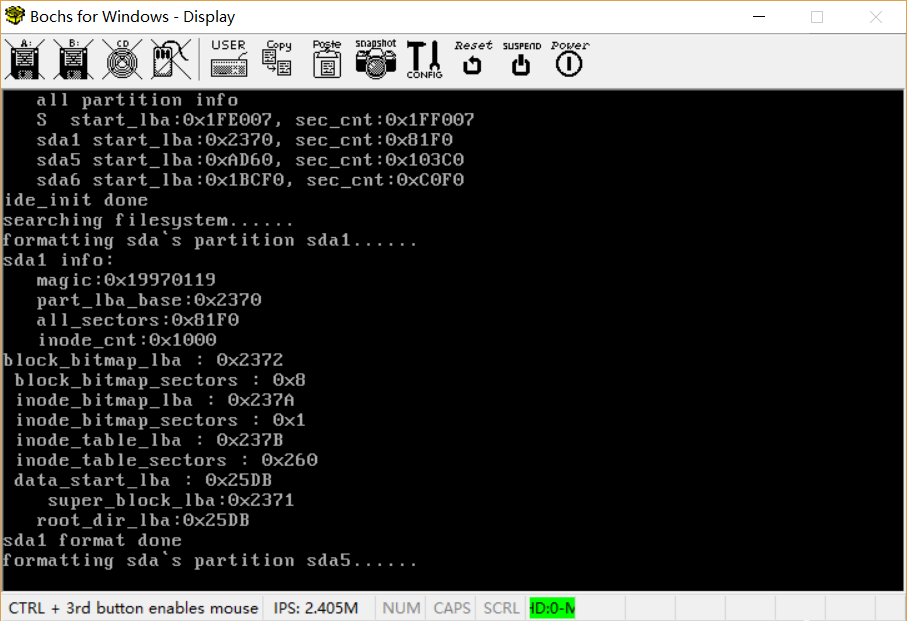
|  |  |  |
| --- | --- | --- |
| 地址范围(物理地址) | |  |
| 0 | 0X3FF | 中断向量表 IVT |
| 0X400 | 0X4FF | BIOS 数据区域 |
| 0X500 | 0X8FF | LOADER栈指针指向0X900 |
| 0X900 | 0X14FF | LOADER |
| 0X1500 | 0X9BFF | 内核程序 |
| 0X9A00 | 0X9DFF | KERNEL/USER、KERNEL VADDR POOL BITMAP |
| 0X9E00 | 0X9EFF | 内核栈顶->0X9F00、PCB->0X9E00 |
| 0X9F00 | 0X9FFFF |  |
| 0X7C00 | 0X7DFF | MBR |
| 0X7E00 | 0X6FFFF |  |
| 0X70000 |  | KERNEL.BIN |
| 0X9FC00 | 0X9FFFF | 扩展BIOS数据区 |
| 0XA0000 | 0XFFFFF |  |
| 0X100000 | 0X100fff | PDE（初始化第0、768、1023个） |
| 0X101000 | 0X200000 | PTE(虚拟地址高1GB的映射 0=768、769-1022、1023=0X100000) |



|  |  |
| --- | --- |
| MBR | 把loader加载到0x900 |
| LOADER | 0x900 loader大小(随后装入内存大小) |
| 0x904 loader 入口地址 |
| 0x90A GDT 地址 |
| 进入保护模式、加载页表、读取kernel |
| Lib/kernel/print | 操控 0xb8000 显示 |
| Kernel/init | 初始化操作 |

Kernel/interrupt

发生中断🡪intr\_entry\_table[中断号] 响应中断🡪idt\_table[中断号] 处理中断

栈变化：

|  |
| --- |
| SS(发生特权级变化时) |
| ESP(发生特权级变化时) |
| EFLAGS |
| CS |
| IP |
| ERROR\_CODE |
| Kernel.asm: |
| DS |
| ES |
| FS |
| GS |
| PUSHAD |
| 中断号 |