Executable and Linkable Format

```
me@nux:~$ ./mini
me@nux:~$ echo $?
42
```

```
    0  1  2  3  4  5  6  7  8  9  A  B  C  D  E  F
00: 7F .E .L .F 01 01 01
10: 02 00 03 00 01 00 00 00 60 00 00 08 40 00 00 00
20:                         34 00 20 00 01 00

40: 01 00 00 00 00 00 00 00 00 00 00 08 00 00 00 08
50: 70 00 00 00 70 00 00 00 05 00 00 00

60: BB 2A 00 00 00 B8 01 00 00 00 CD 80
```

ELF HEADER

IDENTIFY AS AN ELF TYPE
SPECIFY THE ARCHITECTURE

FIELDS	VALUES
e_ident	
EI_MAG	0x7F, "ELF"
EI_CLASS, EI_DATA	1 ELFCLASS32, 1 ELFDATA2LSB
EI_VERSION	1 EV_CURRENT
e_type	2 ET_EXEC
e_machine	3 EM_386
e_version	1 EV_CURRENT
e_entry	0x8000060
e_phoff	0x0000040
e_ehsize	0x0034
e_phentsize	0x0020
e_phnum	0001

PROGRAM HEADER TABLE

EXECUTION INFORMATION

p_type	1 PT_LOAD
p_offset	0
p_vaddr	0x8000000
p_paddr	0x8000000
p_filesz	0x0000070
p_memsz	0x0000070
p_flags	5 PF_R|PF_X

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

CODE

X86 ASSEMBLY

```
mov ebx, 42
mov eax, 1
int 80h
```

SC_EXIT

EQUIVALENT C CODE

```
return 42;
```

Mach-O Object File Format

```
mac:~ me$ ./mini
mac:~ me$ echo $?
42
```

```
    0  1  2  3  4  5  6  7  8  9  A  B  C  D  E  F
00: CE FA ED FE 07 00 00 00 03 00 00 00 02 00 00 00
10: 02 00 00 00 88 00 00 00           01 00 00 00
20: 38 00 00 00
30:             00 00 00 00 C0 00 00 00 00 00 00 00
40: C0 00 00 00           05 00 00 00
50:          05 00 00 00 50 00 00 00 01 00 00 00
60: 10 00 00 00
70:
80:                                  B0 00 00 00

B0: 6A 2A B8 01 00 00 00 83 EC 04 CD 80
```

MACH HEADER

IDENTIFY AS A MACH-O TYPE
SPECIFY THE ARCHITECTURE

FIELDS	VALUES
magic	0xFEEDFACE MH_MAGIC
cputype	7 CPU_TYPE_I386
cpusubtype	3 CPU_SUBTYPE_I386_ALL
filetype	2 MH_EXECUTE
ncmds	2
sizeofcmds	0x88

SEGMENT COMMAND

MAPPING INFORMATION

cmd	1 LC_SEGMENT
cmdsize	0x38
vmaddr	0
vmsize	0xc0
fileoff	0
filesize	0xc0
initprot	5 R|X

THREAD COMMAND

EXECUTION INFORMATION

cmd	5 LC_UNIXTHREAD
cmdsize	0x50
flavor	1 x86_THREAD_STATE_32
count	0x10

THREAD STATE

VALUES TO BE LOADED IN THE PROCESSOR

eip	0xb0

USED AMONG OTHERS,
BY OS X, IOS, STEP...
ON IPHONES, IPODS, MACS...
THE MACH-O FORMAT COMES FROM THE MACH KERNEL,
CREATED AT CARNEGIE MELLON UNIVERSITY IN 1985

CODE

X86 ASSEMBLY

```
push 42
mov  eax, 1
sub  esp, 4
int  0x80
```

SC_EXIT

(STACK ADJUSTMENT)

system call

EQUIVALENT C CODE

```
return 42;
```

Portable Executable

```
D:\>mini.exe

D:\>echo %errorlevel%
42
```

```
    0  1  2  3  4  5  6  7  8  9  A  B  C  D  E  F
000: .M .Z

030:                                  40 00 00 00
040: .P .E 00 00 4C 01
050:                  02 00 0B 01
060:                        40 01 00 00
070:            00 00 40 00 01 00 00 00 01 00 00 00
080:                        04 00
090: 60 01 00 00 40 01 00 00           03 00

140: B8 2A 00 00 00 C3
```

DOS HEADER

IT'S A BINARY

FIELDS	VALUES
e_magic	MZ
e_lfanew	0x40 → PE Header

PE HEADER

IT'S A 'MODERN' BINARY

→Signature	PE\0\0
Machine	0x14C [intel 386]
Characteristics	2 [executable]

OPTIONAL HEADER

EXECUTABLE INFORMATION

Magic	0x10B [32b]
AddressOfEntryPoint	0x140
ImageBase	0x400000
SectionAlignment	1
FileAlignment	1
MajorSubsystemVersion	4 [NT 4 or later]
SizeOfImage	0x160
SizeOfHeaders	0x140
Subsystem	3 [CLI]

USED IN:
- ALL WINDOWS SINCE NT 3.1 (RELEASED IN 1993)
- WINDOWS CE, RT, MOBILE
- XBOX, .NET

CODE

X86 ASSEMBLY

```
mov eax, 42
retn
```

EQUIVALENT C CODE

```
return 42;
```

THE "MZ" MAGIC COMES FROM MARK ZBIKOWSKI (MS-DOS DEV.)
THE OPTIONAL HEADER IS REQUIRED FOR EXECUTABLES.