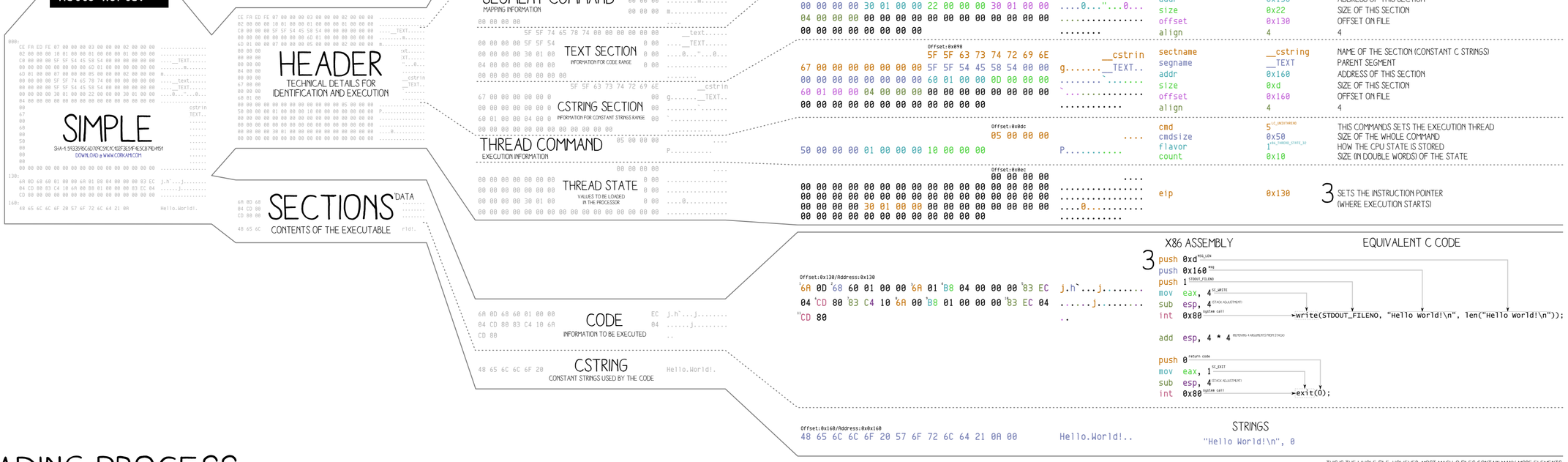
MACH-O[101] an OS X executable walkthrough

ANGE ALBERTINI
CORKAMI.COM

DISSECTED FILE

```
~$ uname -s -m
Darwin x86_64
~$ ./simple
Hello World!
```



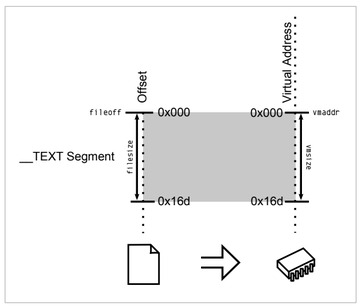
LOADING PROCESS

1 HEADER

THE MACH-O HEADER IS PARSED
THE COMMANDS ARE PARSED

2 MAPPING

THE FILE IS MAPPED IN MEMORY ACCORDING TO ITS SEGMENT(S) AND SECTIONS



3 EXECUTION

THE THREAD STATE IS LOADED IN THE CPU
EXECUTION IS RESUMED

SYSCALLS[KERNEL SERVICES] ARE ACCESSED VIA:
- SYSCALL NUMBER IN THE EAX REGISTER
- CALLING INTERRUPT 0X80

TRIVIA

THE MACH-O FORMAT COMES FROM THE MACH KERNEL, CREATED AT C[CARNEGIE MELLON UNIVERSITY]M[MACHINE]U[UNIVERSAL], IN 1985

IT'S USED AMONG OTHERS,
BY OS X[NEXT], IOS, [NEXT OPEN]STEP...
ON IPHONES, IPODS, MACS...

VERSION 1.0A
2013/12/27
CC BY