Repository Link: <https://github.com/SamanEN/Operating-System-Lab-Projects>

Latest Commit Hash: <hash>

# آشنایی با سیستم‌عامل xv6

## معماری سیستم‌عامل xv6

سیستم عامل xv6 مشابه Unix v6 نوشته شده و معماری و ساختاری شبیه به آن دارد. این سیستم عامل برای پردازنده‌های مبتنی بر x86 نوشته شده (مطابق با داکیومنت این سیستم عامل؛ xv6-rev11). علاوه بر آن در دفاع از این سخن می‌توان به فایل x86.h اشاره کرد که از دستورات پردازنده‌های x86 استفاده شده است. در دیگر فایل‌های “basic headers”، نظیر asm.h و mmu.h نیز می‌توان اشاراتی به معماری x86 مشاهده کرد.

معماری کلی سیستم عامل Unix بصورت زیر می‌باشد:



همانطور که گفته شد، معماری xv6 نیز از Unix پیروی می‌کند. این موضوع از دسته‌بندی فایل‌ها که شامل file systems، system calls، user-level و... می‌شود نیز قابل مشاهده است.

## بخش های پردازه و چگونگی اختصاص پردازنده به پردازه های مختلف

یک پردازه در xv6 از حافظۀ فضای کاربری (user-space) (شامل دستورات، داده‌ها و استک)، و وضعیت پردازه که فقط برای هسته قابل رؤیت است تشکیل شده است.

xv6 زمان را بین پردازه‌ها تقسیم می‌کند و به صورت نامحسوس پردازنده‌ها را برای اجرای دستورات به پردازه‌ها اختصاص می‌دهد. هروقت یک پردازه قرار است از اجرا توسط پردازنده خارج شود، سیستم‌عامل register های CPU که حاوی مقادیر مورد نیاز آن پردازه بوده را ذخیره می‌کند تا دفعه بعدی که آن پردازه قرار است اجرا شود، آنها را بازگرداند.

هسته xv6 به هر پردازه یک شناسه یکتا PID (Process Identifier) اختصاص می‌دهد. با استفاده از system call ء getpid() می‌توان PID پردازۀ کنونی را دریافت کرد.

## مفهوم file descriptor و عملکرد pipe در xv6

## توابع exec و fork

تابع fork برای ایجاد یک process جدید استفاده می‌شود. در واقع این تابع یک نسخه کپی از پردازه‌ای می‌سازد که این تابع را صدا زده است. منظور از کپی این است که دیتا و دستورات پردازه فعلی در حافظه پردازه جدید (child) کپی می‌شوند. با وجود اینکه در لحظه ایجاد پردازه فرزند، داده‌های آن (متغیرها و رجیسترها) با پردازه پدر یکسان هستند، اما در واقع این دو پردازه حافظه جداگانه‌ای خواهند داشت و تغییر یک متغیر در پردازه پدر، آن متغیر در پردازه فرزند را تغییر نمی‌دهد. پردازه پدر پس از ایجاد پردازه فرزند، به caller تابع fork بازمی‌گردد که امکان اجرای همزمان دو پردازه را فراهم می‌سازد. مقدار return شده از تابع fork نیز pid پردازه فرزند خواهد بود. نقطه شروع پردازه فرزند نیز دقیقا همان caller تابع fork است با این تفاوت که مقدار خروجی این تابع عدد 0 خواهد بود. پس اگر با استفاده از کد pid = fork(); یک پردازه جدید درست کنیم، یکی از حالت‌های زیر برای مقدار pid رخ می‌دهد:

* pid = 0: در پردازه فرزند هستیم.
* pid > 0: در پردازه پدر هستیم و مقدار pid در واقع آی‌دی پردازه فرزند است.
* pid < 0: در زمان اجرای تابع fork و پردازه جدید اروری وجود داشته و پردازه فرزند ایجاد نشده است.

اگر پس از fork کردن از تابع wait(int\*) استفاده شود، پردازه پدر منتظر پایان یافتن پردازه فرزند می‌شود و سپس کار خود را ادامه می‌دهد. خروجی این تابع، pid پردازه پایان یافته است. اگر پردازه فعلی هیچ پردازه فرزندی نداشته باشد، خروجی این تابع -1 خواهد بود. همچنین ورودی این تابع پوینتر به متغیری است که در نهایت status code مروبط به پردازه فرزند در آن قرار می‌گیرد. برای ignore کردن این پارامتر از ((int\*)0) استفاده می‌شود.

قطعه کد زیر مثالی برای استفاده از تابع fork را نشان می‌دهد:

int pid = fork();  
if (pid == 0) {  
 printf("This is child process\n");  
 printf("Child process is exiting\n");  
 exit(0);  
}  
else if (pid > 0) {  
 printf("This is parent process\n");  
 printf("Waiting for child process to exit\n");  
 wait((int \*)0);  
 printf("Child process exited\n");  
}  
else {  
 printf("Fork failed\n");  
}

تابع exec حافظه پردازه فعلی را با یک حافظه جدید که در آن یک برنامه با فایل ELF لود شده است، جایگزین می‌کند. در واقع exec() راهی برای اجرای یک برنامه در پردازه فعلی است. بر خلاف تابع fork()، برنامه به caller تابع exec() باز نمی‌گردد و برنامه جدید اجرا می‌شود مگر اینکه در زمان اجرای این تابع یک ارور رخ دهد. برنامه جدید اجرا شده در یک نقطه‌ای با استفاده از تابع exit اجرای پردازه را خاتمه می‌دهد. تابع exec دو پارامتر ورودی دارد که پارامتر اول نام فایل برنامه و پارامتر دوم آرایه آرگومان‌های ورودی برنامه است.

قطعه کد زیر مثالی از اجرای این تابع را نشان می‌دهد:

char\* args[] = {“ls”, “-l”, “/home”, NULL}; *// Null is required*  
exec(“/bin/ls”, args);  
printf(“Exec failed\n”);

مزیت ادغام نکردن این دو تابع در زمان I/O redirection خودش را نشان می‌دهد. زمانی که کاربر در shell یک برنامه را اجرا می‌کند، کاری که در پشت صحنه توسط shell انجام می‌شود به شرح زیر است:

1. ابتدا دستور تایپ شده توسط کاربر در ترمینال را می‌خواند.
2. با استفاده از تابع fork یک پردازه جدید ایجاد می‌کند.
3. در پردازه فرزند با استفاده از تابع exec برنامه درخواست شده توسط کاربر را جایگزین پردازه فعلی (فرزند) می‌کند.
4. در پردازه پدر برای اتمام کار پردازه فرزندwait می‌کند.
5. پس از اتمام پردازه فرزند به main باز می‌گردد و منتظر دستور جدید می‌شود.

زمانی که کاربر برای یک دستور از redirection استفاده می‌کند، تغییرات لازم در file descriptorها پس از fork و پیش از exec و در پردازه فرزند انجام می‌شود.

قطعه کد زیر این مورد را به شکل ساده شده نشان می‌دهد (فرض کنید دستور اجرا شده cat < in.txt است):

char\* args = {“cat”, NULL};  
int pid = fork();  
if (pid == 0) {  
 close(0); *// close stdin*  
 open(“in.txt”, O\_RDONLY); *// open in.txt for reading (fd: 0)*  
 exec(“/bin/cat”, args):  
 printf(“Exec failed\n”)  
}  
else if (pid > 0) {  
 wait((int \*)0);  
 printf(“Child process has exited\n”);  
}  
else {  
 printf(“The fork failed\n”)

}

در صورتی که این دو تابع ادغام شوند، یا باید حالت‌های redirection به عنوان پارامتر به تابع forkexec پاس داده شوند که هندل کردن این حالت دردسرهای خودش را دارد و یا اینکه shell پیش از اجرای این تابع،  
file descriptorهای خود را تغییر دهد و بعد از اتمام کار این تابع نیز به حالت قبل برگرداند و یا در بدترین حالت، هندل کردن redirection را در هر برنامه مانند cat پیاده‌سازی کنیم.

# اضافه کردن یک متن به Boot Message



پس از بوت شدن سیستم‌عامل نام اعضای گروه نمایش داده شده است.

این کار با افزودن یک printf در فایل init.c انجام شده است.

# اضافه کردن چند قابلیت به کنسول xv6

## دستور ctrl + n برای پاک کردن همه اعداد خط کنونی

برای اضافه کردن این قابلیت تابع زیر به فایل console.c اضافه شده است و در switch case تابع consoleintr به ازای حالت C(‘N’)، این تابع صدا زده می‌شود:

static void  
remnums()  
{  
 char cmd[INPUT\_BUF];  
 int j = 0;  
 for(int i = 0; i < input.e - input.w; ++i){  
 int idx = (input.w + i) % INPUT\_BUF;  
 if(input.buf[idx] >= '0' && input.buf[idx] <= '9'){  
 continue;  
 }  
 cmd[j++] = input.buf[idx];  
 }  
 cmd[j] = '\0';  
 consclear();  
 consputs(cmd);  
}

## دستور ctrl + r برای برعکس کردن خط کنونی

همانند قابلیت قبلی، با صدا کردن تابع زیر در switch case تابع consoleintr به ازای حالت C(‘R’)، می‌توان این قابلیت را به ترمینال اضافه کرد:

static void  
revline()  
{  
 char cmd[INPUT\_BUF];  
 memmove(cmd, input.buf + input.w, input.e - input.w);  
 cmd[input.e - input.w] = '\0';  
 revstr(cmd, input.e - input.w);  
 consclear();  
 consputs(cmd);  
}

## دستور tab برای تکمیل کردن خط کنونی

استراکت زیر به منظور ذخیره تاریخچه دستورات استفاده می‌شود:

#define HIST\_SIZE 15  
struct {  
  uint queue\_idx;  
  char cmd\_buf[HIST\_SIZE][INPUT\_BUF];  
  uint last\_used\_idx;  
  
  int is\_suggestion\_used;  
  char original\_cmd[INPUT\_BUF];  
  uint original\_cmd\_size;  
} hist;

متغییر queue\_idx نشان‌دهنده شماره خانه فعلی صف تاریخچه دستورات است. cmd\_buf نیز آرایه نگه‌دارنده دستورات گذشته است. علاوه بر آن از یک شماره خانه به نام last\_used\_idx برای نگه داشتن آخرین پیشنهاد فعلی استفاده می‌کنیم تا هنگام پیشنهاد دادن دستورات مختلف، همواره دستوری جدید از تاریخچه به کاربر ارائه شود. سه متغییر بعدی برای نگه داشتن دستور اصلی است که کاربر قبل از دریافت پیشنهادات وارد کرده بود؛ استفاده از این متغییر ها به این دلیل است که پیشنهادات همواره بر مبنای دستور وارد شده باشند و پس از تغییر دستور توسط پیشنهادات، پیشنهادات عوض نشوند.

دو تابع get\_suggestion و suggest\_cmd نیز به فایل console.c اضافه شده‌اند که به ترتیب وظایف پیشنهاد مناسب برای دستور فعلی و قرار دادن پیشنهاد دریافت شده در کنسول را بر عهده دارند. علاوه بر آن تابع push\_current\_hist نیز برای اضافه کردن دستور وارد شده توسط کاربر به تاریخچه دستورات نوشته شده است. این توابع به صورت زیر می‌باشند:

static int  
get\_suggestion(const char\* cmd, uint cmd\_size)  
{  
  for(int i = 0; i < HIST\_SIZE; ++i){  
    int idx = (i + hist.last\_used\_idx) % HIST\_SIZE;  
    if(strncmp(cmd, hist.cmd\_buf[idx], cmd\_size) == 0){  
      return idx;  
    }  
  }  
  return -1;  
}  
  
static void  
suggest\_cmd()  
{  
  if(!hist.is\_suggestion\_used){  
    hist.original\_cmd\_size = input.e - input.w;  
    memmove(hist.original\_cmd, input.buf + input.w, hist.original\_cmd\_size);  
  }  
  int suggested\_cmd = get\_suggestion(hist.original\_cmd, hist.original\_cmd\_size);  
  if(suggested\_cmd >= 0){  
    hist.is\_suggestion\_used = 1;  
    hist.last\_used\_idx = suggested\_cmd + 1;  
    consclear();  
    consputs(hist.cmd\_buf[suggested\_cmd]);  
  }  
}  
  
static void  
push\_current\_hist()  
{  
  memset(hist.cmd\_buf[hist.queue\_idx], 0, INPUT\_BUF);  
  memmove(hist.cmd\_buf[hist.queue\_idx],  
          input.buf + input.w,  
          input.e - input.w - 1);  
  hist.queue\_idx = (hist.queue\_idx + 1) % HIST\_SIZE;  
  hist.is\_suggestion\_used = 0;  
  hist.last\_used\_idx = 0;  
  memset(hist.original\_cmd, 0, INPUT\_BUF);  
}

در نهایت عملکرد پیاده‌سازی شده در این بخش بدین شرح می‌باشد: به ازای هر دستور وارد شده توسط کاربر، آن دستور در تاریخچه دستورات قرار می‌گیرد. این تاریخچه شامل حداکثر 15 دستور آخر می‌باشد. علاوه بر آن دستورات قرار گرفته در این تاریخچه صحت‌سنجی نشده و دستورات نامعتبری نیز ذخیره می‌شوند. هر بار که کاربر کلید tab را فشار دهد، یک پیشنهاد توسط این تاریخچه به کاربر ارئه می‌شود که تکمیل کننده رشته وارد شده است. پیشنهادات از اولین دستورات وارد شده شروع می‌شوند و با هر بار فشردن مجدد tab دستور بعدی پیشنهاد داده می‌شود. در صورت اتمام پیشنهادات و پیمایش تمام دستورات موجود در تاریخچه، پیشنهادات دوباره از اول ارائه خواهند شد و اینکار بصورت دایره‌وار ادامه خواهد یافت.

# اجرا و پیاده‌سازی یک برنامه سطح کاربر



فایل prime\_numbers.c همانند برنامه های دیگر از جمله wc.c و mkdir.c نوشته شده و به متغیر UPROGS در Makefile اضافه شده است.

# مقدمه‌ای درباره سیستم‌عامل و xv6

## سه وظیفه اصلی سیستم‌عامل

## گروه های فایل های اصلی xv6

# کامپایل سیستم‌عامل xv6

## دستور make -n و کدام دستور فایل نهایی را می‌سازد؟

## متغیر های UPROGS و ULIB در Makefile

متغیر UPROGS: این متغیر لیستی از برنامه‌های کاربر را دارد که در هنگام ساخت و کامپایل xv6، این برنامه‌ها نیز کامپایل و تبدیل به فایل‌های قابل اجرا توسط سیستم عامل می‌شوند. نام هر یک از این برنامه‌ها به صورت \_file\_name در این لیست قرار گرفته است. تمام اسامی به صورت \_file\_name (اسامی که یک \_ ابتدایشان دارند)، یک هدف[[1]](#footnote-1) با پیشنیاز[[2]](#footnote-2)های فایل آبجکت هدف (file\_name.o) و متغیر ULIB دارد. بنابراین هدف‌های موجود در UPROGS منجر به ساخت فایل آبجکت برنامه‌های کاربر، اجرا شدن هدف‌های مربوط به ULIB می‌شود و در نهایت اجرای دستور ld می‌شود. دستور ld برای پیوست فایل‌های مورد نیاز و تولید یک فایل قابل اجرا مورد استفاده قرار می‌گیرد. علاوه بر آن فایل‌های آبجکت مربوط به هر برنامه (file\_name.o) توسط یک قانون درونی[[3]](#footnote-3) MakeFile ساخته می‌شوند و به صورت صریح در MakeFile نوشته نشده‌اند.  
متغیر ULIB: این متغیر شامل تعدادی از کتاب‌خانه‌های زبان c می‌باشد. در بسیاری از کدهای xv6 توابع این کتاب‌خانه‌ها استفاده شده‌اند و برای اجرایشان به کامپایل این فایل‌ها نیاز داریم. برای مثال برنامه‌های سطح کاربر نیازمند کامپایل فایل‌های ULIB می‌باشند؛ بنابراین همانطور که در بخش قبل نیز گفته شد، فایل‌های ULIB به عنوان پیشنیاز در قوانین قرار گرفته‌اند و در نهایت توسط دستور ld به فایل‌های اجرایی پیوست[[4]](#footnote-4) می‌شوند. فایل‌های ULIB شامل توابعی مانند printf، strcmp، strcpy، malloc و ... هستند.

در نهایت، همانطور که از اسم این متغیرها نیز پیداست، UPROGS معادل user programs و ULIB معادل User Libraries است که به ترتیب برنامه‌های کاربر و کتاب‌خانه‌های کاربر محسوب می‌شوند.

# اجرا بر روی شبیه‌ساز QEMU

## محتوای دو دیسک ورودی QEMU

# مراحل بوت سیستم‌عامل xv6

# اجرای بوت‌لودر

## محتوای سکتور نخست دیسک قابل بوت

## مقایسه فایل باینری بوت با بقیه فایل های باینری xv6 و تبدیل آن به اسمبلی

## علت استفاده از objcopy در هنگام make

## چرا برای بوت کردن فقط از فایل C استفاده نشده و اسمبلی هم هست؟

## وظیفه ثبات های x86

* ثبات عام منظوره: پردازنده‌های x86 دارای 8 ثبات عام منظوره هستند. از این ثبات‌ها می‌توان به ثبات انباشت‌کننده[[5]](#footnote-5) اشاره کرد که یک ثبات میانی برای ذخیره خروجی بخش محاسباتی (ALU) است. نام این ثبات از این رو انباشت‌کننده نهاده شده که پس از هر بار انجام محاسبات، نتیجه در آن ذخیره شده و در محاسبات بعدی از مقدار ذخیره شده در آن به عنوان ورودی استفاده می‌شود و دوباره نتیجه آن در همین ثبات ذخیره می‌شود. به عبارتی دیگر بصورت نوبتی، نتایج محاسبات در آن انباشت می‌شوند.
* ثبات قطعه: پردازنده‌های x86 دارای 6 ثبات عام منظوره هستند. یک ثبات قطعه، ثبات پشته[[6]](#footnote-6) می‌باشد. این ثبات اطلاعاتی مربوط به قطعه‌ای از حافظه را ذخیره می‌کند که از آن برای پشته فراخوانی[[7]](#footnote-7) استفاده می‌شود. دقت شود که ثبات قطعه پشته (SS) با ثبات نشانگر پشته (SP) تفاوت دارد؛ برای اطلاعات بیشتر در این خصوص به [این پیوست](https://stackoverflow.com/questions/8642813/what-is-the-difference-between-esp-register-and-ss-register) مراجعه کنید.
* ثبات وضعیت: ثبات FLAGS، ثبات وضعیتی است که نشان‌دهنده حالت فعلی پردازنده است. این ثبات مخصوص پردازنده‌های 16 بیتی است. EFLAGS و RFLAGS ثبات‌های مشابه برای پردازنده‌های 32بیتی و 64بیتی می‌باشند. هر بیت از این ثبات نشان‌دهنده یک پرچم[[8]](#footnote-8) برای یک وضعیت می‌باشد که می‌تواند حالت درست یا غلط داشته باشد. این پرچم‌ها نشان‌دهنده وضعیت اعمال منطقی و محاسباتی یا محدودیت‌های اعمال شده بر عملیات فعلی پردازنده هستند. واضح است که عملکرد این پرچم‌ها به تعداد بیت‌های رجیستر و معماری پردازنده بستگی دارد. ثبات FLAGS برای پردازنده Intel x86 به شرح زیر می‌باشد:

|  |  |  |  |
| --- | --- | --- | --- |
| Intel x86 FLAGS register | | | |
| بیت | مخفف | توضیح | دسته‌بندی |
| 0 | CF | Carry flag | وضعیت |
| 1 |  | رزرو شده |  |
| 2 | PF | Parity flag | وضعیت |
| 3 |  | رزرو شده |  |
| 4 | AF | Adjust Flag | وضعیت |
| 5 |  | رزرو شده |  |
| 6 | ZF | Zero flag | وضعیت |
| 7 | SF | Sign flag | وضعیت |
| 8 | TF | Trap flag | کنترل |
| 9 | IF | Interrup en flag | کنترل |
| 10 | DF | Direction flag | کنترل |
| 11 | OF | Overflow flag | وضعیت |
| 12-13 | IOPL | سطح دسترسی ورودی خروجی | سیستم |
| 14 | Nt | پرچم فعالیت تو در تو | سیستم |
| 15 |  | رزرو شده |  |

* ثبات کنترلی: این نوع از ثبات‌ها مسئول تغییر در رفتار کلی پردازنده و یا دیگر دستگاه‌های مرتبطند. از این دسته ثبات‌ها می‌توان به ثبات CR0 اشاره کرد که در پردازنده‌های 32بیتی مانند i386 و بالاتر استفاده می‌شود. بیت‌های این ثبات نشان‌دهنده تغییرات و کنترل‌های مختلفی در رفتار کلی پردازنده هستند که به شرح زیر می‌باشد:

|  |  |  |
| --- | --- | --- |
| بیت | مخفف | نام |
| 0 | PE | Protected Mode Enable |
| 1 | MP | Monitor co-processor |
| 2 | EM | Emulation |
| 3 | TS | Task switched |
| 4 | ET | Extension type |
| 5 | NE | Numeric error |
| 16 | WP | Write protect |
| 18 | AM | Alignment mask |
| 29 | NW | Not-write through |
| 30 | CD | Cache disabled |
| 31 | PG | Paging |

## نقص اصلی real mode پردازنده x86

## آدرس دهی حافظه در real mode

## کد bootmain.c چرا هسته را در آدرس 0x100000 قرار می‌دهد؟

## کد معادل entry.s در هسته لینوکس

# اجرای هسته xv6

## چرا آدرس فیزیکی است؟

## توابع entry.s را توضیح دهید و تابع معادل در هسته لینوکس را بیابید

## مختصری راجع به محتوای فضای آدرس مجازی هسته

## چرا برای کد و داده های سطح کاربر پرچم SEG\_USER تنظیم شده است؟

# اجرای نخستین برنامه سطح کاربر

## اجزای struct proc و معادل آن در لینوکس

## چرا به خواب رفتن در کد مدیریت‌کننده سیستم مشکل ساز است؟

## تفاوت فضای آدرس هسته با فضای آدرس توسط kvmalloc

## تفاوت فضای آدرس inituvm با فضای آدرس کاربر در کد مدیریت سیستم

## کدام بخش از آماده‌سازی سیستم بین تمامی هسته های پردازنده مشترک و کدام بخش اختصاصی است؟

## برنامه معادل initcode.s در هسته لینوکس

# اشکال زدایی

# روند اجرای GDB

## دستور مشاهده breakpoint ها

## دستور حذف یک breakpoint

# کنترل روند اجرا و دسترسی به حالت سیستم

## خروجی bt

## تفاوت دستور x و print

## نمایش وضعیت ثبات ها و متغیر های محلی؛ رجیستر های edi و esi

## ساختار struct input

# اشکال زدایی در سطح کد اسمبلی

## خروجی دستور های layout src و layout asm در TUI

## دستور های جابجایی میان توابع زنجیره فراخوانی جاری (نقطه توقف)

1. Target [↑](#footnote-ref-1)
2. Prerequisite [↑](#footnote-ref-2)
3. Built-in rule [↑](#footnote-ref-3)
4. Link [↑](#footnote-ref-4)
5. Accumulator register [↑](#footnote-ref-5)
6. Stack [↑](#footnote-ref-6)
7. Call stack [↑](#footnote-ref-7)
8. Flag [↑](#footnote-ref-8)