AARON PHILIP
SY PANEL C1
MAIDT ASSIGNMENT 10
ROLL NO. -2

Parameters Passed to file open syscall.

sys_open
rax 2
rdi const char *filename
rsi int flags
rdx int mode

const char *filename (path) represents file name that the program wants to open/create.
int flag specifies how file should be opened i.e read-only, write-only / read & write
int mode specifies permissions of the file for newly created file as an octal number

Steps of file copy operation
1) Open the source file in read mode
2) Read the source file content & store into buffer
3) Create the destination file in read-write mode
4) Write the buffer contents into created / opened file
5) Close the files

Sequence followed - 3, 1, 2, 4, 5
If this sequence is followed a destination file is created and the contents of the source file are the copied successfully into the destination file.

Q3) Can we declare following variable in section .bss
variable: msg2 db "File copied successfully",10

A3) No we cannot declare the above variable in section .bss as this section is used to declare only uninitialized variables.

Q4) operate 2, fname2, 2, 0777q
mov [fd2], rax

0777q must be replaced with 0754q to meet the mentioned requirements.

Owner access is 111 = 7q
group access is 101 = 5q
Other access is 100 = 4q

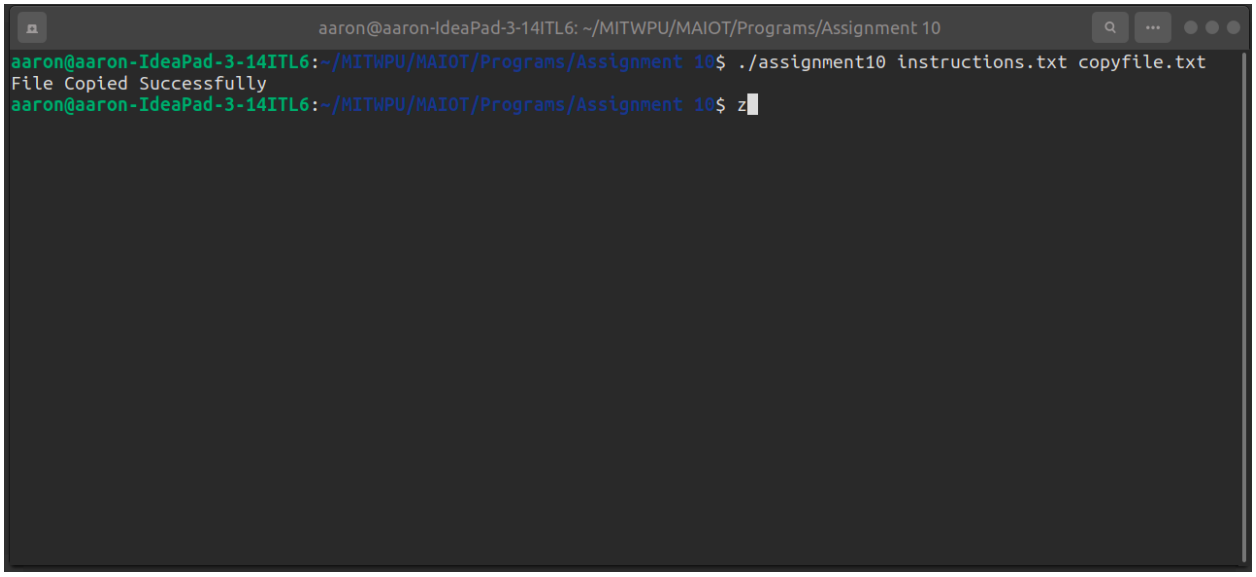
15/2/23

CODE :

```
%macro operate 4
mov rax,%1
mov rdi,%2
mov rsi,%3
mov rdx,%4
syscall
%endmacro

section .data
msg1 db "Error:",10
msgl1 equ $-msg1
msg2 db "File Copied Successfully",10
msgl2 equ $-msg2

section .bss
fname1 resb 15
fd1 resq 1
fname2 resb 15
fd2 resq 1
buff resb 1024
bufflen resq 1

section .text
global _start
_start:
pop r8 ; command line args are stored in the r8 register
cmp r8,3 ; check if 3 arguments were given (./fname one.txt two.txt)
jne err ; if 3 args are not given then jump to the err label
pop r8 ; pop the second (arg2)
pop r8 ; pop the first (arg1)

mov rsi,fname1 ; (copy the full file name till the null string is reached)

above:
mov al,[r8]; (first .txt) so f will be moved to rsi then i and so on
cmp al,00; if al is 00 then we know that the null character was loaded in al
je next
mov [rsi],al
inc r8
inc rsi
jmp above ; the point of the above loop was to copy name of source file into fname1
```

```
next:
pop r8
mov rsi,fname2

above2:
mov al,[r8]
cmp al,00
je next2
mov [rsi],al
inc r8
inc rsi
jmp above2

next2:
operate 2,fname1,000000q,0777q ; 000000q means read-mode and 0777q is read write exec
perm
mov [fd1],rax

operate 0,[fd1],buff,1024 ; read the first file
mov [bufflen],rax


operate 85,fname2,0777q,0 ; create the second file (85)
operate 2,fname2,2,0777q ; open second file
mov [fd2],rax

operate 1,[fd2],buff,[bufflen] ; write into the Second file
operate 3,[fd2],0,0 ; close the second file
operate 3,[fd1],0,0 ; close the first file

operate 1,1,msg2,msgl2
jmp end

err:
operate 1,1,msg1,msgl1
end:
operate 60,0,0,0
```

OUTPUT :


aaron@aaron-IdeaPad-3-14ITL6: ~/MITWPU/MAIOT/Programs/Assignment 10
aaron@aaron-IdeaPad-3-14ITL6:~/MITWPU/MAIOT/Programs/Assignment 10$ ./assignment10 instructions.txt copyfile.txt
File Copied Successfully
aaron@aaron-IdeaPad-3-14ITL6:~/MITWPU/MAIOT/Programs/Assignment 10$ z