CS344: Operating Systems Lab
Assignment 3

Group- M10

Dhruvesh Bhure, Roll- 200123018
Soham Roy, Roll- 200123055
Dev Sandip Shah, Roll- 200123074

Part A:

Lazy Memory Allocation:-

In this part of the lab, we have implemented the Lazy Memory Allocation for xv6, which is a feature in most modern operating systems. In the case of the original xv6, it makes use of the sbrk() system call, to allocate physical memory and map it to the virtual address space. In the first section, we modified the sbrk() system call to remove the memory allocation and cause a page fault. In the second section, we have modified the trap.c file to resolve this page fault via lazy allocation.

1.Eliminate allocation from sbrk():

In this section, we have modified the sbrk() system call (also provided to us in the patch file). After initial declarations and error handling, the sbrk() system call has 4 essential lines in it.

```
int
sys_sbrk(void)
{
  int addr;
  int n;

  if(argint(0, &n) < 0)
    return -1;
  addr = myproc()->sz;
  myproc()->sz += n;
  /*if(growproc(n) < 0)
    return -1;*/
  return addr;
}
```

Line 53: Assigns addr to the start of the newly allocated region Line 54: Increases the size for the current process by a factor n Line 55: Calls the growproc(n) function in proc.c, which allocates n bytes of memory for the process. Line 56: Returns the addr
.
Now we comment-out the line 55 and 56, and this makes the process to believe that it has got it's requested memory, while in reality it does not. This will cause a trap error, with the code 14 when we try to run something like echo hi or ls. The code 14 corresponds to the page fault error,

```
$ echo hi
pid 3 sh: trap 14 err 6 on cpu 0 eip 0x112c addr 0x4004--kill proc
```

2. <u>Lazy Allocation in xv-6:</u>

In this section, we handle the page fault resulting from the changes in part A.1. For this we make use of the following observations:

a. The file trap.c has the code that produces the trap error as observed in part A.1. This is present in the default case for the switch(tf->trapno) as follows:

```
    // In user space, assume process misbehaved.
    cprintf("pid %d %s: trap %d err %d on cpu %d "
            "eip 0x%x addr 0x%x--kill proc\n",
            myproc()->pid, myproc()->name, tf->trapno,
            tf->err, cpuid(), tf->eip, rcr2());
    myproc()->killed = 1;
  }
```

b. Comparing with the above output we realise that rcr2() represents the contents of the control register 2 which in turn has the faulting virtual address. This is what goes into the input of PGROUNDDOWN(va) later.

c. Inside the T_PGFLT case, we make use of PGROUNDDOWN(va) to round down the virtual address to the start of the page boundary.

d. In vm.c, we have the function allocuvm() which is what sbrk() makes use of via the growproc() function.

e. Studying allocuvm(), makes it clear that it assigns 4KB (PGSIZE) of pages to a function making use of kalloc(), in a loop for as many pages as are needed. In our case we need a similar thing, except that we can do away with the loop and assign 1 page of size 4KB (PGSIZE) as and when a page fault occurs.

f. A final observation is to remove the static keyword for the mappages function in vm.c and declare it as extern in trap.c. This will make sure that we can call it inside the switch case. We also add a break; statement to make sure that fall-through does not occur and the default statements are not executed.

The code changed in various files are as:

In trap.c:

```c
extern int mappages(pde_t *pgdir, void *va, uint size, uint pa, int perm);
```

```c
    case T_PGFLT:
    {
      // code from allocuvm
      //cprintf("Trap Number : %x\n", tf->trapno);
      cprintf("rcr2() : 0x%x\n", rcr2());

      uint newsz = myproc()->sz;
      uint a = PGROUNDDOWN(rcr2());
      if(a < newsz){
        char *mem = kalloc();
        if(mem == 0) {
          cprintf("out of memory\n");
          exit();
          break;
        }
        memset(mem, 0, PGSIZE);
        mappages(myproc()->pgdir, (char*)a, PGSIZE, V2P(mem), PTE_W|PTE_U);
      }
      break;
    }
```

In vm.c:

```c
int
mappages(pde_t *pgdir, void *va, uint size, uint pa, int perm)
```

The output on running commands like echo and ls is shown below. As can be seen, the trap error does not occur any more. Additionally, we have used cprintf in our code to print the faulting virtual address in each case, which shows up in the terminal output -

```
sb: size 1000 nblocks 941 ninodes 200 nlog 30 logstart 2 inodestart 32 bmap sta8
init: starting sh
$ echo
rcr2() : 0x4004
rcr2() : 0xbfa4
$ echo hi
rcr2() : 0x4004
rcr2() : 0xbfa4
hi
$ ls
rcr2() : 0x4004
rcr2() : 0xbfa4
.              1 1 512
..             1 1 512
README         2 2 2286
cat            2 3 15516
echo           2 4 14400
forktest       2 5 8836
grep           2 6 18352
init           2 7 15020
kill           2 8 14484
ln             2 9 14380
ls             2 10 16948
mkdir          2 11 14508
rm             2 12 14488
sh             2 13 28536
stressfs       2 14 15416
usertests      2 15 62888
wc             2 16 15936
zombie         2 17 14056
console        3 18 0
$
```

PART B:

Answer to the given questions: -

1. How does the kernel know which physical pages are used and unused?
   Ans. -

```c
struct {
  struct spinlock lock;
  int use_lock;
  struct run *freelist;
} kmem;
```

xv-6 maintains a **linked list** of free pages in **kalloc.c** called **kmem**. Initially the list is empty so xv-6 calls **kinit1** through **main**() which adds 4MB of free pages to the list.

2. What data structures are used to answer this question?
   Ans. -
   A **linked list** named **freelist** as shown in the above image. Every node of the linked list is a structure defined in **kalloc.c** namely **struct run** (pages are typecast to (struct run *) when inserting into freelist in kfree (char *v)).

3. Where do these reside?
   Ans: -
   This **linked list** is declared inside **kalloc.c** inside a structure **kmem.** Every node is of the type struct run which is also defined inside **kalloc.c**

4. Does xv6 memory mechanism limit the number of user processes?
   Ans: -
   Due to a limit on the size of ptable (a max of **NPROC** elements which is set to **64** by default), the number of user processes are limited in xv-6. **NPROC** is defined in **param.h**.

5. If so, what is the lowest number of processes xv6 can 'have' at the same time (assuming the kernel requires no memory whatsoever)?
   Ans: -
   When the xv-6 operating system boots up, there is only one process named **initproc** (this process forks the sh process which forks other user processes). Also, since a process can have a virtual address space of 2GB (**KERNBASE**) and the assumed maximum physical memory is 240 MB (**PHYSTOP**), one process can take up all of the physical memory (We added this since the question asks from a memory management perspective). Hence, **the answer is 1.**

   There cannot be zero processes after boot since, all user interactions need to be done using user processes which are forked from initproc/sh.

Task 1:

The **create_kernel_process**() function was created in **proc.c**. The kernel process will remain in kernel mode the whole time. Thus, **we do not need to initialise its trapframe** (trapframes store userspace register values), user space and the user section of its page table. The **eip** register of the process' context stores the address of the next instruction. We want the process to start executing at the entry point (which is a function pointer).

Thus, **we set the eip value of the context to entry point** (Since entry point is the address of a function). **allocproc** assigns the process a spot in ptable. **setupkvm** sets up the kernel part of the process' page table that maps virtual addresses above **KERNBASE** to physical addresses between 0 and **PHYSTOP**.

proc.c :

```
void create_kernel_process(const char *name, void (*entrypoint)()){

  struct proc *p = allocproc();

  if(p == 0)
    panic("create_kernel_process failed");

  //Setting up kernel page table using setupkvm
  if((p->pgdir = setupkvm()) == 0)
    panic("setupkvm failed");

  //This is a kernel process. Trap frame stores user space registers. We don't need to initialise tf.
  //Also, since this doesn't need to have a userspace, we don't need to assign a size to this process.

  //eip stores address of next instruction to be executed
  p->context->eip = (uint)entrypoint;

  safestrcpy(p->name, name, sizeof(p->name));

  acquire(&ptable.lock);
  p->state = RUNNABLE;
  release(&ptable.lock);

}
```

Task 2:

This task has various parts. First, we need a **process queue** that keeps track of the processes that were refused additional memory since there were no free pages available. We created a **circular queue struct** called **rq**. And the specific queue that holds processes with **swap out requests** is **rqueue**. We have also created the functions corresponding to rq, namely **rpush()** and **rpop()**. The queue needs to be accessed with a lock that we have initialised in **pinit**. We have also initialised the initial values of **s** and **e** to zero in **Userinit**. Since the queue and the functions relating to it are needed in other files too, we added prototypes in **defs.h** too.

proc.c : -

```
struct rq{
  struct spinlock lock;
  struct proc* queue[NPROC];
  int s;
  int e;
};
```

```
void
userinit(void)
{
  acquire(&rqueue.lock);
  rqueue.s=0;
  rqueue.e=0;
  release(&rqueue.lock);
```

```c
void
pinit(void)
{
  initlock(&ptable.lock, "ptable");
  initlock(&rqueue.lock, "rqueue");
  initlock(&sleeping_channel_lock, "sleeping_channel");
  initlock(&rqueue2.lock, "rqueue2");
}
```

```c
struct proc* rpop(){

  acquire(&rqueue.lock);
  if(rqueue.s==rqueue.e){
        release(&rqueue.lock);
        return 0;
  }
  struct proc *p=rqueue.queue[rqueue.s];
  (rqueue.s)++;
  (rqueue.s)%=NPROC;
  release(&rqueue.lock);

  return p;
}
```

```c
int rpush(struct proc *p){

  acquire(&rqueue.lock);
  if((rqueue.e+1)%NPROC==rqueue.s){
        release(&rqueue.lock);
    return 0;
  }
  rqueue.queue[rqueue.e]=p;
  rqueue.e++;
  (rqueue.e)%=NPROC;
  release(&rqueue.lock);

  return 1;
}
```

defs.h :-

*__Note__: **rqueue2** (and correspondingly **rpush2** and **rpop2**) is used in **Task 3.**

```c
struct rq;
```

```c
extern int swap_out_process_exists;
extern int swap_in_process_exists;
extern struct rq rqueue;
extern struct rq rqueue2;
int rpush(struct proc *p);
struct proc* rpop();
struct proc* rpop2();
int rpush2(struct proc* p);
```

Now, whenever **kalloc** is not able to allocate pages to a process, it returns zero. This notifies **allocuvm** that the requested memory wasn't allocated (mem=0). Here, we first need to change the process state to sleeping. (***Note**: The process sleeps on a special sleeping channel called **sleeping_channel** that is secured by a lock called **sleeping_channel_lock**. **sleeping_channel_count** is used for corner cases when the system boots) Then, we need to add the current process to the swap out request queue, **rqueue**:

vm.c:

Global declarations (Note: These are also declared in defs.h as extern Yariables. We are not adding the defs.h screenshots):

```
struct spinlock sleeping_channel_lock;
int sleeping_channel_count=0;
char * sleeping_channel;
```

allocuvm:

```
  if(mem == 0){
    // cprintf("allocuvm out of memory\n");
    deallocuvm(pgdir, newsz, oldsz);

    //SLEEP
    myproc()->state=SLEEPING;
    acquire(&sleeping_channel_lock);
    myproc()->chan=sleeping_channel;
    sleeping_channel_count++;
    release(&sleeping_channel_lock);

          rpush(myproc());
    if(!swap_out_process_exists){
      swap_out_process_exists=1;
      create_kernel_process("swap_out_process", &swap_out_process_function);
    }

    return 0;
  }
```

***Note:** create_kernel_process here creates a swapping out kernel process to allocate a page for this process if it doesn't already exist. When the swap out process ends, the **swap_out_process_exists (declared as extern in defs.h and initialised in proc.c to 0)** variable is set to 0. When it is created, it is set to 1 (as seen above). This is done so multiple swap out processes are not created. **swap_out_process** is explained later.

Next, we create a mechanism by which whenever free pages are available, all the processes sleeping on **sleeping_channel** are woken up. We edit **kfree** in **kalloc.c** in the following way: Basically, all processes that were preempted due to lack of availability of pages were sent sleeping on the sleeping channel. We wake all processes currently sleeping on **sleeping_channel** by calling the **wakeup()** system call.

```c
// initializing the allocator; see kinit above.)
void
kfree(char *v)
{

  struct run *r;
  // struct proc *p=myproc();

  if((uint)v % PGSIZE || v < end || V2P(v) >= PHYSTOP){
    panic("kfree");
  }

  // Fill with junk to catch dangling refs.
  // memset(v, 1, PGSIZE);
  for(int i=0;i<PGSIZE;i++){
    v[i]=1;
  }

  if(kmem.use_lock)
    acquire(&kmem.lock);
  r = (struct run*)v;
  r->next = kmem.freelist;
  kmem.freelist = r;
  if(kmem.use_lock)
    release(&kmem.lock);

  //Wake up processes sleeping on sleeping channel.
  if(kmem.use_lock)
    acquire(&sleeping_channel_lock);
  if(sleeping_channel_count){
    wakeup(sleeping_channel);
    sleeping_channel_count=0;
  }
  if(kmem.use_lock)
    release(&sleeping_channel_lock);

}
```

Now, we will explain the **swapping out process**. The entry point for the swapping out process in **swap_out_process_function**. Since the function is very long, we have attached two screenshots:

```c
void swap_out_process_function(){

  acquire(&rqueue.lock);
  while(rqueue.s!=rqueue.e){
    struct proc *p=rpop();

    pde_t* pd = p->pgdir;
    for(int i=0;i<NPDENTRIES;i++){

      //skip page table if accessed. chances are high, not every page table was accessed.
      if(pd[i]&PTE_A)
        continue;
      //else
      pte_t *pgtab = (pte_t*)P2V(PTE_ADDR(pd[i]));
      for(int j=0;j<NPTENTRIES;j++){

        //Skip if found
        if((pgtab[j]&PTE_A) || !(pgtab[j]&PTE_P))
          continue;
        pte_t *pte=(pte_t*)P2V(PTE_ADDR(pgtab[j]));

        //for file name
        int pid=p->pid;
        int virt = ((1<<22)*i)+((1<<12)*j);

        //file name
        char c[50];
        int_to_string(pid,c);
        int x=strlen(c);
        c[x]='_';
        int_to_string(virt,c+x+1);
        safestrcpy(c+strlen(c),".swp",5);

        // file management
        int fd=proc_open(c, O_CREATE | O_RDWR);
        if(fd<0){
          cprintf("error creating or opening file: %s\n", c);
          panic("swap_out_process");
        }
```

```c
        if(proc_write(fd,(char *)pte, PGSIZE) != PGSIZE){
          cprintf("error writing to file: %s\n", c);
          panic("swap_out_process");
        }
        proc_close(fd);

        kfree((char*)pte);
        memset(&pgtab[j],0,sizeof(pgtab[j]));

        //mark this page as being swapped out.
        pgtab[j]=((pgtab[j])^(0x080));

        break;
      }
    }

  }

  release(&rqueue.lock);

  struct proc *p;
  if((p=myproc())==0)
    panic("swap out process");

  swap_out_process_exists=0;
  p->parent = 0;
  p->name[0] = '*';
  p->killed = 0;
  p->state = UNUSED;
  sched();
}
```

Image 1: The process runs a loop until the swap out requests queue (**rqueue1**) is non empty. When the queue is empty, a set of instructions are executed for the termination of **swap_out_process** (**Image2**). The loop starts by popping the first process from **rqueue** and uses the LRU policy to determine a victim page in its page table. We iterate through each entry in the process' page table (**pgdir**) and extracts the physical address for each secondary page table. For each secondary page table, we iterate through the page table and look at the **accessed bit (A)** on each of the entries (The accessed bit is the sixth bit from the right. We check if it is set by checking the **bitwise &** of the entry and **PTE_A (which we defined as 32 in mmu.c)).**

Important note regarding the Accessed flag: Whenever the process is being context switched into by the scheduler, all accessed bits are unset. Since we are doing this, the accessed bit seen by swap_out_process_function will indicate whether the entry was accessed in the last iteration of the process:

```
    for(int i=0;i<NPDENTRIES;i++){
      //If PDE was accessed

      if(((p->pgdir)[i])&PTE_P && ((p->pgdir)[i])&PTE_A){

        pte_t* pgtab = (pte_t*)P2V(PTE_ADDR((p->pgdir)[i]));

        for(int j=0;j<NPTENTRIES;j++){
          if(pgtab[j]&PTE_A){
            pgtab[j]^=PTE_A;
          }
        }

        ((p->pgdir)[i])^=PTE_A;
      }
    }

    // Switch to chosen process.  It is the process's job
    // to release ptable.lock and then reacquire it
    // before jumping back to us.
    c->proc = p;
    switchuvm(p);
```

This code resides in the scheduler and it basically unsets every accessed bit in the process' page table and its secondary page tables.

Now, back to swap_out_process_function. As soon as the function finds a secondary page table entry with the accessed bit unset, it chooses this entry's physical page number (using macros mentioned in part A report) as the victim page. This page is then swapped out and stored to drive.

We use the process' pid and virtual address of the page to be eliminated to name the file that stores this page. We have created a new function called **'int_to_string'** that copies an integer into a given string. We use this function to make the filename using integers **pid** and **virt**. Here is that function (declared in **proc.c**):

```c
void int_to_string(int x, char *c){
  if(x==0)
  {
    c[0]='0';
    c[1]='\0';
    return;
  }
  int i=0;
  while(x>0){
    c[i]=x%10+'0';
    i++;
    x/=10;
  }
  c[i]='\0';

  for(int j=0;j<i/2;j++){
    char a=c[j];
    c[j]=c[i-j-1];
    c[i-j-1]=a;
  }

}
```

We need to write the contents of the victim page to the file with the name **<pid>_<vid>.swp**. But we encounter a problem here. We store the filename in a string called c. File system calls cannot be called from proc.c. The solution was that we copied the **open, write, read, close** etc. functions from **sysfile.c** to **proc.c**, modified them since the **sysfile.c** functions used a different way to take arguments and then renamed them to **proc_open, proc_read, proc_write, proc_close etc**. so we can use them in proc.c. Some examples:

```c
int
proc_write(int fd, char *p, int n)
{
  struct file *f;
  if(fd < 0 || fd >= NOFILE || (f=myproc()->ofile[fd]) == 0)
    return -1;
  return filewrite(f, p, n);
}
```

There are many more functions **(proc open, proc_fdalloc etc.)** and you can check them out in proc.c. We can't paste all of them here.

```c
int
proc_close(int fd)
{
  struct file *f;

  if(fd < 0 || fd >= NOFILE || (f=myproc()->ofile[fd]) == 0)
    return -1;

  myproc()->ofile[fd] = 0;
  fileclose(f);
  return 0;
}
```

Now, using these functions, we write back a page to storage. We open a file (**using proc_open**) with **O_CREATE** and **O_RDWR** permissions (we have imported **fcntl.h** with these macros). **O_CREATE** creates this file if it doesn't exist and O_RDWR refers to read/write. The file descriptor is stored in an integer called **fd**. Using this file descriptor, we write the page to this file using **proc_write**. Then, this page is added to the **free page queue** using **kfree** so it is available for use (remember we also wake up all processes sleeping on sleeping_channel when kfree adds a page to the free queue). We then clear the page table entry too using memset. After this, we do something important: **for Task 3, we need to know if the page that caused a fault was swapped out or not. In order to mark this page as swapped out, we set the 8th bit from the right (2^7) in the secondary page table entry. We use xor to accomplish this task**

Suspending kernel process when no requests are left:

When the queue is empty, the loop breaks and suspension of the process is initiated. While exiting the kernel processes that are running, we can't clear their **kstack** from within the process because after this, they will not know which process to execute next. We need to clear their **kstack** from outside the process. For this, we first preempt the process and wait for the scheduler to find this process.

When the scheduler finds a kernel process in the UNUSED state, it clears this process' kstack and name. The scheduler identifies the kernel process in unused state by checking its name in which the first character was changed to '*' when the process ended.

Thus the ending of kernel processes has two parts:
1. from within process:

```c
  struct proc *p;
  if((p=myproc())==0)
    panic("swap out process");

  swap_out_process_exists=0;
  p->parent = 0;
  p->name[0] = '*';
  p->killed = 0;
  p->state = UNUSED;
  sched();
}
```

2. From scheduler

```c
    for(p = ptable.proc; p < &ptable.proc[NPROC]; p++){

      //If the swap out process has stopped running, free its stack and name.
      if(p->state==UNUSED && p->name[0]=='*'){

        kfree(p->kstack);
        p->kstack=0;
        p->name[0]=0;
        p->pid=0;
      }
```

All check marks in assignment accomplished:

- **Note**: the swapping out process must support a request queue for the swapping requests.
- **Note**: whenever there are no pending requests for the swapping out process, this process must be suspended from execution.
- **Note**: whenever there exists at least one free physical page, all processes that were suspended due to lack of physical memory must be woken up.
- **Note**: only user-space memory can be swapped out (this does not include the second level page table) (**since we are iterating all top tables from to bottom and all user space entries come first (until KERNBASE), we will swap out the first user space page that was not accessed in the last iteration.**)

Task 3:
We first need to create a **swap in request queue**. We used the same struct (**rq**) as in Task 2 to create a swap in request queue called **rqueue2** in **proc.c**. We also declare an extern prototype for rqueue2 in defs.h. Along with declaring the queue, we also created the corresponding functions for **rqueue2** (**rpop2()** and **rpush2()**) in proc.c and declared their prototype in defs.h. We also initialised its lock in **pinit**. We also initialised its **s** and **e** variables in userinit.
Since all the functions/variables are similar to the ones shown in Task 2, I am not attaching their screenshots here.

Next, we add an additional entry to the **struct proc** in **proc.h** called **addr (int)**. This entry will tell the swapping in function at which virtual address the page fault occurred:

proc.h (in struct proc):

```
char name[16];               // Process name (debugging)
int addr;                    // ADDED: virtual address of pagefault
```

Next, we need to handle page fault (**T_PGFLT**) traps raised in trap.c. We do it in a function called **handlePageFault()**:

trap.c:

```
case T_PGFLT:
  handlePageFault();
break;
```

```
void handlePageFault(){
  int addr=rcr2();
  struct proc *p=myproc();
  acquire(&swap_in_lock);
  sleep(p,&swap_in_lock);
  pde_t *pde = &(p->pgdir)[PDX(addr)];
  pte_t *pgtab = (pte_t*)P2V(PTE_ADDR(*pde));

  if((pgtab[PTX(addr)])&0x080){
    //This means that the page was swapped out.
    //virtual address for page
    p->addr = addr;
    rpush2(p);
    if(!swap_in_process_exists){
      swap_in_process_exists=1;
      create_kernel_process("swap_in_process", &swap_in_process_function);
    }
  } else {
    exit();
  }
}
```

In **handlePageFault**, just like **Part A**, we find the virtual address at which the page fault occurred by using **rcr2()**. We then put the current process to sleep with a new lock called **swap_in_lock** (**initialised in trap.c and with extern in defs.h**). We then obtain the page table entry corresponding to this address (the logic is identical to **walkpgdir**). Now, we need to check whether this page was swapped out. In Task 2, **whenever we swapped out a page**, **we set its page table entry's bit of 7th order (2^7)**. Thus, in order to check whether the page was swapped out or not, we check its 7th order bit using **bitwise & with 0x080**. If it is set, we initiate **swap_in_process (if it doesn't already exist - check using swap_in_process_exists)**. Otherwise, we safely suspend the process using exit() as the assignment asked us to do.

Now, we go through the **swapping in process.** The entry point for the swapping out process is **swap_in_process_function (declared in proc.c)** as you can see in handlePageFault.

Note: swap_in_process_function is shown on the next page since it is long. Refer to the next page for the actual function.

We have already mentioned how we have implemented file management functions in **proc.c** in the **Task 2** part of the report. I will just mention which functions I used and how I used them here. The function runs a loop until **rqueue2** is not empty. In the loop, it pops a process from the queue and extracts its **pid** and **addr** value to get the file name. Then, it creates the filename in a string called “**c**” using **int_to_string (described in Task 2 of this report).** Then, it used **proc_open** to open this file in read only mode (**O_RDONLY**) with file descriptor **fd**. We then allocate a free frame (**mem**) to this process using **kalloc.** We read from the file with the fd file descriptor into this free frame using **proc_read**. We then make **mappages** available to **proc.c** by removing the **static** keyword from it in **vm.c** and then declaring a prototype in **proc.c.** We then use **mappages** to map the page corresponding to **addr** with the physical page that got using kalloc and read into (**mem**). Then we wake up, the process for which we allocated a new page to fix the page fault using **wakeup**. Once the loop is completed, we run the kernel process termination instructions.

In Task 3 too, all the check marks were accomplished.

```
int mappages(pde_t *pgdir, void *va, uint size, uint pa, int perm);

```

```
void swap_in_process_function(){

        acquire(&rqueue2.lock);
        while(rqueue2.s!=rqueue2.e){
                struct proc *p=rpop2();

                int pid=p->pid;
                int virt=PTE_ADDR(p->addr);

                char c[50];
            int_to_string(pid,c);
            int x=strlen(c);
            c[x]='_';
            int_to_string(virt,c+x+1);
            safestrcpy(c+strlen(c),".swp",5);

            int fd=proc_open(c,O_RDONLY);
            if(fd<0){
                release(&rqueue2.lock);
                cprintf("could not find page file in memory: %s\n", c);
                panic("swap_in_process");
            }
            char *mem=kalloc();
            proc_read(fd,PGSIZE,mem);

            if(mappages(p->pgdir, (void *)virt, PGSIZE, V2P(mem), PTE_W|PTE_U)<0){
                release(&rqueue2.lock);
                panic("mappages");
            }
            wakeup(p);
        }

    release(&rqueue2.lock);
    struct proc *p;
        if((p=myproc())==0)
          panic("swap_in_process");

        swap_in_process_exists=0;
        p->parent = 0;
        p->name[0] = '*';
        p->killed = 0;
        p->state = UNUSED;
        sched();

}
```

Task 4: Sanity Test:

In this part our aim is to create a testing mechanism in order to test the functionalities created by us in the previous parts. We will implement a user-space program named memtest that will do this job for us. The implementation of memtest is given below.

```
#include "types.h"
#include "stat.h"
#include "user.h"

int math_func(int num){
        return num*num - 4*num + 1;
}

int
main(int argc, char* argv[]){

        for(int i=0;i<20;i++){
                if(!fork()){
                        printf(1, "Child %d\n", i+1);
                        printf(1, "Iteration Matched Different\n");
                        printf(1, "--------- ------- ---------\n\n");

                        for(int j=0;j<10;j++){
                                int *arr = malloc(4096);
                                for(int k=0;k<1024;k++){
                                        arr[k] = math_func(k);
                                }
                                int matched=0;
                                for(int k=0;k<1024;k++){
                                        if(arr[k] == math_func(k))
                                                matched+=4;
                                }

                                if(j<9)
                                        printf(1, "    %d       %dB       %dB\n", j+1, matched, 4096-matched);
                                else
                                        printf(1, "   %d       %dB       %dB\n", j+1, matched, 4096-matched);

                        }
                        printf(1, "\n");

                        exit();
                }
        }

        while(wait()!=-1);
        exit();

}
```

We can make the following observations by looking at the implementation:

- The main process creates 20 child processes using fork() system call.
- Each child process executes a loop with 10 iterations
- At each iteration, 4096B(4 KB) of memory is being allocated using malloc()
- The value stored at index i of the array is given by mathematical expression i^2 - 4i +1 which is computed using math_func().
- A counter named **matched** is maintained which stores the number of bytes that contain the right values. This is done by checking the value stored at every index with the value returned by the function for that index.

In order to run memtest, we need to include it in the Makefile under UPROGS and EXTRA to make it accessible to the xv6 user.

On running memtest, we obtain the following output-

```
$ memtest
Child 1
Iteration Matched Different
--------- ------- ---------

    1      4096B      0B
    2      4096B      0B
    3      4096B      0B
    4      4096B      0B
    5      4096B      0B
    6      4096B      0B
    7      4096B      0B
    8      4096B      0B
    9      4096B      0B
   10      4096B      0B

Child 2
Iteration Matched Different
--------- ------- ---------

    1      4096B      0B
    2      4096B      0B
    3      4096B      0B
    4      4096B      0B
    5      4096B      0B
    6      4096B      0B
    7      4096B      0B
    8      4096B      0B
    9      4096B      0B
   10      4096B      0B

Child 3
Iteration Matched Different
--------- ------- ---------

    1      4096B      0B
    2      4096B      0B
    3      4096B      0B
    4      4096B      0B
    5      4096B      0B
    6      4096B      0B
    7      4096B      0B
    8      4096B      0B
    9      4096B      0B
   10      4096B      0B

Child 4
Iteration Matched Different
```

As can be seen int the output, our implementation **passes** the sanity test as all the indices store the correct value.

Now, to test our implementation even further, we run the tests on different values of **PHYSTOP** (defined in memlayout.h). The default value of PHYSTOP is 0xE000000(224MB). **We changed its value to 0x0400000(4MB)** . We chose 4MB because this is the minimum memory needed by xv6 to execute **kinit1**. On running memtest, **the obtained output is identical to the previous output** indicating that the implementation is correct.