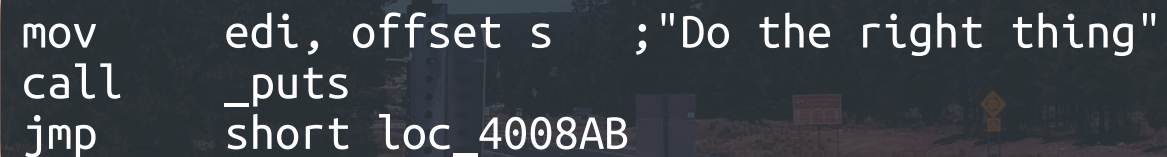




# CFG

## Control-flow Graph

CFG is a graph with (conceptually) basic blocks as nodes and jumps/calls/rets/etc as edges. - angr



A diagram illustrating a basic block in a control-flow graph. It consists of a rounded rectangular box with an orange border containing assembly code. A blue arrow points down to the box from above, and another blue arrow points down from the bottom of the box, representing the flow of execution.

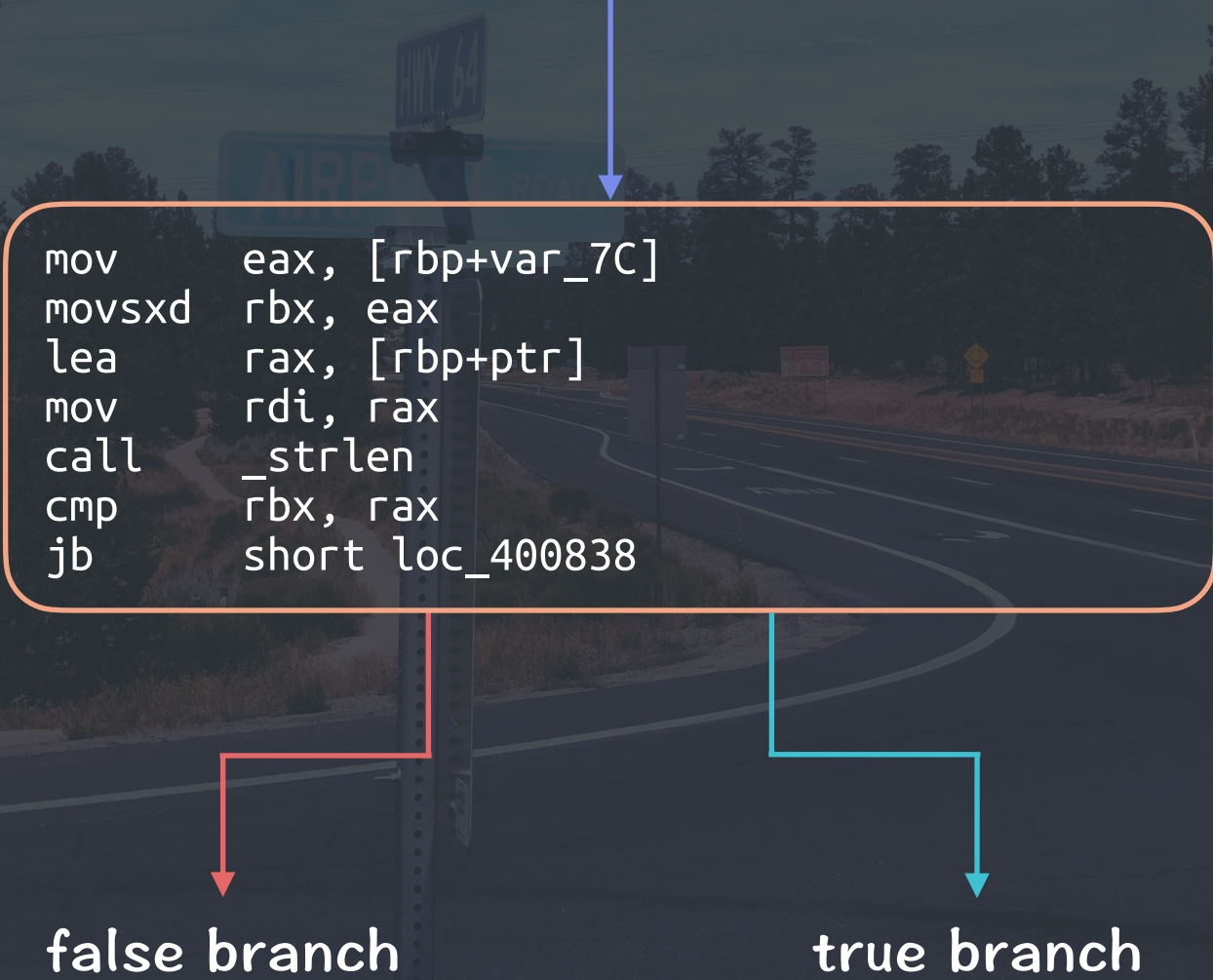
```
mov     edi, offset s    ;"Do the right thing"  
call    _puts  
jmp     short loc_4008AB
```



# CFG

## Control-flow Graph

CFG is a graph with (conceptually) basic blocks as nodes and jumps/calls/rets/etc as edges. - angr



```
mov     eax, [rbp+var_7C]
movsxd  rbx, eax
lea     rax, [rbp+ptr]
mov     rdi, rax
call    _strlen
cmp     rbx, rax
jb      short loc_400838
```

false branch

true branch

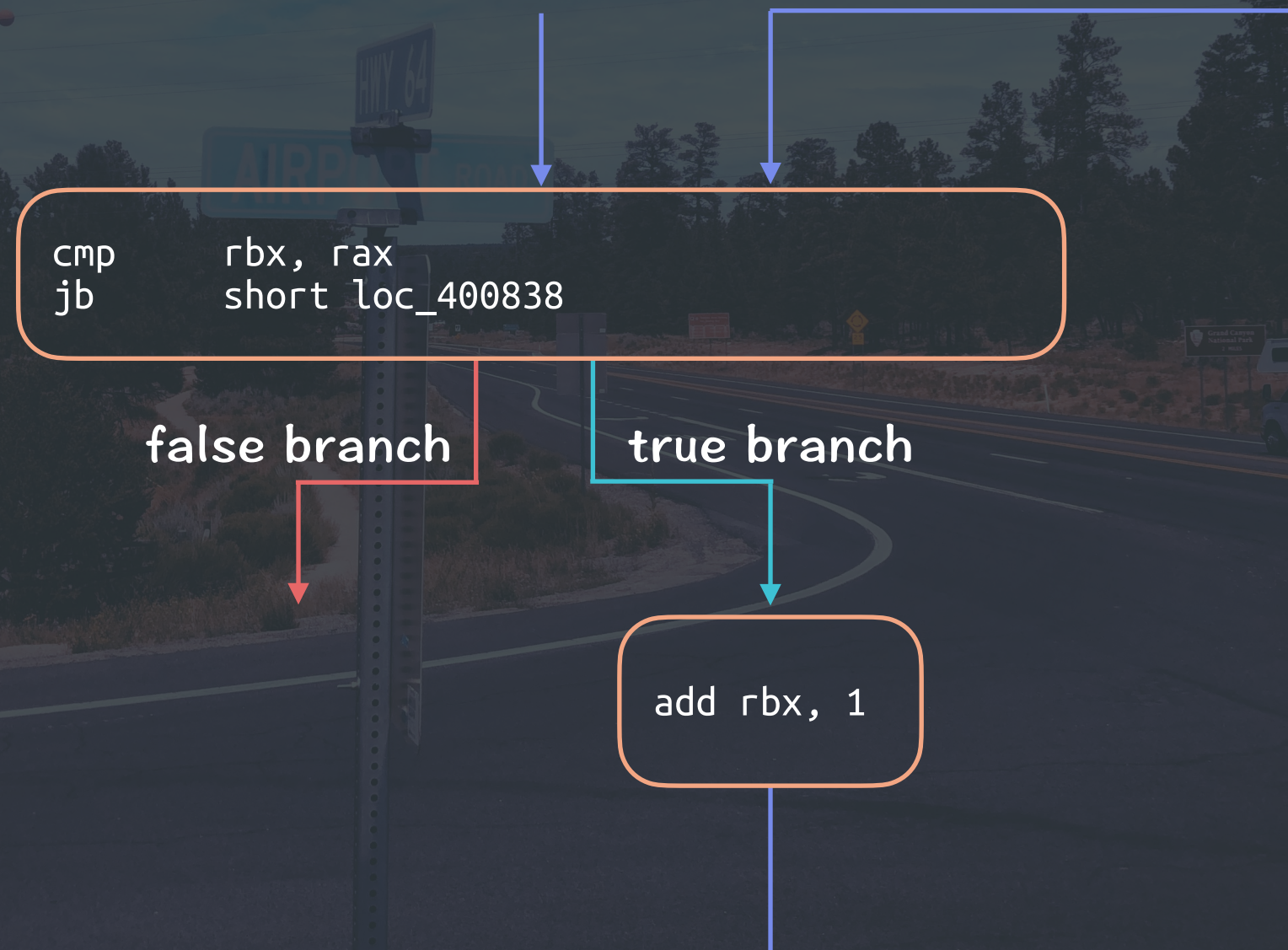




# CFG

## Control-flow Graph

CFG is a graph with (conceptually) basic blocks as nodes and jumps/calls/rets/etc as edges. - angr



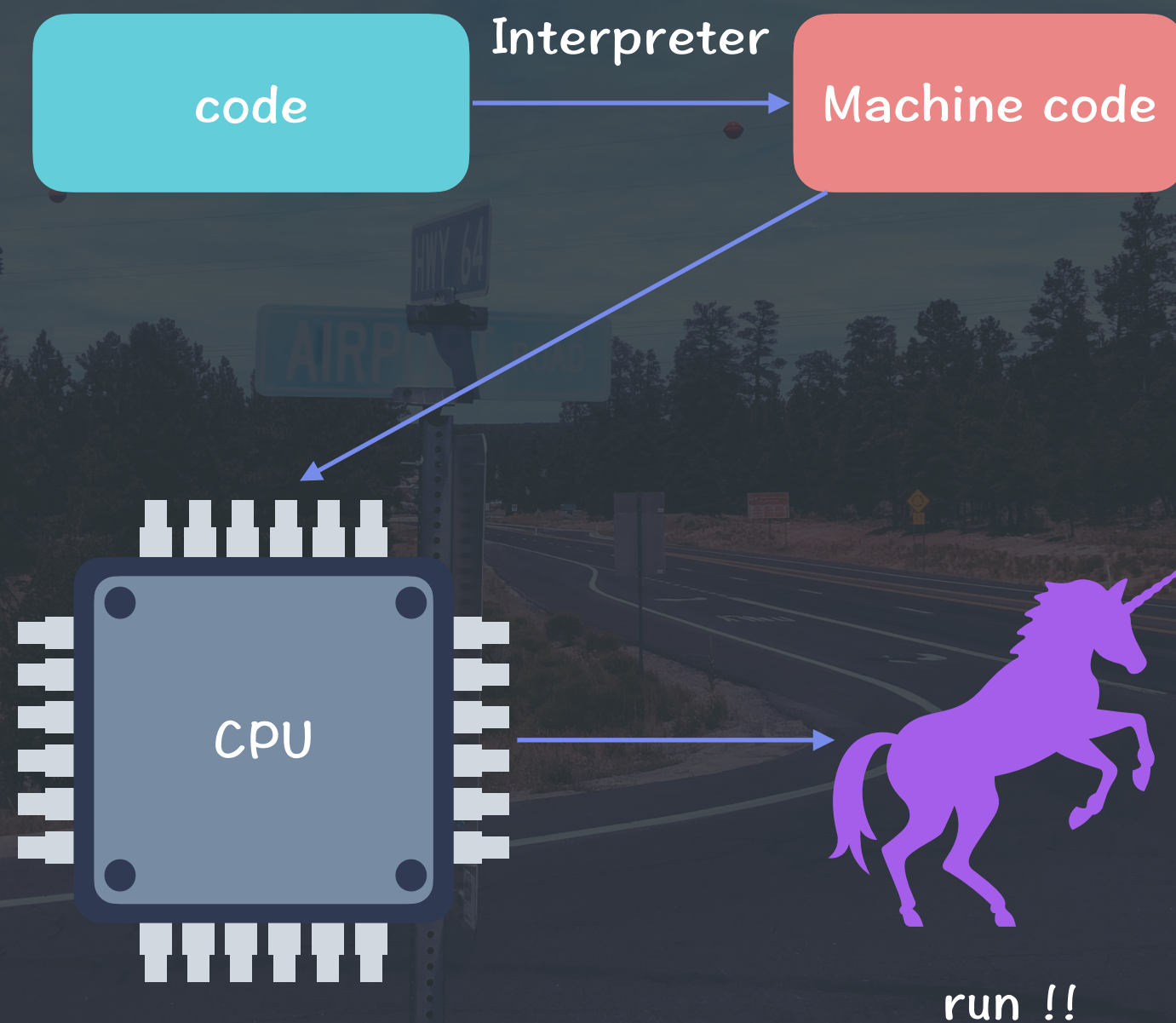


Try it!



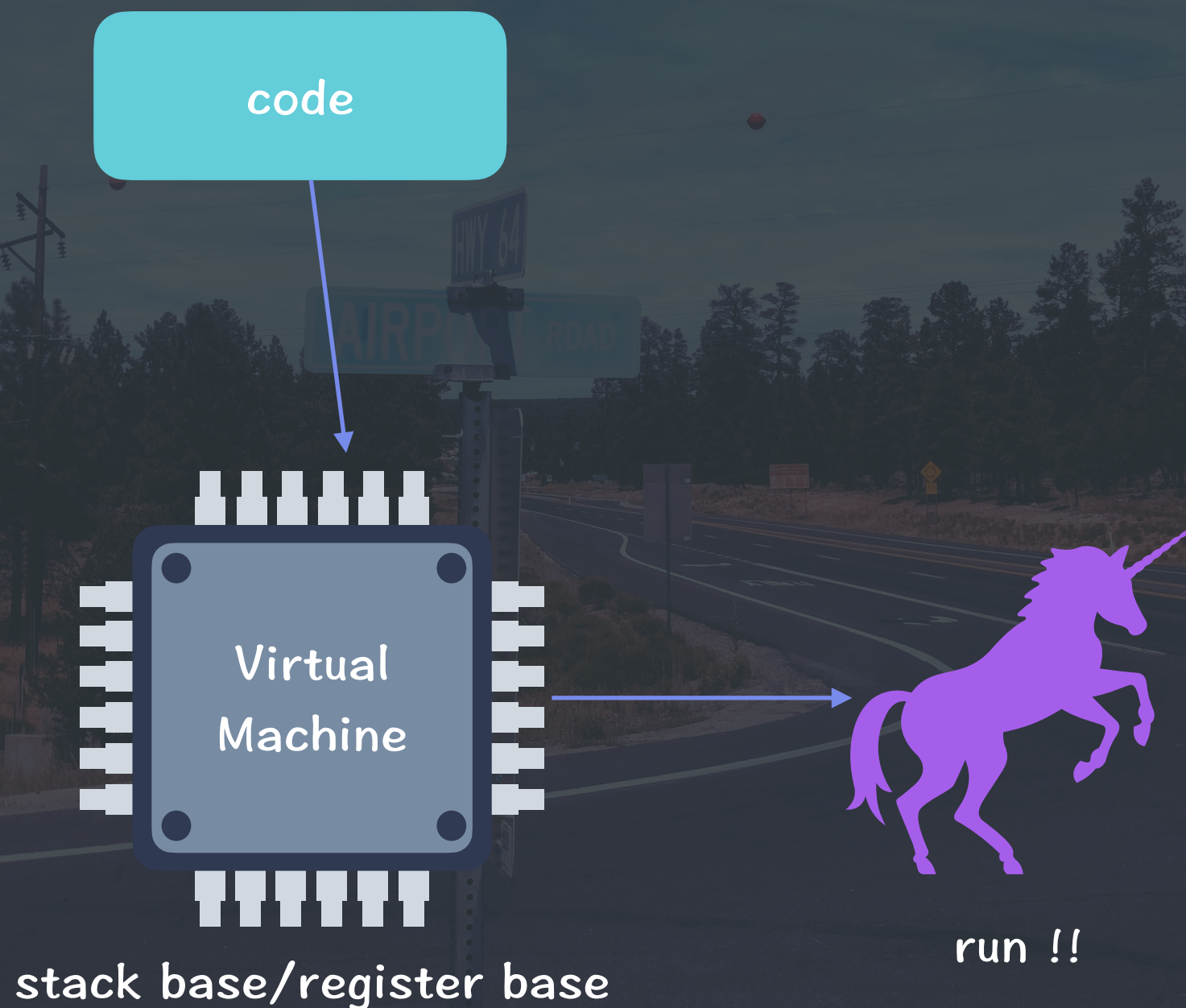


# Interpreted language



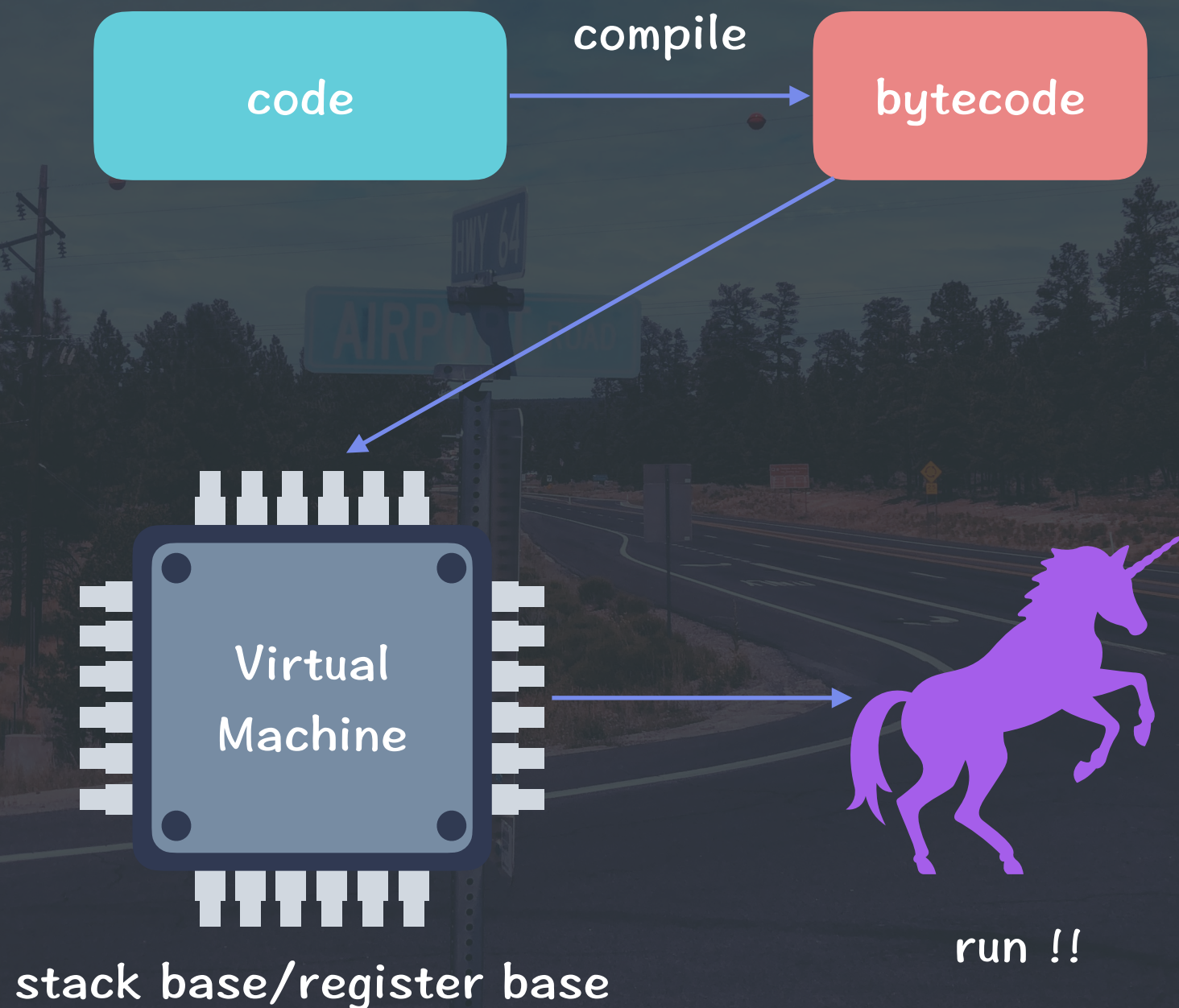


# Interpreted language





# Interpreted language





# .NET PE

PE HEADER

CLR HEADER

CLR DATA

Other Sections





Try it!





# Learn from CTF

## Magic Number

TeaserDragon\_2018  
Brutal oldskull





# Learn from CTF

Codegate2020  
Malicious





# Learn from CTF

PlaidCTF  
reee





# Learn from CTF

SMT solver

PlaidCTF  
you\_wa\_shockwave





# Learn from CTF





# Learn from CTF

Flare-on  
12-Help

