



从零开始

DEVELOPING YOUR OWN

自制操作系统

实践
Practice

OPERATING SYSTEM DEVELOPMENT

TUTORIAL SERIES

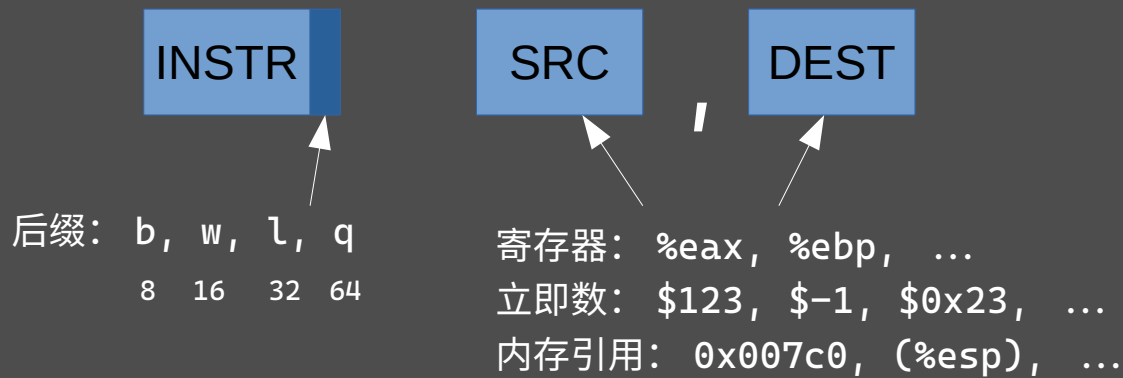
EP 5-4.1

开始编码!

ATT ASM & Multiboot



AT&T vs. Intel Assembly



Intel

```
mov ax, 12
```

```
mov eax, DWORD PTR [0x007c0]
```

```
cmp eax, ebx
```

```
add eax, 1
```

AT&T

Mnemonics: move **word** 12 to register(%) ax

```
movw $12, %ax
```

```
movl 0x007c0, %eax
```

```
cmpl %ebx, %eax
```

```
addl $1, %eax
```



什么是 Multiboot ?

一个相当成熟的 Bootloader 规范（家喻户晓的 GRUB 便是这个标准的一个实现）

Spec:

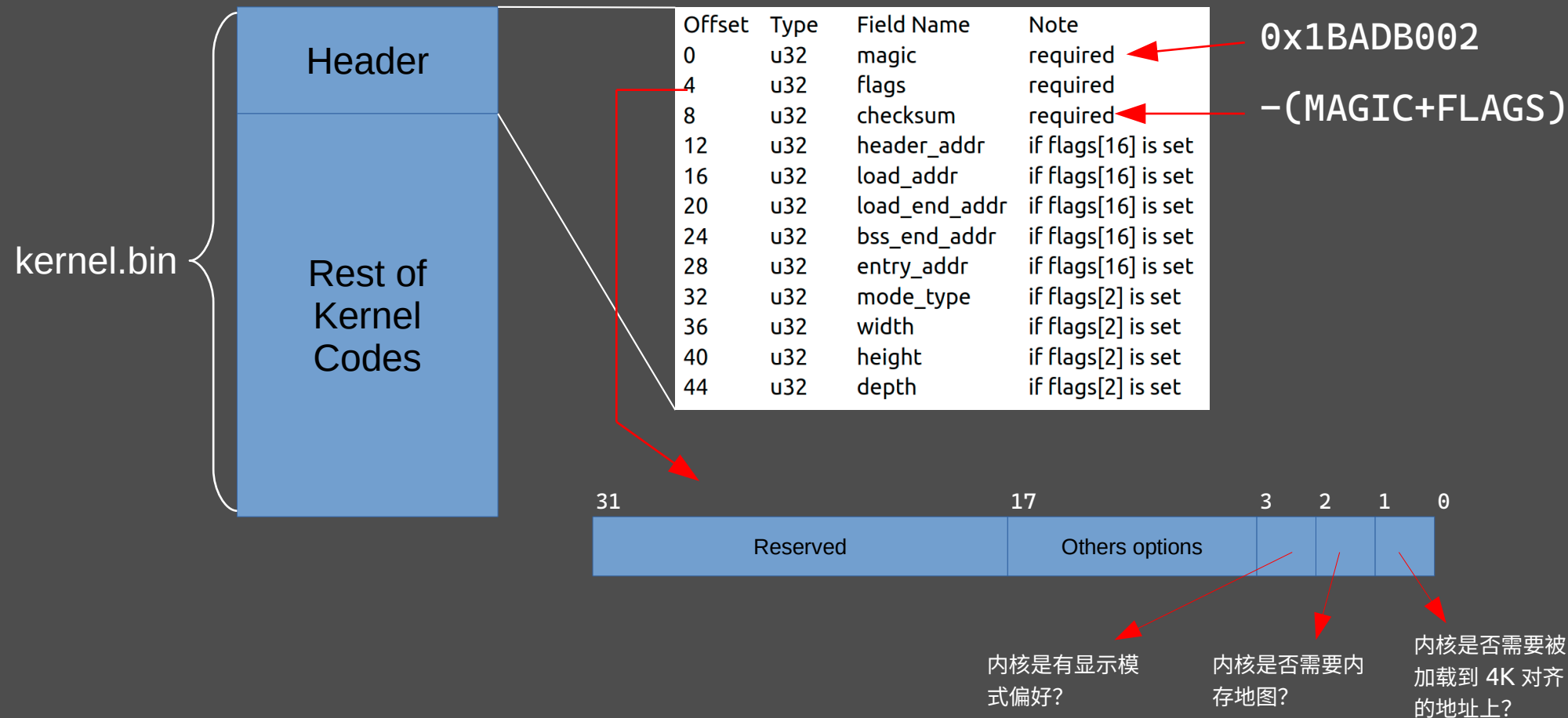
<https://www.gnu.org/software/grub/manual/multiboot/multiboot.html>

省去了相当的麻烦：比如加载内核，开启 A20 总线（ Tricky! ），进入保护模式

允许我们直接进入内核的开发！



如何声明我们的 OS 是 Multiboot 兼容的?





加载后，我们处在一个什么样的状态？

已定义（节选）

`%EAX = 0x2BADB002`

`%EBX = Bootloader 信息表
物理地址`

`%{C|D|E|F|G|S}S = 0x0`

A20：已打开

`%CR0 = (%CR0 & 0x7FFFFFFF) | 0x1`

`%EFLAGS = %EFLAGS & 0xFFFFEFFF`

未定义（需要我们自己设定）

`%ESP`：调用栈地址（非常重要！）

`%GDTR, %IDTR`：描述表，中断表

GDTR 未初始化！在我们设定他以前，避免任何对 `%{C|D|E|F|G|S}S` 的操作！否则会引发 `#GP` 异常，进而导致 `Triple Fault`.

`PE = 1, PG = 0`

`IF = VM = 0` (Interrupts disabled!)



0	+	+	0	+	+
		flags			
	+	+		+	+
4		mem_lower	(present if flags[0] is set)	72	vbe_control_info
8		mem_upper	(present if flags[0] is set)	76	vbe_mode_info
	+	+		80	vbe_mode
12		boot_device	(present if flags[1] is set)	82	vbe_interface_seg
	+	+		84	vbe_interface_off
16		cmdline	(present if flags[2] is set)	86	vbe_interface_len
	+	+			+
20		mods_count	(present if flags[3] is set)	88	framebuffer_addr
24		mods_addr	(present if flags[3] is set)	96	framebuffer_pitch
	+	+		100	framebuffer_width
28 - 40		syms	(present if flags[4] or flags[5] is set)	104	framebuffer_height
	+	+		108	framebuffer_bpp
44		mmap_length	(present if flags[6] is set)	109	framebuffer_type
48		mmap_addr	(present if flags[6] is set)	110-115	color_info
	+	+			+
52		drives_length	(present if flags[7] is set)		
56		drives_addr	(present if flags[7] is set)		
	+	+			
60		config_table	(present if flags[8] is set)		
	+	+			
64		boot_loader_name	(present if flags[9] is set)		
	+	+			
68		apm_table	(present if flags[10] is set)		
	+	+			

此 flags 非彼 flags !



Let's code!