

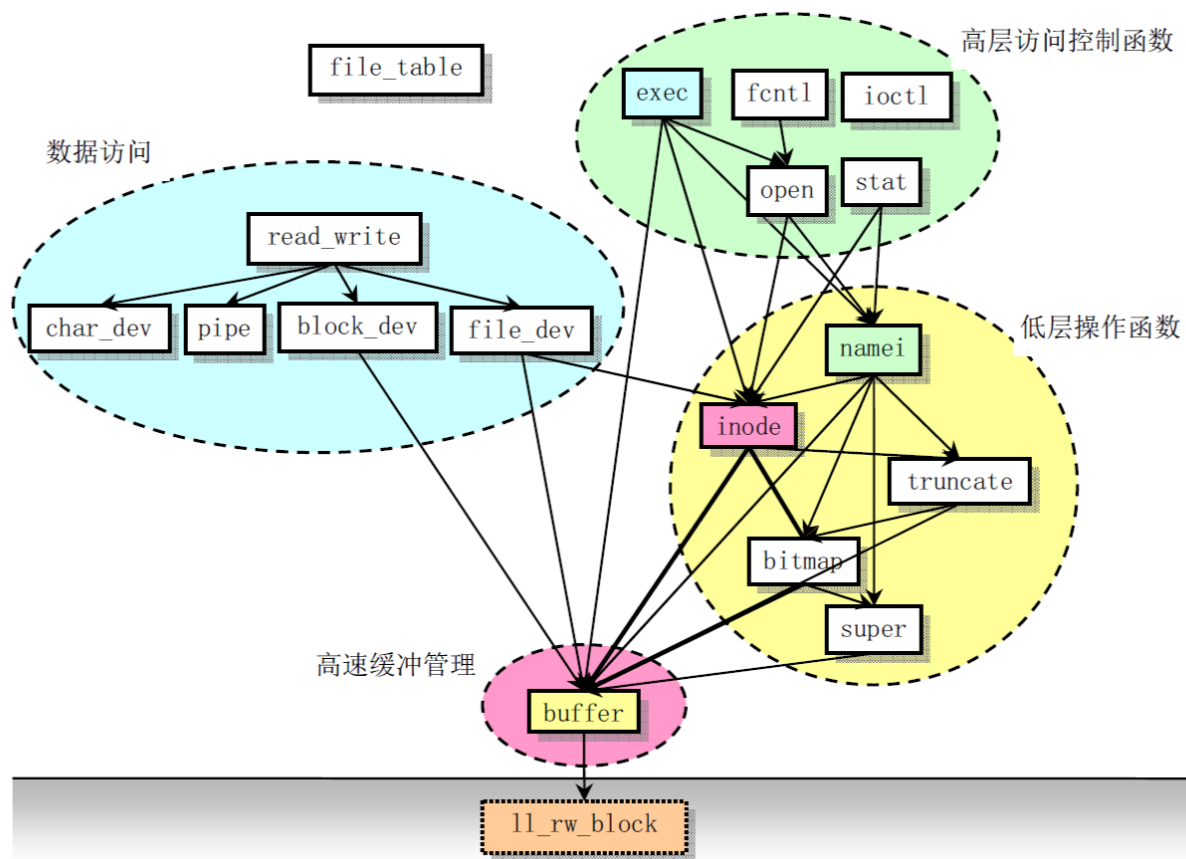
Linux 0.11源码分析与可视化（三）

数据提取与筛选

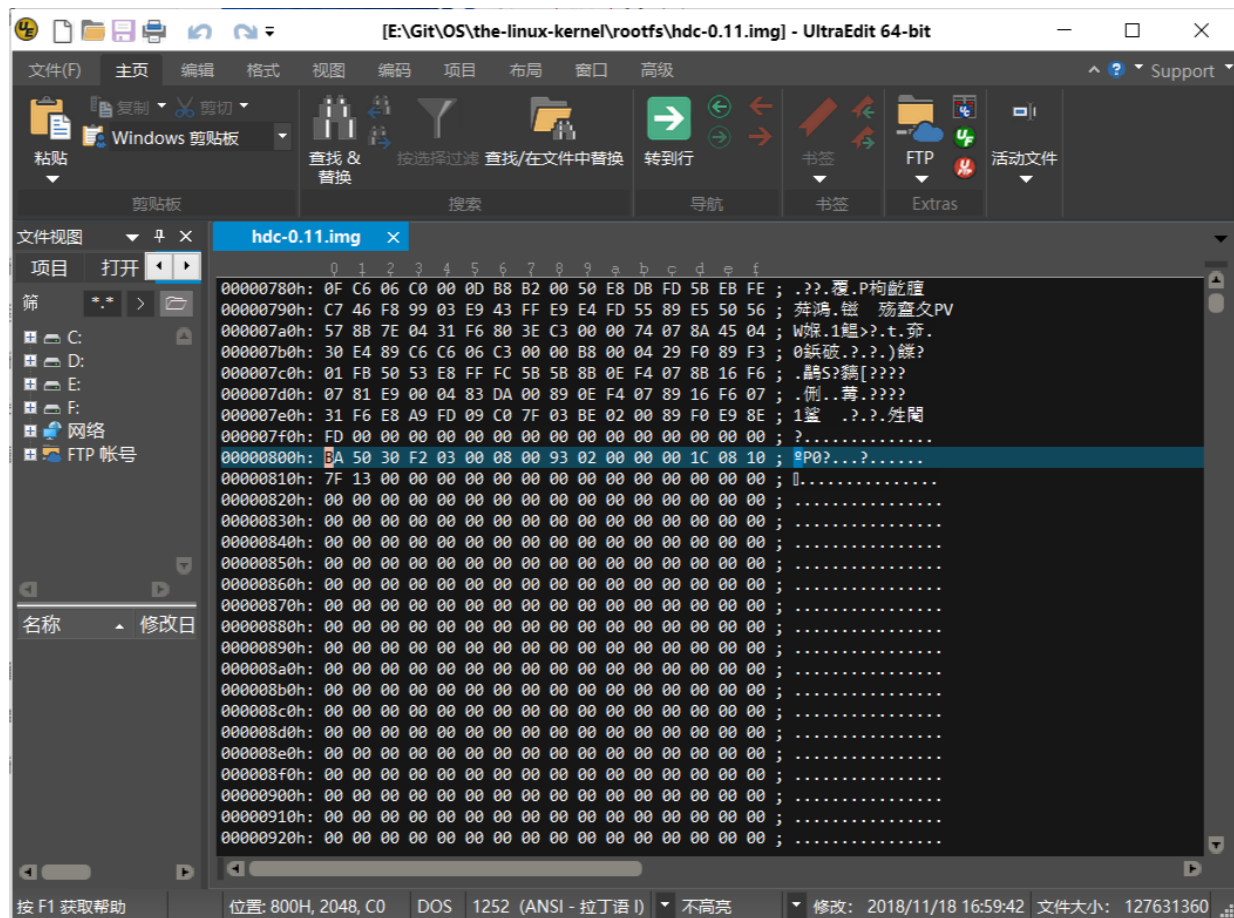
201605130116 杜洪超

201600301291 王文嵩

选读部分-文件系统



文件系统-静态展示



[E:\Git\OS\the-linux-kernel\rootfs\hdc-0.11.img] - UltraEdit 64-bit

文件(F) 主页 编辑 格式 视图 编码 项目 布局 窗口 高级

粘贴 Windows 剪贴板 查找 & 替换 按选择过滤 查找/在文件中替换 转到行 书签 FTP 活动文件

文件视图 hdc-0.11.img

项目 打开

名称 修改日

```
00000780h: 0F C6 06 C0 00 0D B8 B2 00 50 E8 DB FD 5B E8 FE ; .??.覆.P构鮎謹
00000790h: C7 46 F8 99 03 E9 43 FF E9 E4 FD 55 89 E5 50 56 ; 莽鸿.磁 殇查父PV
000007a0h: 57 8B 7E 04 31 F6 80 3E C3 00 00 74 07 8A 45 04 ; W媒.1鯢>?.t.莠.
000007b0h: 30 E4 89 C6 C6 06 C3 00 00 B8 00 04 29 F0 89 F3 ; 0紙破.?.?)鯢?
000007c0h: 01 F8 50 53 E8 FF FC 5B 5B 8B 0E F4 07 8B 16 F6 ; .鯢S?藕[???
000007d0h: 07 81 E9 00 04 83 DA 00 89 0E F4 07 89 16 F6 07 ; .俐..莠.????
000007e0h: 31 F6 E8 A9 FD 09 C0 7F 03 BE 02 00 89 F0 E9 8E ; 1監 .??.姓聞
000007f0h: FD 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ; ?.....
00000800h: 5A 50 30 F2 03 00 08 00 93 02 00 00 00 1C 08 10 ; #P0?...?.....
00000810h: 7F 13 00 00 00 00 00 00 00 00 00 00 00 00 00 ; 0.....
00000820h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ; .....
00000830h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ; .....
00000840h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ; .....
00000850h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ; .....
00000860h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ; .....
00000870h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ; .....
00000880h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ; .....
00000890h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ; .....
000008a0h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ; .....
000008b0h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ; .....
000008c0h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ; .....
000008d0h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ; .....
000008e0h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ; .....
000008f0h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ; .....
00000900h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ; .....
00000910h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ; .....
00000920h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ; .....
```

按 F1 获取帮助 位置: 800H, 2048, C0 DOS 1252 (ANSI - 拉丁语 I) 不高亮 修改: 2018/11/18 16:59:42 文件大小: 127631360

文件系统 hdc-0.11.img

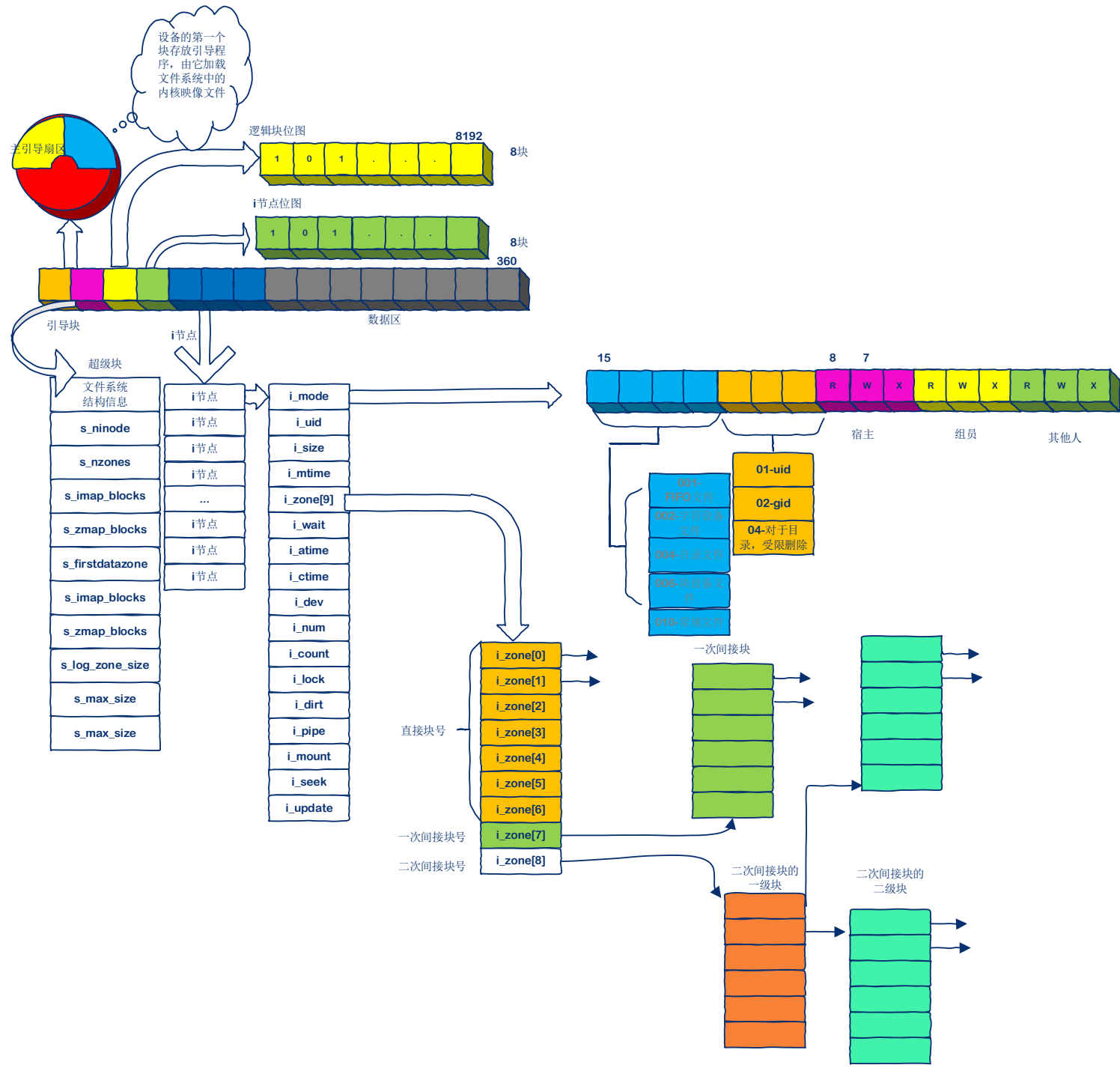
```
mrtd@mrtd-ubuntu16: ~/mrtd/Git/OS/the-linux-kernel/rootfs
命令(输入 m 获取帮助): p
Disk hdc-0.11.img: 121.7 MiB, 127631360 bytes, 249280 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: dos
Disk identifier: 0x00000000

设备          启动  start 末尾 扇区  Size Id 类型
hdc-0.11.img1      2 124031 124030 60.6M 81 Minix / 旧 Linux
hdc-0.11.img2     124032 248063 124032 60.6M 81 Minix / 旧 Linux

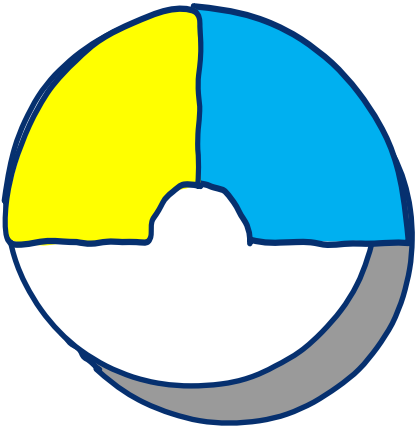
命令(输入 m 获取帮助):
```

文件系统 hdc-0.11.img

- ▣总大小: 124640KB 121MB+736KB 00000000~079B7FFF
- ▣扇区大小: 512bytes
- ▣引导扇区: 00000000~000003FF 1KB
- ▣分区1: 00000800~03C903FF 62016KB 60MB+576KB
- ▣分区2: 03C90400~079207FF 62017KB 60MB+577KB
- ▣其它: 079207FF~079B7FFF 606KB



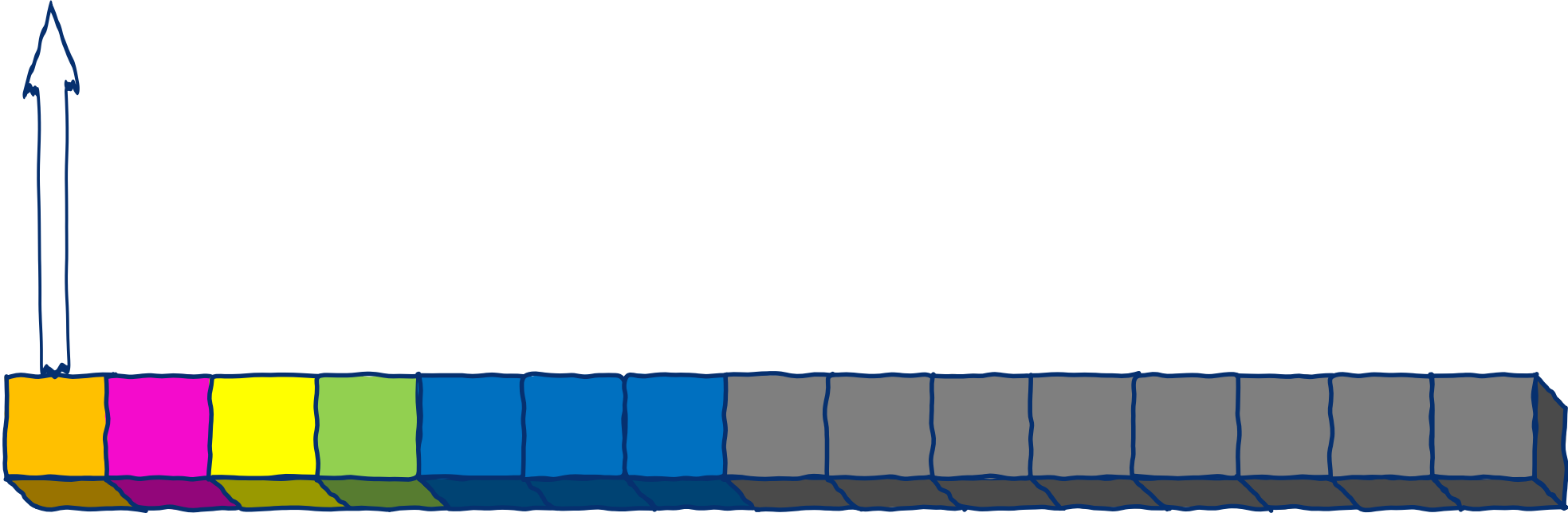
主引导扇区

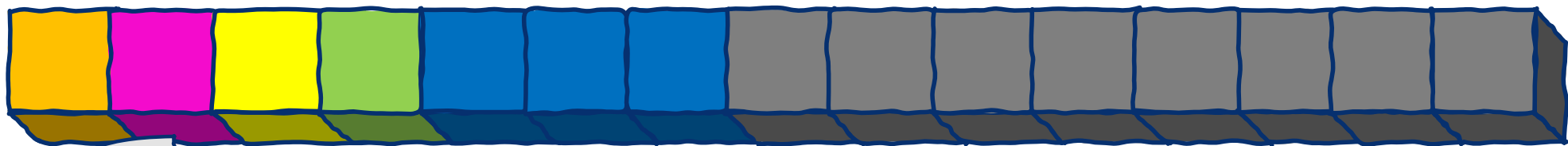


...



00000400~000007FF 1KB





超级块

文件系统
结构信息

s_ninode

s_nzones

s_imap_blocks

s_zmap_blocks

s_firstdatazone

s_imap_blocks

s_zmap_blocks

s_log_zone_size

s_max_size

00000800~00000BFF 1KB

05BA 2F30 0003 0008 0293 0000

1C00 1008 137F 0000 0000

05BA: inode节点数 1466

2F30 : 逻辑块数 12080

0003: i节点位图占数据块数

0008: 逻辑块位图占数据块数

0293: 第一个数据逻辑块号 659

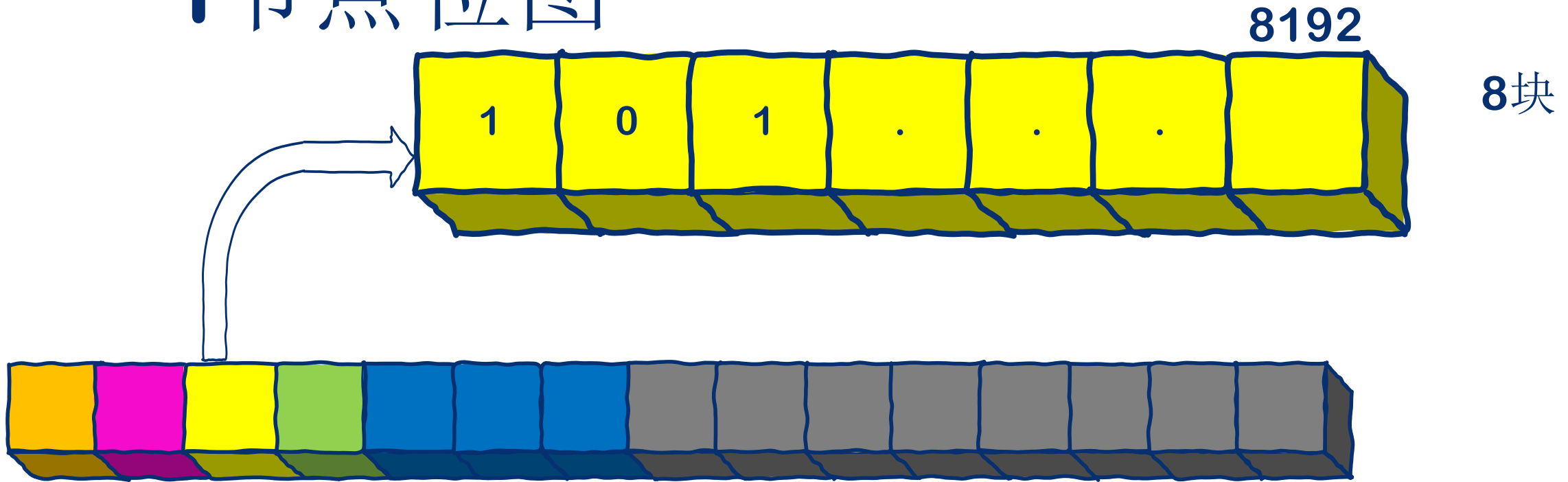
0000: $\log(\text{数据块数}/\text{逻辑块})$

1C00 1008: 文件最大长度

137f : magic number

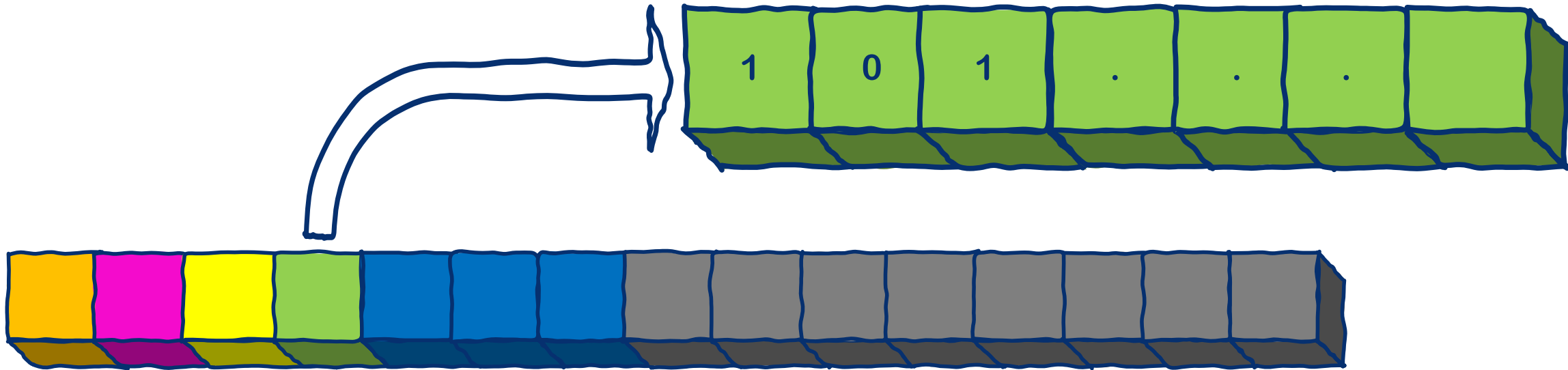
00000C00~000017FF 3KB

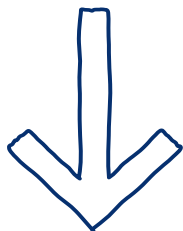
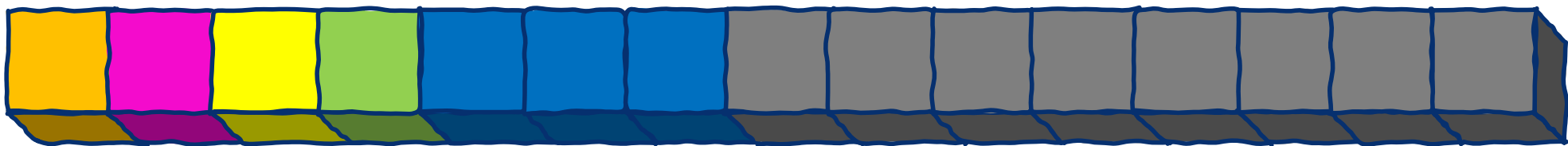
i节点位图



逻辑块位图

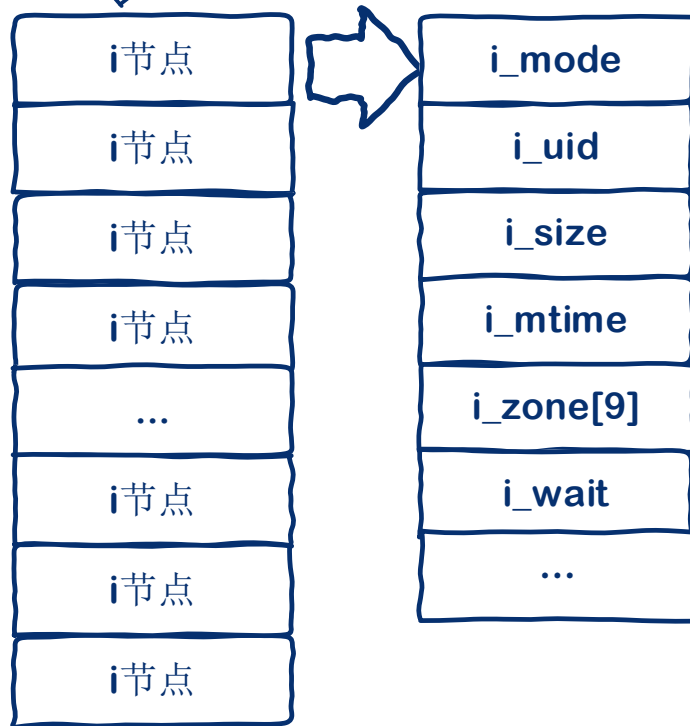
00001800~000037FF 8KB

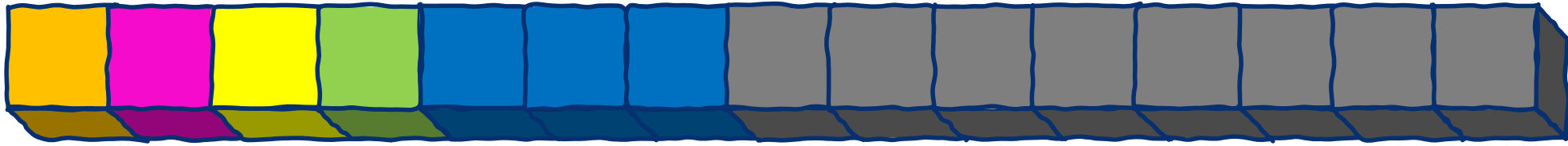




00038000~000A4FFF

645kb

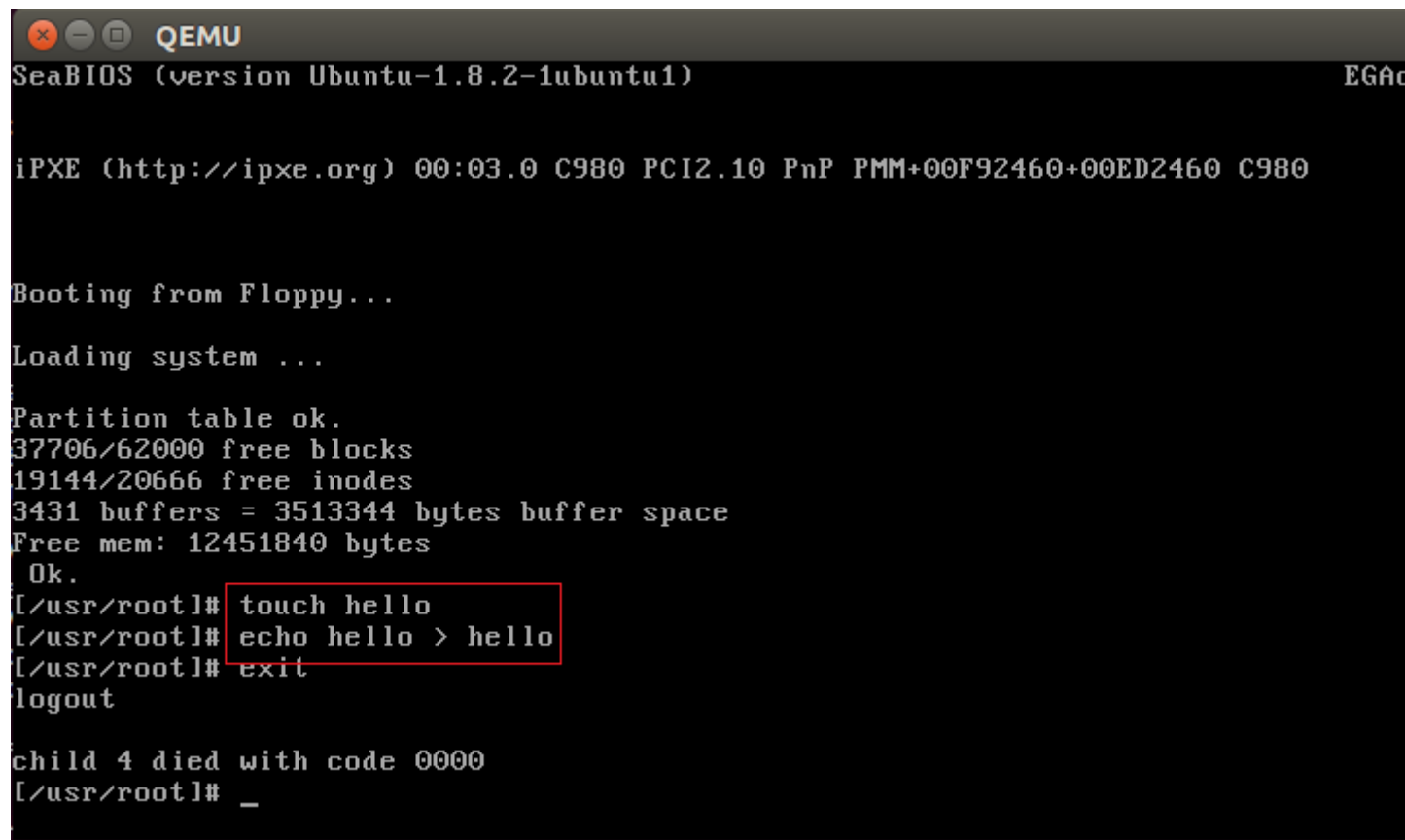




000A5000~03C903FF

61357kb 59MB+941KB

文件系统-动态展示



```
QEMU
SeaBIOS (version Ubuntu-1.8.2-1ubuntu1)

iPXE (http://ipxe.org) 00:03.0 C980 PCI2.10 PnP PMM+00F92460+00ED2460 C980

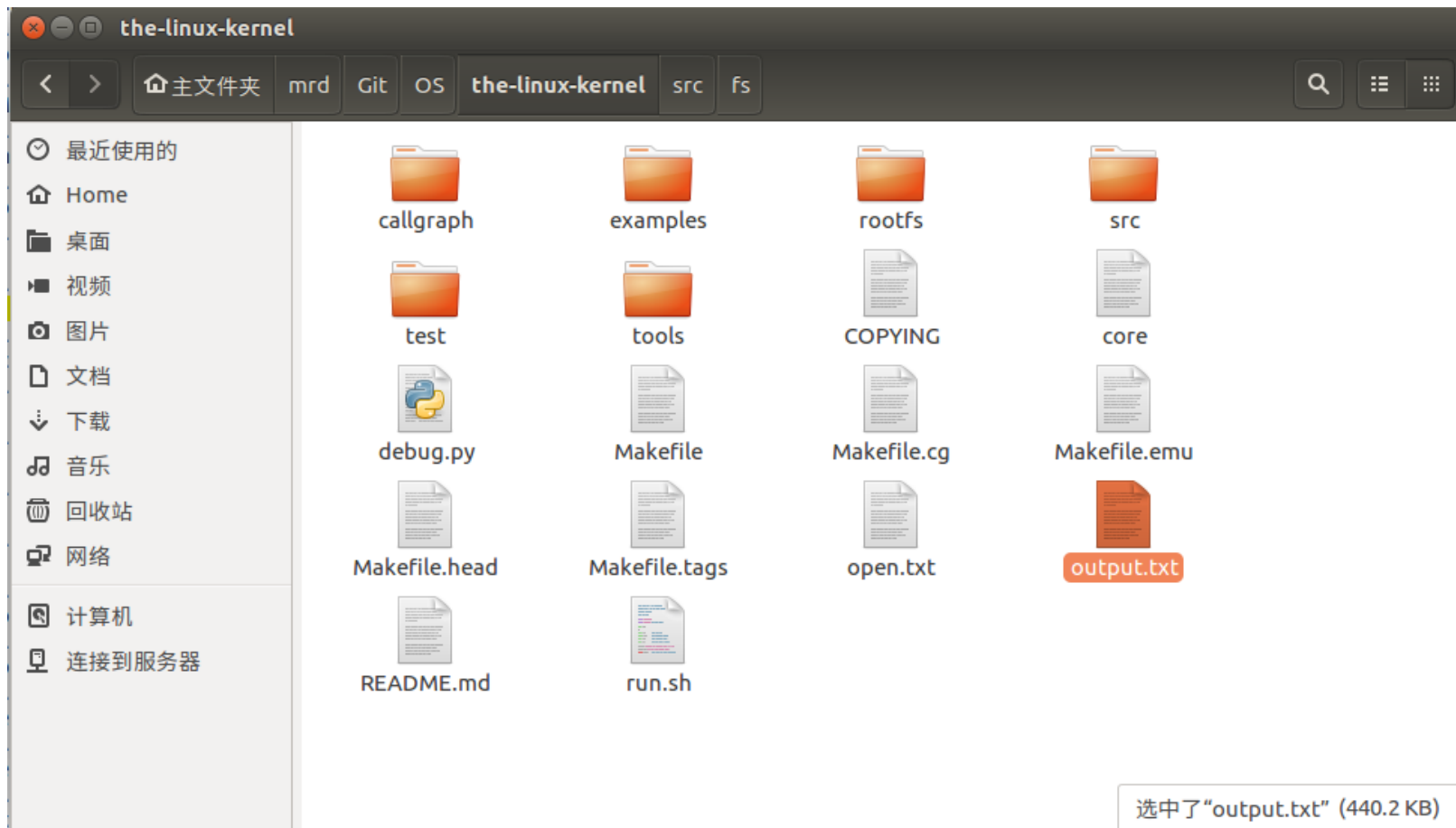
Booting from Floppy...

Loading system ...

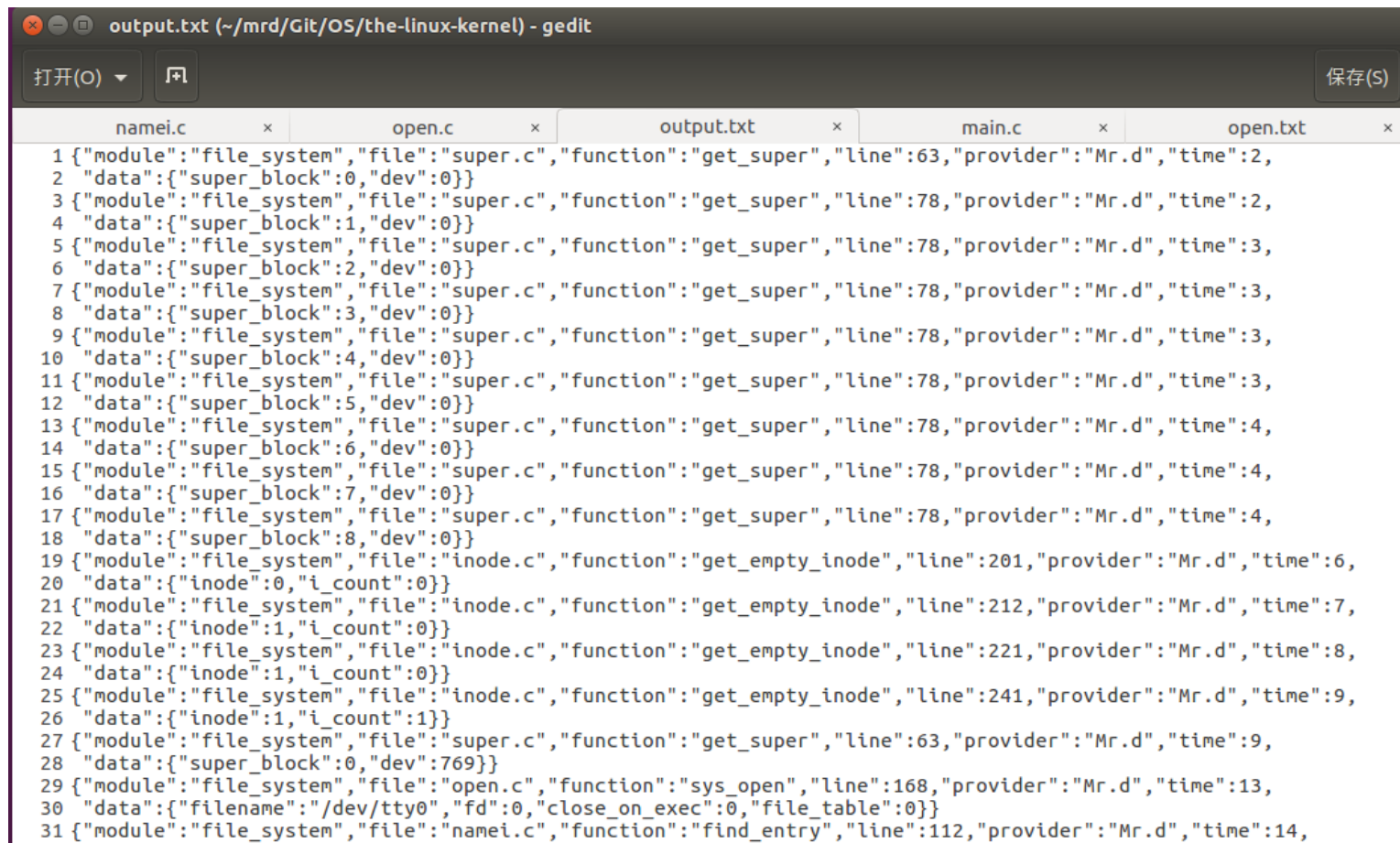
Partition table ok.
37706/62000 free blocks
19144/20666 free inodes
3431 buffers = 3513344 bytes buffer space
Free mem: 12451840 bytes
Ok.
[/usr/root]# touch hello
[/usr/root]# echo hello > hello
[/usr/root]# exit
logout

child 4 died with code 0000
[/usr/root]# _
```

文件系统-动态展示



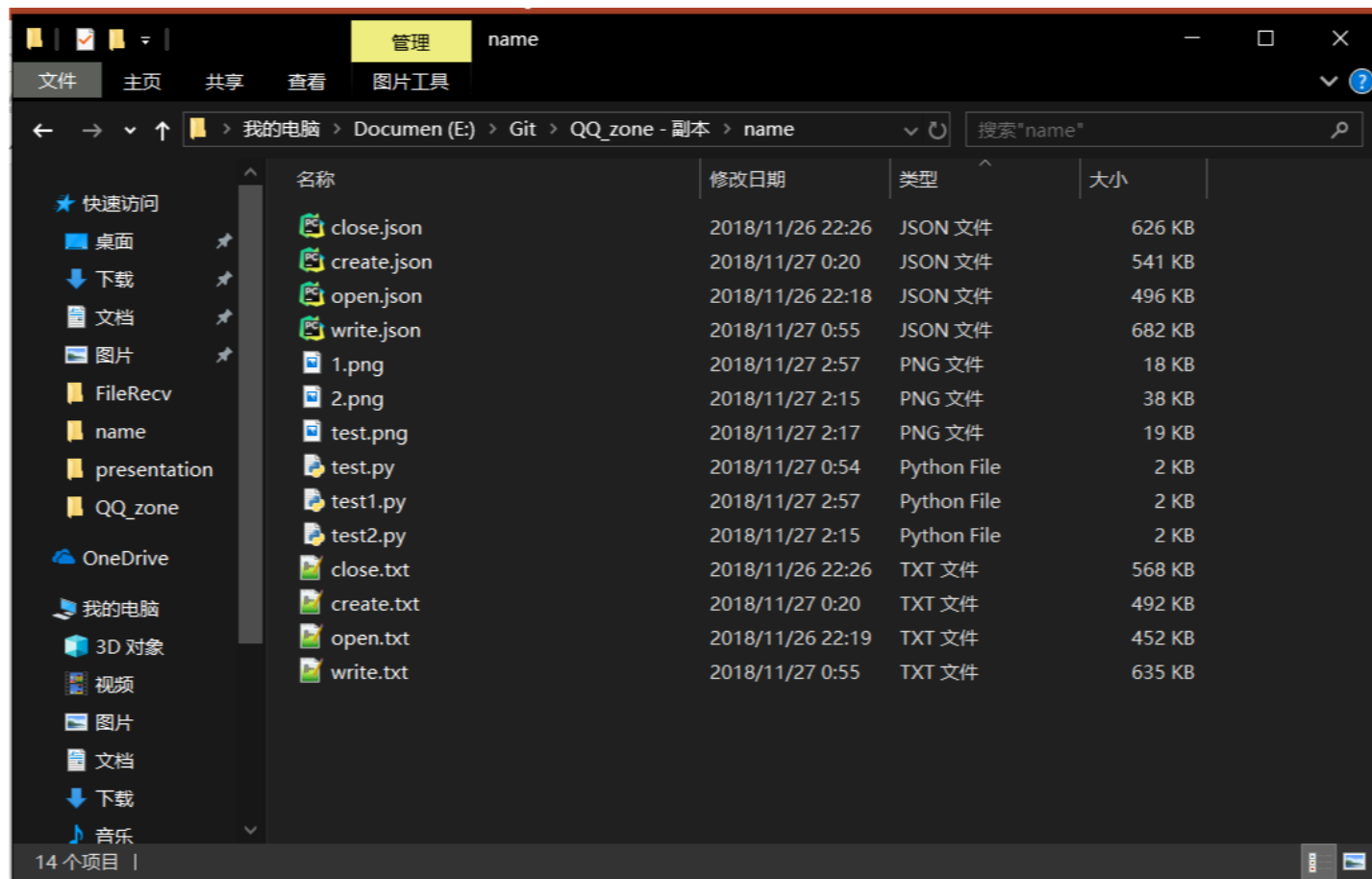
动态展示-数据格式



The screenshot shows a gedit editor window titled "output.txt (~/.mrd/Git/OS/the-linux-kernel) - gedit". The window has a menu bar with "打开(O)" and "保存(S)" buttons. Below the menu bar is a tab bar with five tabs: "namei.c", "open.c", "output.txt", "main.c", and "open.txt". The "output.txt" tab is active, displaying a JSON log of kernel events. The log consists of 31 entries, each representing a kernel event. Each entry is a JSON object with the following fields: "module", "file", "function", "line", "provider", and "time". The log shows events from the "file_system" module, the "super.c" file, the "get_super" function, and the "inode.c" file, the "get_empty_inode" function. The log also shows events from the "open.c" file, the "sys_open" function, and the "namei.c" file, the "find_entry" function. The log is as follows:

```
1 {"module":"file_system","file":"super.c","function":"get_super","line":63,"provider":"Mr.d","time":2,
2  "data":{"super_block":0,"dev":0}}
3 {"module":"file_system","file":"super.c","function":"get_super","line":78,"provider":"Mr.d","time":2,
4  "data":{"super_block":1,"dev":0}}
5 {"module":"file_system","file":"super.c","function":"get_super","line":78,"provider":"Mr.d","time":3,
6  "data":{"super_block":2,"dev":0}}
7 {"module":"file_system","file":"super.c","function":"get_super","line":78,"provider":"Mr.d","time":3,
8  "data":{"super_block":3,"dev":0}}
9 {"module":"file_system","file":"super.c","function":"get_super","line":78,"provider":"Mr.d","time":3,
10 "data":{"super_block":4,"dev":0}}
11 {"module":"file_system","file":"super.c","function":"get_super","line":78,"provider":"Mr.d","time":3,
12 "data":{"super_block":5,"dev":0}}
13 {"module":"file_system","file":"super.c","function":"get_super","line":78,"provider":"Mr.d","time":4,
14 "data":{"super_block":6,"dev":0}}
15 {"module":"file_system","file":"super.c","function":"get_super","line":78,"provider":"Mr.d","time":4,
16 "data":{"super_block":7,"dev":0}}
17 {"module":"file_system","file":"super.c","function":"get_super","line":78,"provider":"Mr.d","time":4,
18 "data":{"super_block":8,"dev":0}}
19 {"module":"file_system","file":"inode.c","function":"get_empty_inode","line":201,"provider":"Mr.d","time":6,
20 "data":{"inode":0,"i_count":0}}
21 {"module":"file_system","file":"inode.c","function":"get_empty_inode","line":212,"provider":"Mr.d","time":7,
22 "data":{"inode":1,"i_count":0}}
23 {"module":"file_system","file":"inode.c","function":"get_empty_inode","line":221,"provider":"Mr.d","time":8,
24 "data":{"inode":1,"i_count":0}}
25 {"module":"file_system","file":"inode.c","function":"get_empty_inode","line":241,"provider":"Mr.d","time":9,
26 "data":{"inode":1,"i_count":1}}
27 {"module":"file_system","file":"super.c","function":"get_super","line":63,"provider":"Mr.d","time":9,
28 "data":{"super_block":0,"dev":769}}
29 {"module":"file_system","file":"open.c","function":"sys_open","line":168,"provider":"Mr.d","time":13,
30 "data":{"filename":"/dev/tty0","fd":0,"close_on_exec":0,"file_table":0}}
31 {"module":"file_system","file":"namei.c","function":"find_entry","line":112,"provider":"Mr.d","time":14,
```

动态展示-数据格式



动态展示-数据格式

JSON原始数据头

保存复制全部折叠

▼ 0:

module:

"file_system"

file:

"super.c"

function:

"get_super"

line:

63

provider:

"Mr.d"

time:

2

▼ data:

super_block:

0

dev:

0

▼ 1:

module:

"file_system"

file:

"super.c"

创建文件



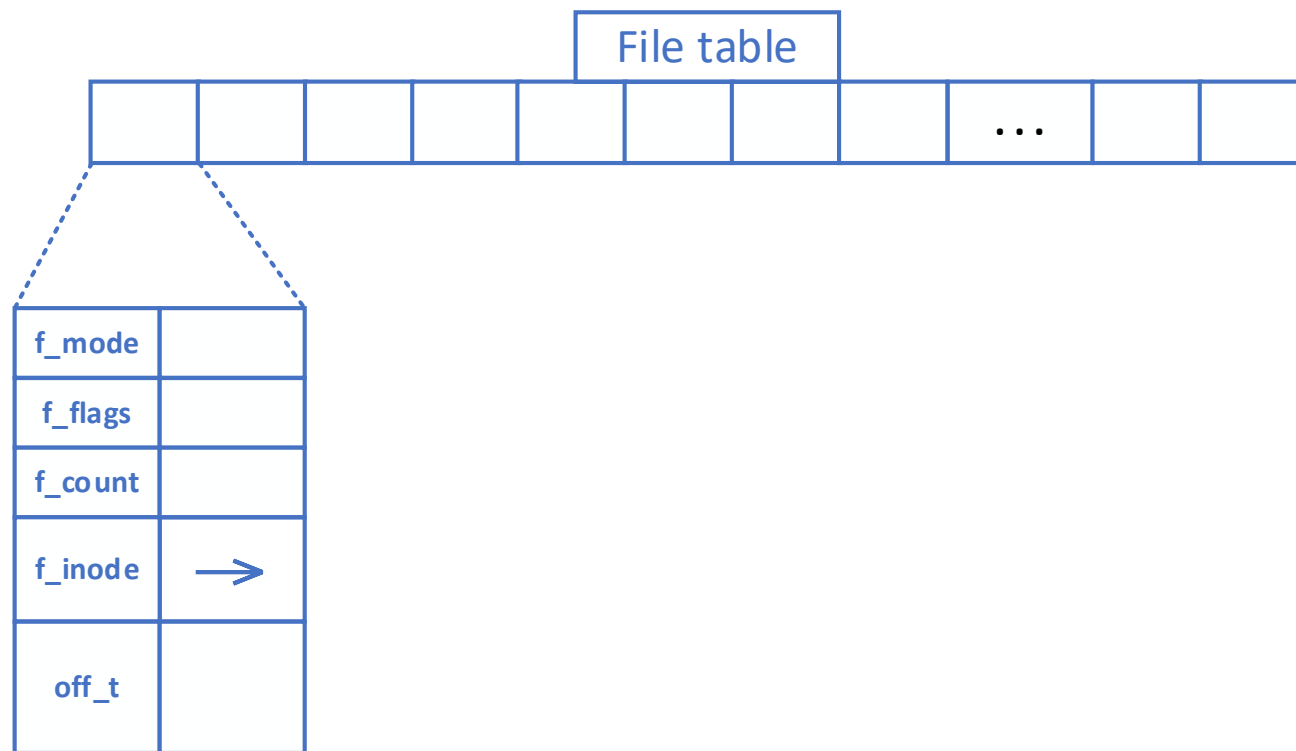
filp

0	→
1	→
2	→
3	→
	⋮
19	→

动态展示-filp

```
▼ 1802:
  module:      "file_system"
  file:        "open.c"
  function:    "sys_open"
  line:        157
  provider:    "Mr.d"
  time:        679
  ▼ data:
    filp[0]:    161584
▶ 1803:        {...}
▶ 1804:        {...}
▼ 1805:
  module:      "file_system"
  file:        "open.c"
  function:    "sys_open"
  line:        157
  provider:    "Mr.d"
  time:        680
  ▼ data:
    filp[3]:    0
```

创建文件



动态展示-file_table

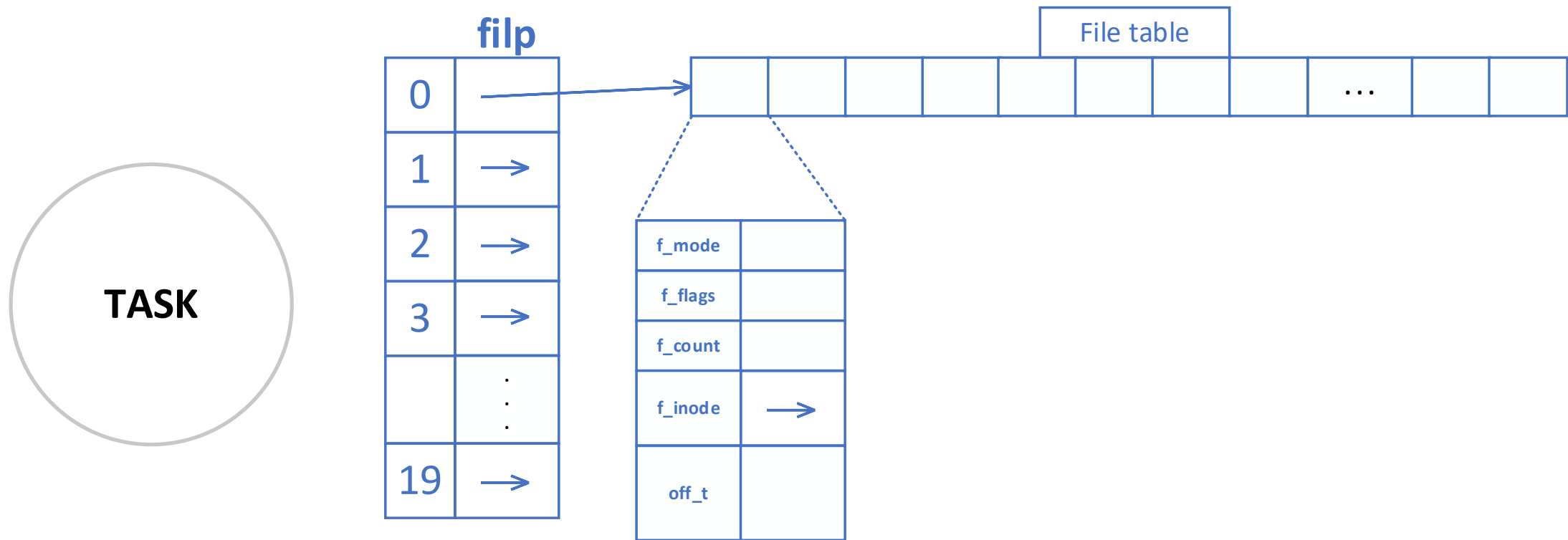
```
▼ 1806:
  module:      "file_system"
  file:        "open.c"
  function:    "sys_open"
  line:        169
  provider:    "Mr.d"
  time:        680
  ▼ data:
    file_table[0]: 3
▼ 1807:
  module:      "file_system"
  file:        "open.c"
  function:    "sys_open"
  line:        169
  provider:    "Mr.d"
  time:        680
  ▼ data:
    file_table[1]: 6
```

创建文件



close_on_exec

创建文件



动态展示-open

▼ 1808:	
module:	"file_system"
file:	"open.c"
function:	"sys_open"
line:	174
provider:	"Mr.d"
time:	680
▼ data:	
filename:	"hello"
fd:	3
close_on_exec:	0
file_table:	2

创建文件



动态展示-pwd

▼ 1810:

module: "file_system"

file: "namei.c"

function: "get_dir"

line: 309

provider: "Mr.d"

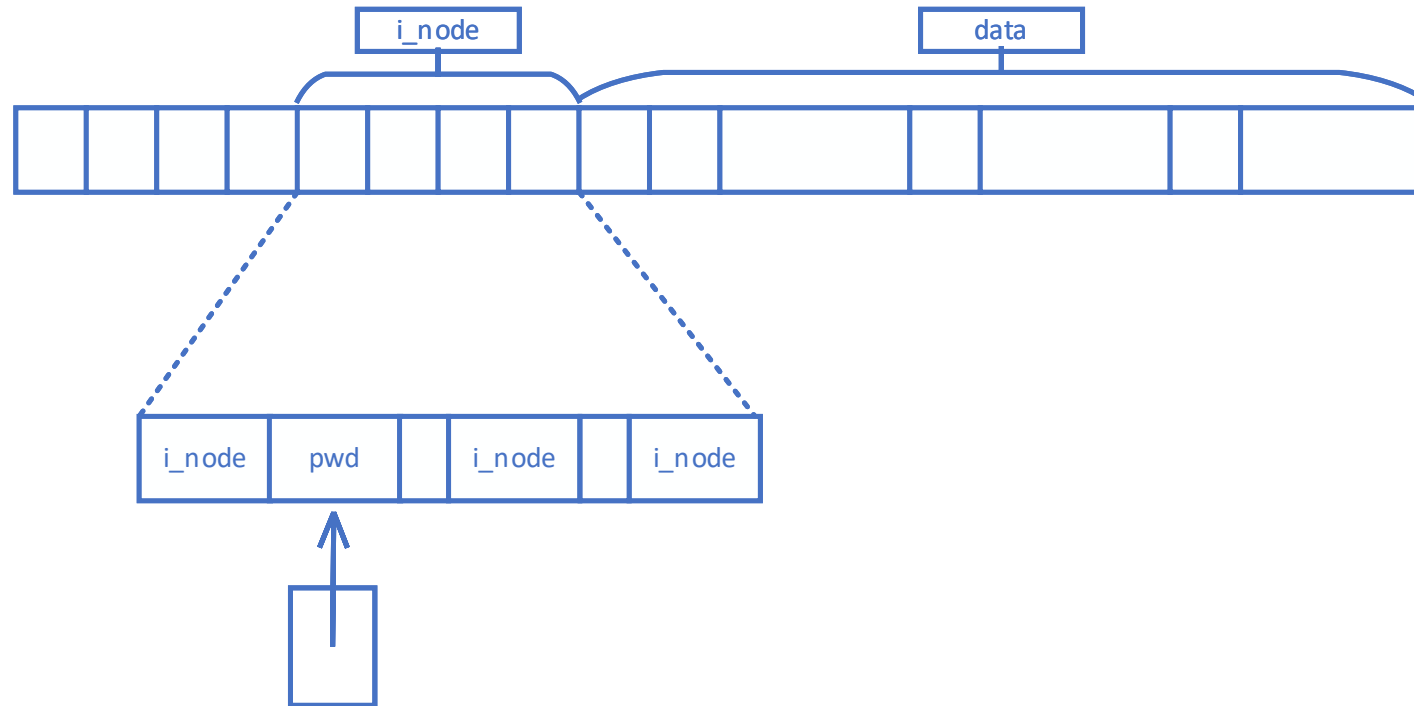
time: 680

▼ data:

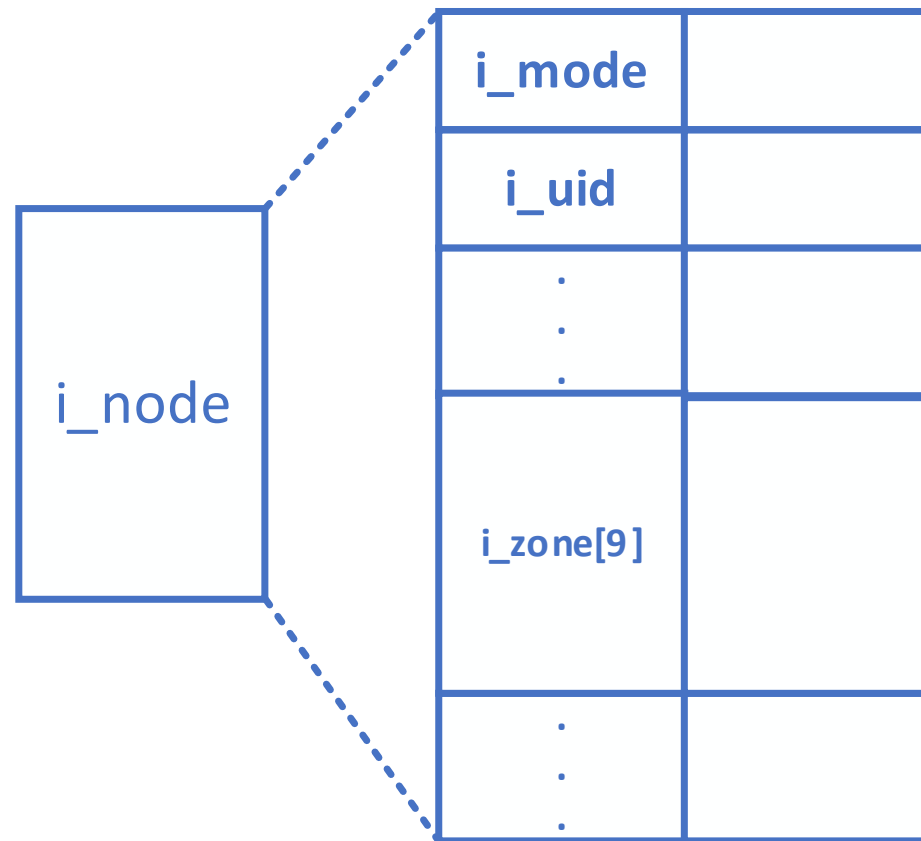
pwd: "256b8"

i_count: 2

创建文件



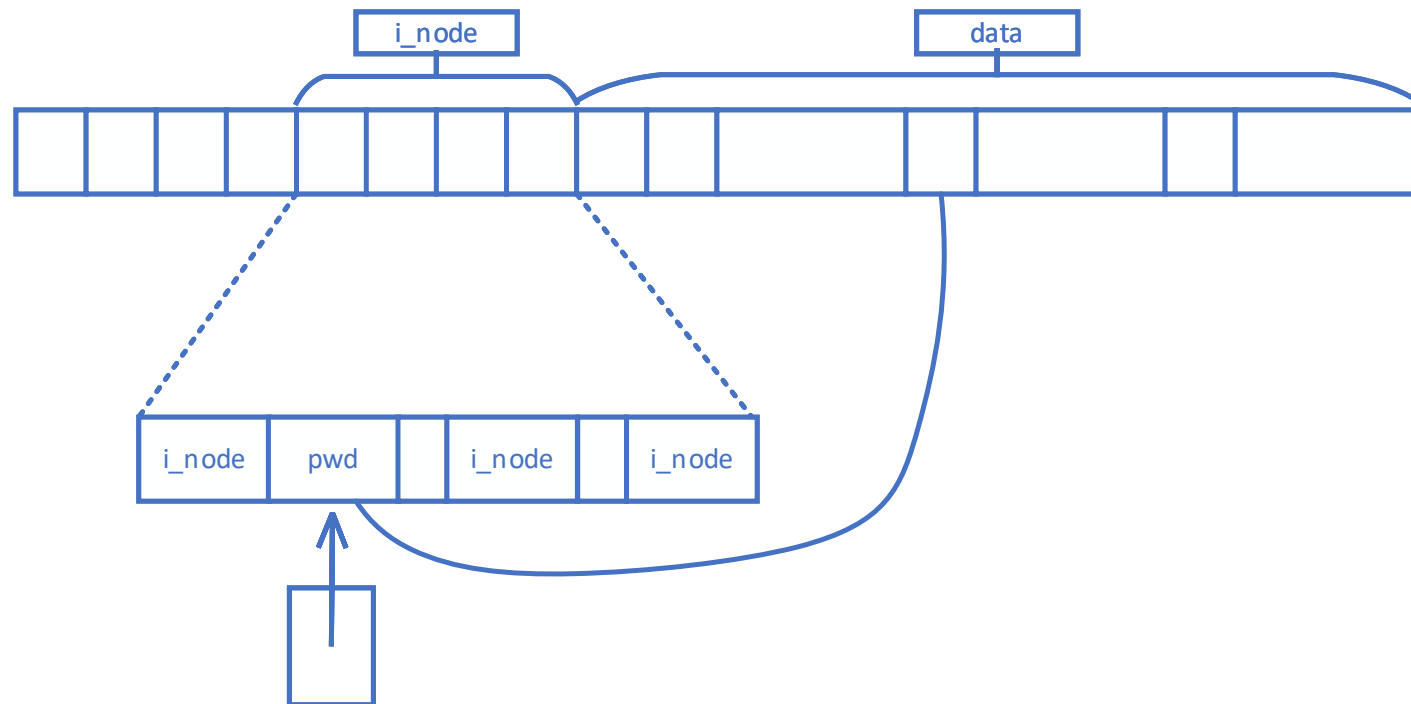
创建文件



动态展示-entries

▼ 1811:	
module:	"file_system"
file:	"namei.c"
function:	"find_entry"
line:	112
provider:	"Mr.d"
time:	705
▼ data:	
m_inode:	"256b8"
i_size:	304
entries:	19

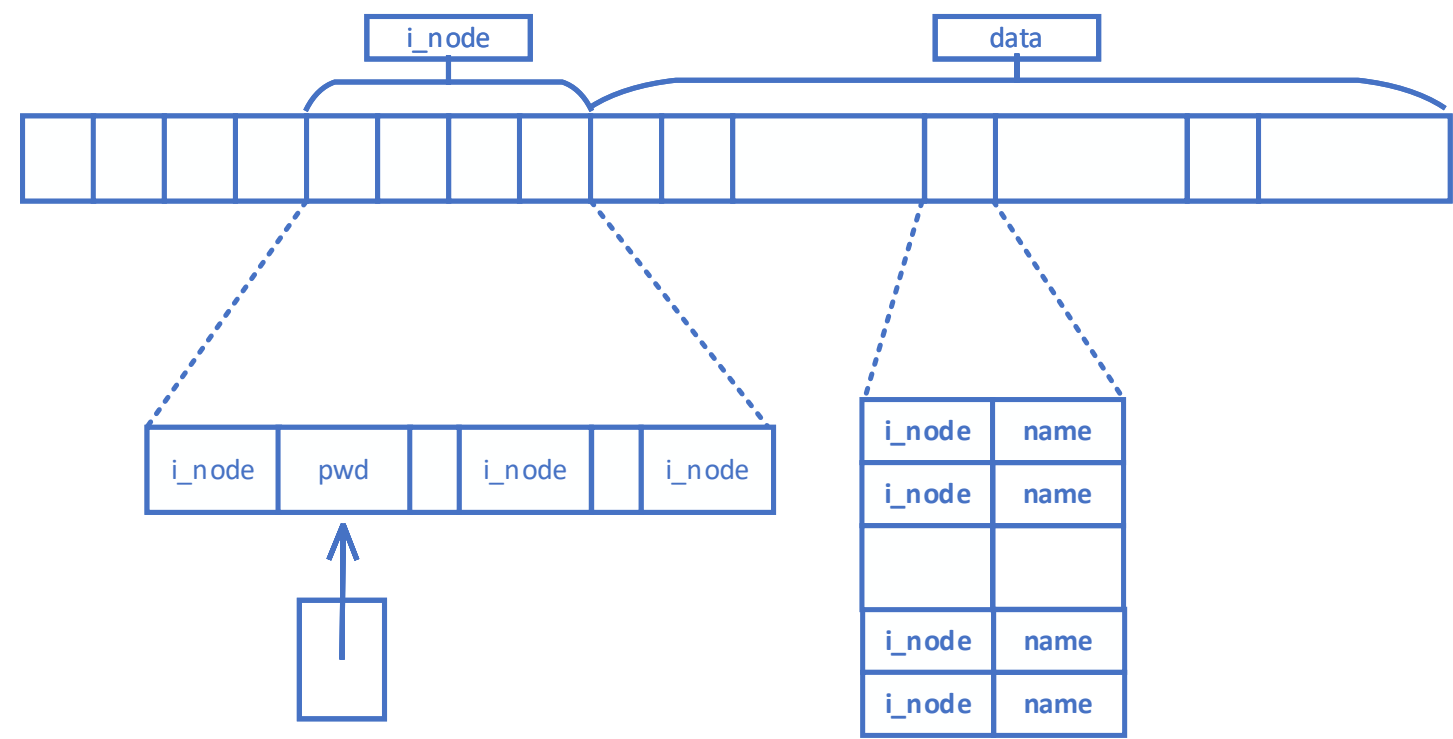
创建文件



动态展示-i_zone

▼ 1812:	
module:	"file_system"
file:	"namei.c"
function:	"find_entry"
line:	135
provider:	"Mr.d"
time:	680
▼ data:	
m_inode:	"256b8"
i_zone[0]:	"36dd"

创建文件



动态展示-entry

▼ 1813:

```
module:      "file_system"  
file:        "namei.c"  
function:    "find_entry"  
line:        164  
provider:    "Mr.d"  
time:        705  
▼ data:  
  dir_entry[0]:  "."
```

动态展示-entry

▼ 1831:	
module:	"file_system"
file:	"namei.c"
function:	"find_entry"
line:	164
provider:	"Mr.d"
time:	707
▼ data:	
dir_entry[18]:	"part14"

动态展示-inode_table

▼ 1834:	
module:	"file_system"
file:	"inode.c"
function:	"get_empty_inode"
line:	221
provider:	"Mr.d"
time:	708
▼ data:	
inode:	15
i_count:	0

动态展示-super_block

▼ 1836:	
module:	"file_system"
file:	"super.c"
function:	"get_super"
line:	63
provider:	"Mr.d"
time:	708
▼ data:	
super_block:	0
dev:	769

动态展示-empty_inode

▼ 1837:	
module:	"file_system"
file:	"bitmap.c"
function:	"new_inode"
line:	151
provider:	"Mr.d"
time:	708
▼ data:	
sb->s_imap[0]:	163828
▼ 1838:	
module:	"file_system"
file:	"bitmap.c"
function:	"new_inode"
line:	159
provider:	"Mr.d"
time:	708
▼ data:	
first_zero:	2

动态展示-new_inode

▼ 1839:	
module:	"file_system"
file:	"bitmap.c"
function:	"new_inode"
line:	172
provider:	"Mr.d"
time:	708
▼ data:	
i_count:	1
i_nlinks:	1
i_dev:	769
i_uid:	0
i_gid:	0
i_dirt:	1
i_num:	2
i_time:	1543249203

动态展示-add_entry

▼ 1840:	
module:	"file_system"
file:	"namei.c"
function:	"add_entry"
line:	242
provider:	"Mr.d"
time:	708
▼ data:	
Empty entry:	14
de->name:	"hello"
▼ 1841:	
module:	"file_system"
file:	"namei.c"
function:	"open_namei"
line:	499
provider:	"Mr.d"
time:	708
▼ data:	
de->inode:	2

动态展示-finish!

```
▼ 1842:  
  module: "file_system"  
  file: "open.c"  
  function: "sys_open"  
  line: 183  
  provider: "Mr.d"  
  time: 709  
  ▼ data:  
    filename: "hello"  
    Event: "Open finished"
```


写入文件

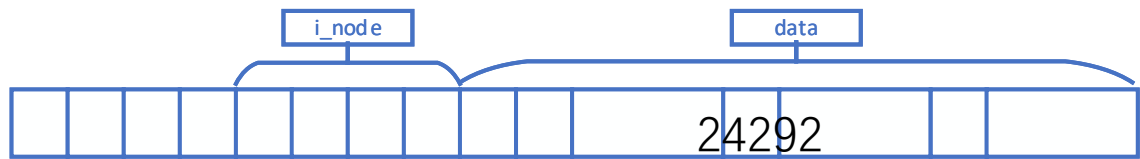
TASK

filp

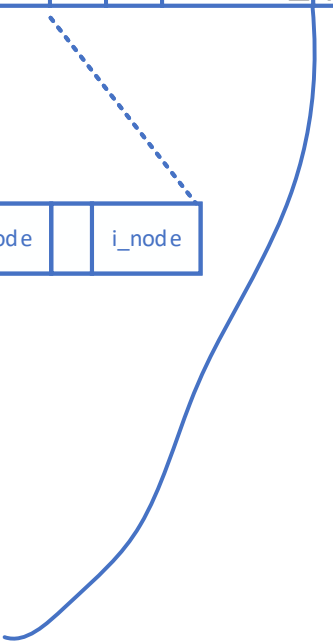
0	→
1	→
2	→
3	→
	⋮
19	→



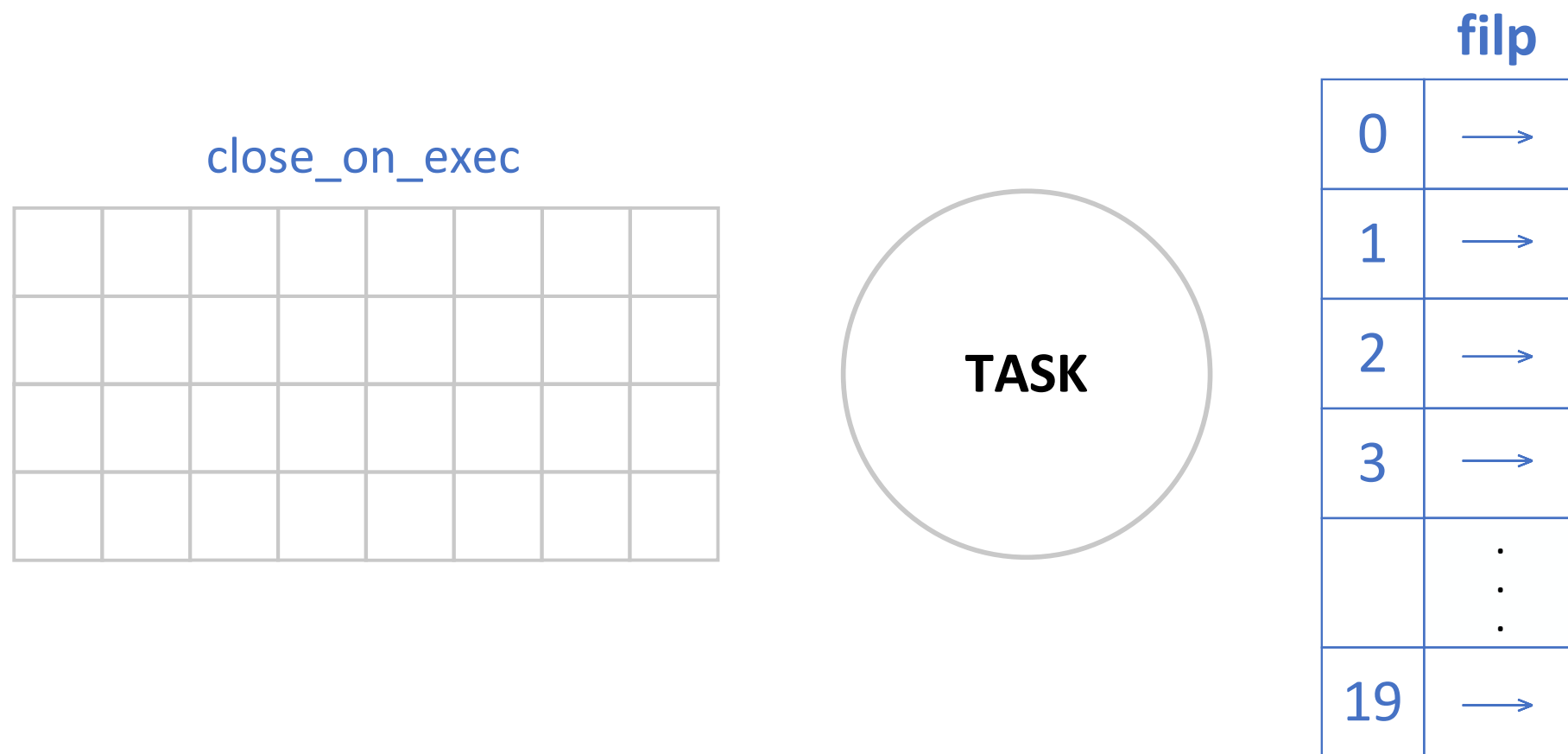
f_mode	
f_flags	577
f_count	
f_inode	→
off_t	
f_pos	0



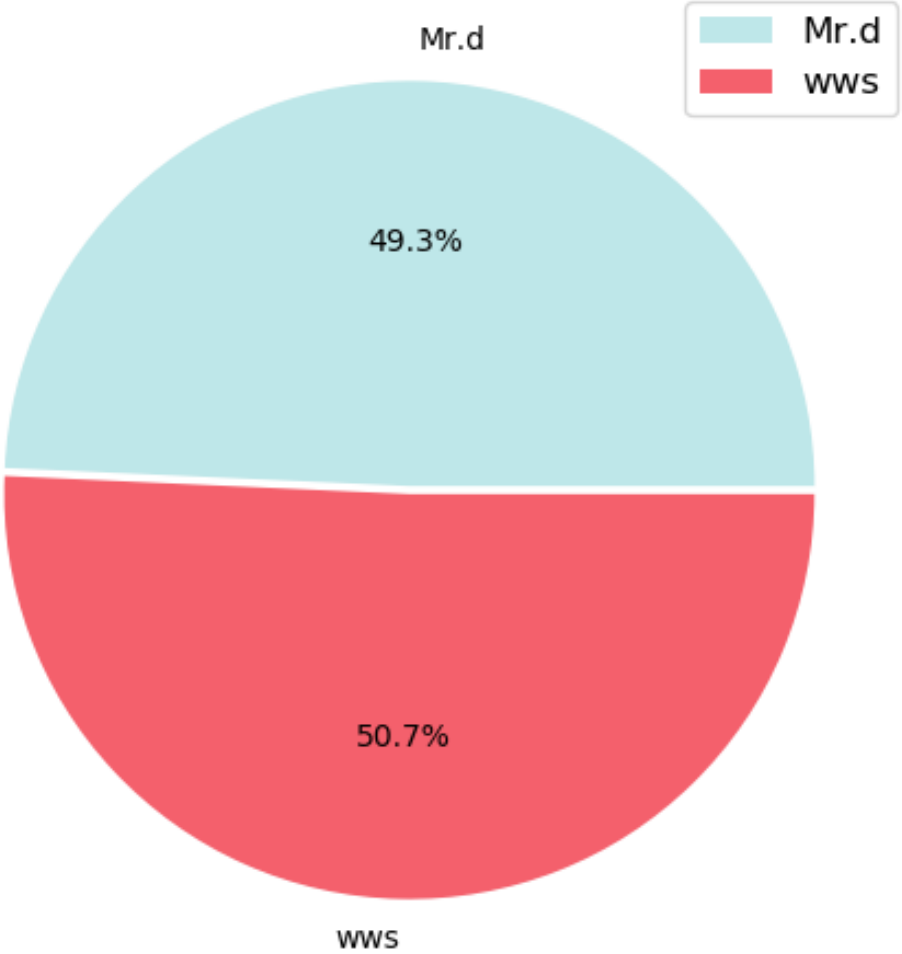
i_mode	100600
i_pipe	0
i_dev	769
i_zone[9]	
ic_time	1543243302
i_dirt	1



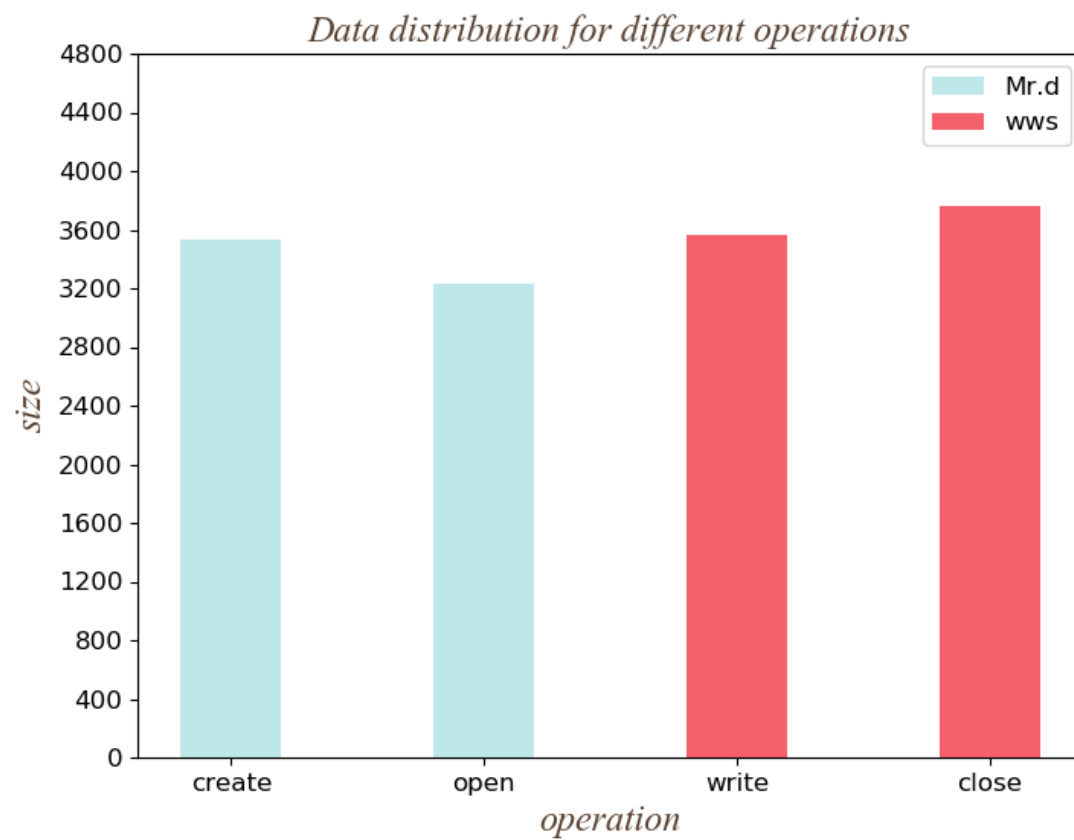
关闭文件



统计数据



统计数据



Thank you

