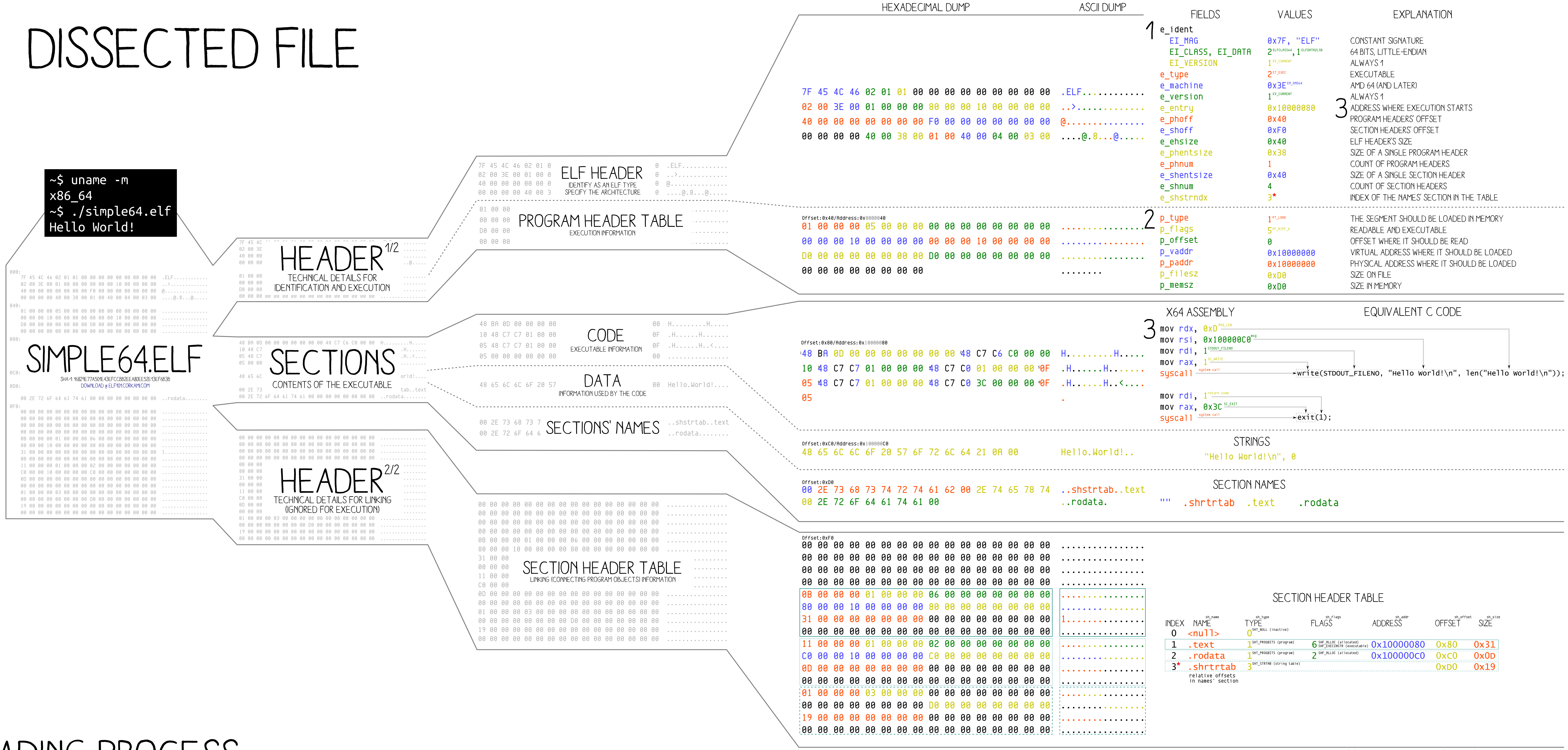
ELF[101] a Linux executable walkthrough

ANGE ALBERTINI
CORKAMI.COM

DISSECTED FILE


~$ uname -m
x86_64
~$ ./simple64.elf
Hello World!
SIMPLE64.ELF
HEADER 1/2
TECHNICAL DETAILS FOR IDENTIFICATION AND EXECUTION
SECTIONS
CONTENTS OF THE EXECUTABLE
HEADER 2/2
TECHNICAL DETAILS FOR LINKING (IGNORED FOR EXECUTION)
ELF HEADER
IDENTIFY AS AN ELF TYPE
SPECIFY THE ARCHITECTURE
PROGRAM HEADER TABLE
EXECUTION INFORMATION
CODE
EXECUTABLE INFORMATION
DATA
INFORMATION USED BY THE CODE
SECTIONS' NAMES
SECTION HEADER TABLE
LINKING (CONNECTING PROGRAM OBJECTS) INFORMATION
HEXADECIMAL DUMP
ASCII DUMP
FIELDS
VALUES
EXPLANATION
e_ident
EI_MAG 0x7F, "ELF" CONSTANT SIGNATURE
EI_CLASS, EI_DATA 2, 1 64 BITS, LITTLE-ENDIAN
EI_VERSION 1 ALWAYS 1
e_type 2 EXECUTABLE
e_machine 0x3E AMD 64 (AND LATER)
e_version 1 ALWAYS 1
e_entry 0x10000080 ADDRESS WHERE EXECUTION STARTS
e_phoff 0x40 PROGRAM HEADERS' OFFSET
e_shoff 0xF0 SECTION HEADERS' OFFSET
e_ehsize 0x40 ELF HEADER'S SIZE
e_phentsize 0x38 SIZE OF A SINGLE PROGRAM HEADER
e_phnum 1 COUNT OF PROGRAM HEADERS
e_shentsize 0x40 SIZE OF A SINGLE SECTION HEADER
e_shnum 4 COUNT OF SECTION HEADERS
e_shstrndx 3* INDEX OF THE NAMES' SECTION IN THE TABLE
p_type 1 THE SEGMENT SHOULD BE LOADED IN MEMORY
p_flags 5 READABLE AND EXECUTABLE
p_offset 0 OFFSET WHERE IT SHOULD BE READ
p_vaddr 0x10000000 VIRTUAL ADDRESS WHERE IT SHOULD BE LOADED
p_paddr 0x10000000 PHYSICAL ADDRESS WHERE IT SHOULD BE LOADED
p_filesz 0xD0 SIZE ON FILE
p_memsz 0xD0 SIZE IN MEMORY
X64 ASSEMBLY
EQUIVALENT C CODE
mov rdx, 0xD
mov rsi, 0x100000C0
mov rdi, 1
mov rax, 1
syscall
write(STDOUT_FILENO, "Hello World!\n", len("Hello World!\n"));
mov rdi, 1
mov rax, 0x3C
syscall
exit(1);
STRINGS
"Hello World!\n", 0
SECTION NAMES
"" .shrtrtab .text .rodata
SECTION HEADER TABLE
INDEX NAME TYPE FLAGS ADDRESS OFFSET SIZE
0 <null> 0
1 .text 1 6 0x10000080 0x80 0x31
2 .rodata 1 2 0x100000C0 0xC0 0x0D
3* .shrtrtab 3 0xD0 0x19
THIS IS THE WHOLE FILE. HOWEVER, MOST ELF FILES CONTAIN MANY MORE ELEMENTS.
EXPLANATIONS ARE SIMPLIFIED, FOR CONCISENESS.

LOADING PROCESS

1 HEADER

THE ELF HEADER IS PARSED

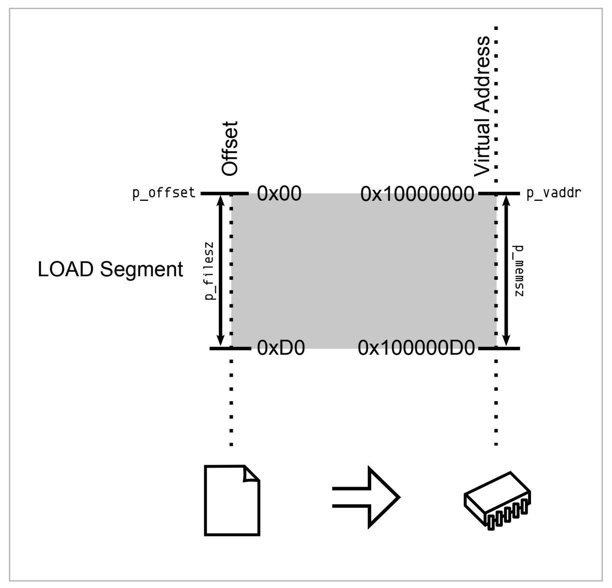
THE PROGRAM HEADER IS PARSED

(SECTIONS ARE NOT USED)

2 MAPPING

THE FILE IS MAPPED IN MEMORY

ACCORDING TO ITS SEGMENT(S)



3 EXECUTION

ENTRY IS CALLED

SYSCALLS ARE ACCESSED VIA:

- SYSCALL NUMBER IN THE RAX REGISTER
- CALLING INSTRUCTION SYSCALL

TRIVIA

THE ELF WAS FIRST SPECIFIED BY U.S. L. AND U.I.
FOR UNIX SYSTEM V, IN 1989

THE ELF IS USED, AMONG OTHERS, IN:

- LINUX, ANDROID, *BSD, SOLARIS, BEOS
- PSP, PLAYSTATION 2-4, DREAMCAST, GAMECUBE, WII
- VARIOUS OSES MADE BY SAMSUNG, ERICSSON, NOKIA,
- MICROCONTROLLERS FROM ATMEL, TEXAS INSTRUMENTS

VERSION 1.0C
2013/12/04