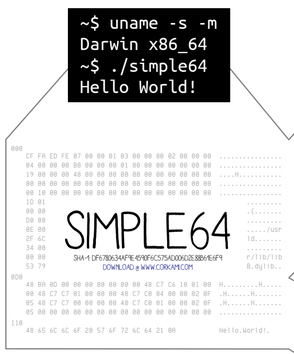
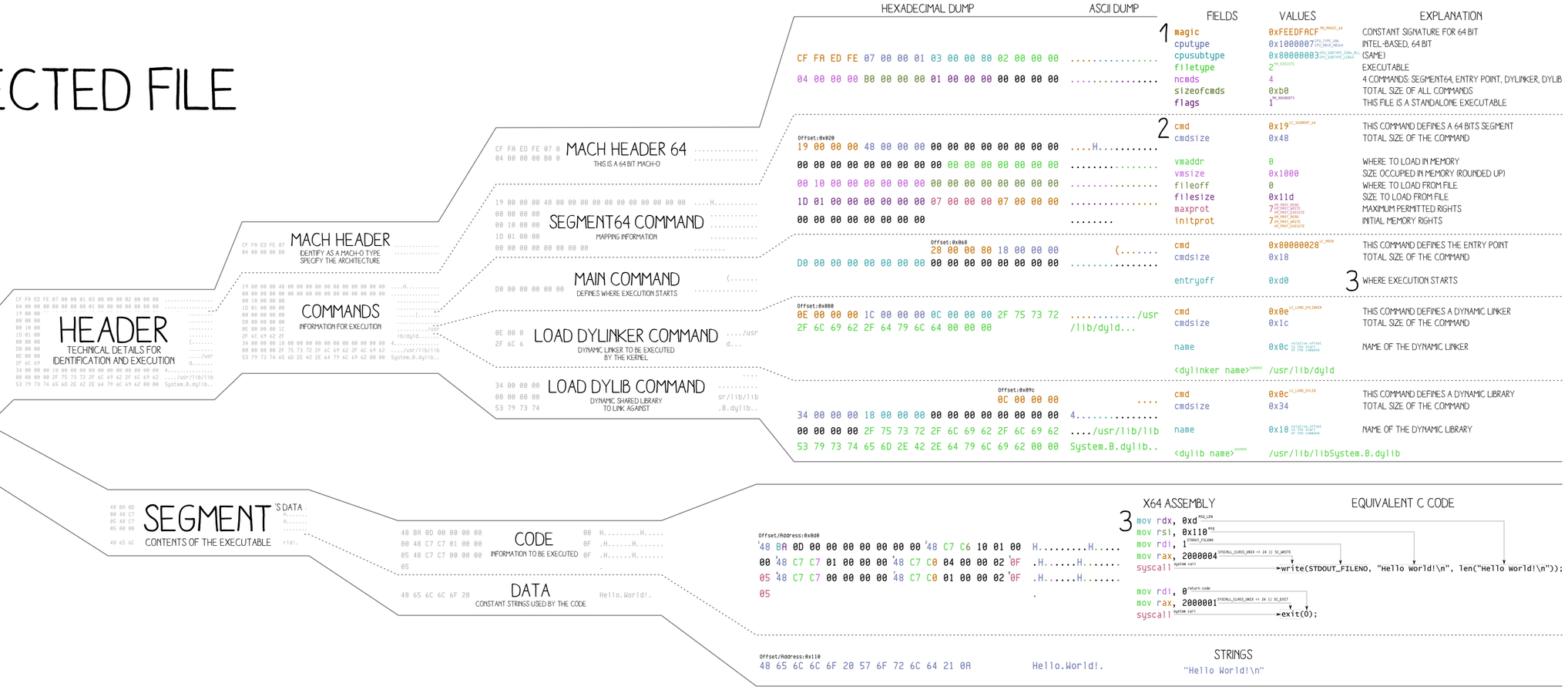
MACH-O 101 (OBJECT FILE FORMAT) a 64b OS X executable walk-through

ANGE ALBERTINI
CORKAMI.COM



DISSECTED FILE



THIS KIND OF MACH-O FILES IS ONLY SUPPORTED SINCE OS X VERSION 10.8 (MOUNTAIN LION).
THIS IS THE WHOLE FILE. HOWEVER, MOST MACH-O FILES CONTAIN MANY MORE ELEMENTS.
EXPLANATIONS ARE SIMPLIFIED, FOR CONCISENESS.

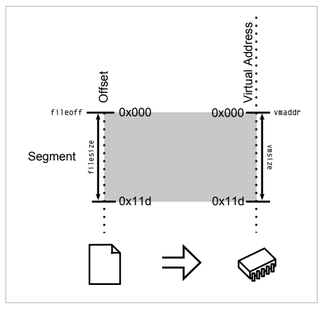
LOADING PROCESS

1 HEADER

THE MACH-O HEADER IS PARSED
THE COMMANDS ARE PARSED

2 MAPPING

THE FILE IS MAPPED IN MEMORY ACCORDING TO ITS SEGMENT AND COMMANDS



3 EXECUTION

THE ENTRY POINT IS CALLED

SYSCALLS (KERNEL SERVICES) ARE ACCESSED VIA:
- SYSCALL NUMBER AND CLASS, IN THE RAX REGISTER
- CALLING INSTRUCTION SYSCALL

TRIVIA

THE MACH-O FORMAT COMES FROM THE MACH KERNEL, CREATED AT C"M"U, (CARNEGIE MELLON UNIVERSITY) IN 1985

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

VERSION 1.00
2014/01/02