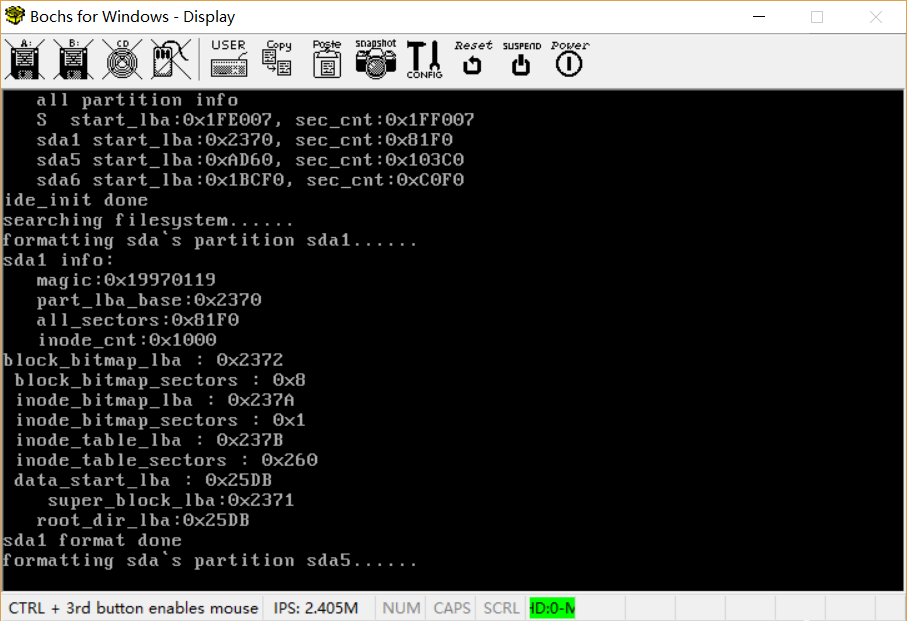
|  |  |  |
| --- | --- | --- |
| 地址范围(物理地址) | |  |
| 0 | 0X3FF | 中断向量表 IVT |
| 0X400 | 0X4FF | BIOS 数据区域 |
| 0X500 | 0X8FF | LOADER栈指针指向0X900 |
| 0X900 | 0X14FF | LOADER |
| 0X1500 | 0X7BFF | 内核程序 |
| 0X7C00 | 0X7DFF | MBR |
| 0X7E00 | 0X6FFFF |  |
| 0X70000 |  | KERNEL.BIN |
| 0X9A000 | 0X9DFFF | 内核内存位图、用户内存位图、内核虚拟地址位图 |
| 0X9E000 | 0X9EFFF | 内核栈顶->0X9F00、PCB->0X9E00 |
| 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 | 中断 |

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 |

|  |  |
| --- | --- |
| Device/timer | 初始化定时器、中断处理函数 |

|  |  |
| --- | --- |
| Kernel/memory | 内存管理、分配 |

mem\_block\_desc k\_block\_descs [7]

可分配 16、32、64、128、256、512、1024为单位的内存

kernel\_pool

内核物理内存池

user\_pool

用户物理内存池

kernel\_vaddr

内核虚拟地址内存池

sys\_malloc 分配内存

大于1024字节的内存直接分配页整数倍

小于1024字节每次分配一页后细分

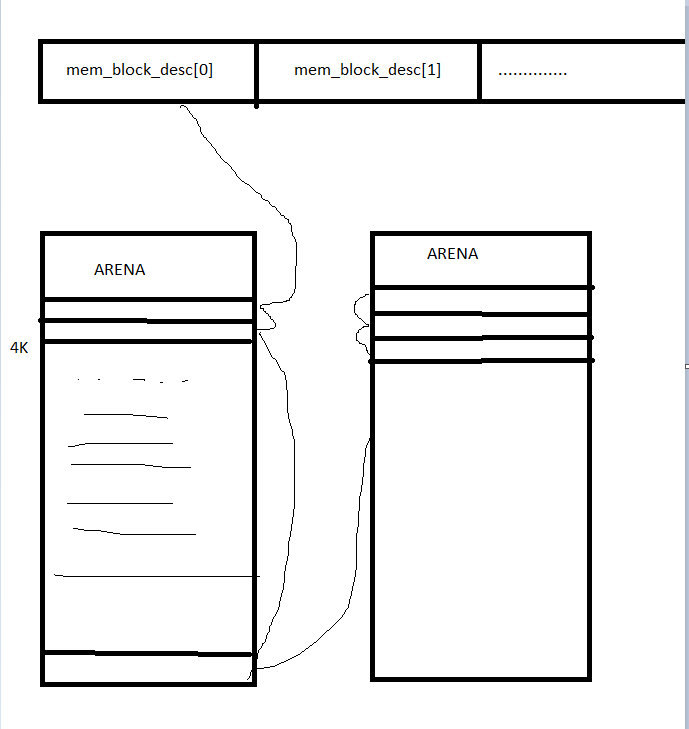
|  |  |
| --- | --- |
| arena | 每页头部信息 |
| mem\_block\_desc | 细分的字节数（block\_size）  组成链表 |
| mem\_block\_desc |
| mem\_block\_desc |
| mem\_block\_desc |

sys\_free 释放内存

大于1024字节的内存直接释放

小于1024字节的内存地址& 0xfffff000可得到 arena结构地址

Arena所在页的内存所分的mem\_block\_desc 的个数与对应每页所能分配的mem\_block\_desc的个数相等时释放内存



Kernel/thread

thread\_stack

内核线程

thread\_ready\_list 就绪队列

填充PCB结构、填充栈、ESP指向thread\_stack头部.

Schedule 调度时switch\_to返回到kernel\_thread、 kernel\_thread执行

function（func\_arg）

|  |
| --- |
| intr\_stack: |
| 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 |
| thread\_stack: |
| FUNC\_ARG(参数) |
| FUNCTION（参数） |
| RET ADDR（填充） |
| EIP(返回地址) kernel\_thread |
| ESI |
| EDI |
| EBX |
| EBP |
|  |
| ………………… |
|  |
| task\_struct（PCB） |

esp

用户进程

Schedule 调度时switch\_to返回到 start\_process

start\_process 填充intr\_stack 模拟中断返回 intr\_stack->eip指向用户程序

通过iret返回，完成特权级转换

esp

|  |
| --- |
| intr\_stack: |
| 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 |
| thread\_stack: |
| FUNC\_ARG(参数) |
| FUNCTION（参数） |
| RET ADDR（填充） |
| EIP(返回地址) start\_process |
| ESI |
| EDI |
| EBX |
| EBP |
|  |
| ………………… |
|  |
| task\_struct（PCB） |