

Operating Systems Lab 04 (Handouts)

Course: Operating Systems (CL2006)
Instructor: Sameer Faisal

Semester: Fall 2025
T.A: N/A

Note:

- Maintain discipline during the lab.
 - Listen and follow the instructions as they are given.
 - Just raise hand if you have any problem.
 - Completing all tasks of each lab is compulsory.
 - Get your lab checked at the end of the session.
-

OBJECTIVE

The objective of this lab is to learn about Linux process management, commands to see running processes, system call to create processes, get their IDs, and wait and exec system call and to learn about zombie and orphan processes.

Linux Processes

A Linux process or task is known as the instance of a program running under Linux environment. This means that if 10 users from servers are running gedit editor, then there are 10 gedit processes running on the server. Although they are sharing same executable code. The processes running in a Linux system can be view using 'ps' command which we covered in lab 01.

Process ID

In Linux system, each process running has been assigned a unique ID which is known as PID (Process Identification Number). For example, Firefox is a running process if you are browsing the internet. Each time you start a new Firefox browser the system will automatically assign a PID to the new process of Firefox. A PID is automatically assigned when a new process is created on the system. If you wish to find out the PID of the running process like Firefox you may use the command 'pidof'.

1. pidof firefox
2. pidof bash
3. pidof bioset

```
sameer@virtual-machine:~/Desktop/lab04$ pidof firefox
2832 2830 2790 2788 2737 2713 2660 2599
sameer@virtual-machine:~/Desktop/lab04$ pidof bash
2556
sameer@virtual-machine:~/Desktop/lab04$ |
```

To view the running process in a form of a tree we can use ‘pstree’ command. Which shows the running process in a form of a tree.

```

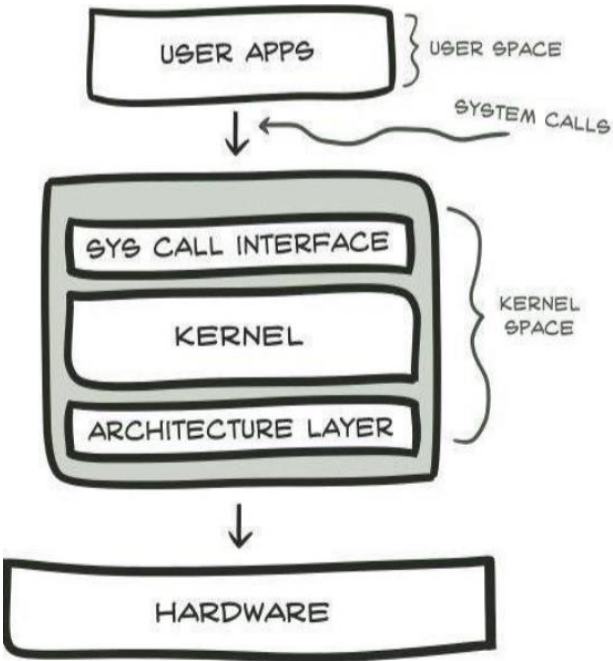
sameer@virtual-machine:~/Desktop/lab04$ pstree
systemd┌─ModemManager─2*[{ModemManager}]
      │┌─NetworkManager─2*[{NetworkManager}]
      │├─VGAuthService
      │├─accounts-daemon─2*[{accounts-daemon}]
      │├─acpid
      │├─avahi-daemon─avahi-daemon
      │├─bluetoothd
      │├─colord─2*[{colord}]
      │├─cron
      │├─cups-browsed─2*[{cups-browsed}]
      │├─cupsd─dbus
      │├─dbus-daemon
      │├─gdm3┌─gdm-session-wor┌─gdm-x-session┌─Xorg─{Xorg}
      │      │               │               │├─gnome-session-b└─ssh-agent
      │      │               │               │                2*[{gnome-session-b}]
      │      │               │               └─2*[{gdm-x-session}]
      │      │               └─2*[{gdm-session-wor}]
      │      └─2*[{gdm3}]
      │├─gnome-keyring-d─3*[{gnome-keyring-d}]
      │├─irqbalance─{irqbalance}
      │├─2*[{kerneloops}]
      │├─networkd-dispat
      └─polkitd─2*[{polkitd}]
  
```

Process Management

In general, a process is an instance of a program written and compiled. There can be multiple instances of a same program. In other words, a program that is loaded into computer’s memory and is in a state of execution is called a process. Processes are dynamic entity. Process essentially requires CPU and RAM resources but may also require I/O, Network or Printer depending on the program written.

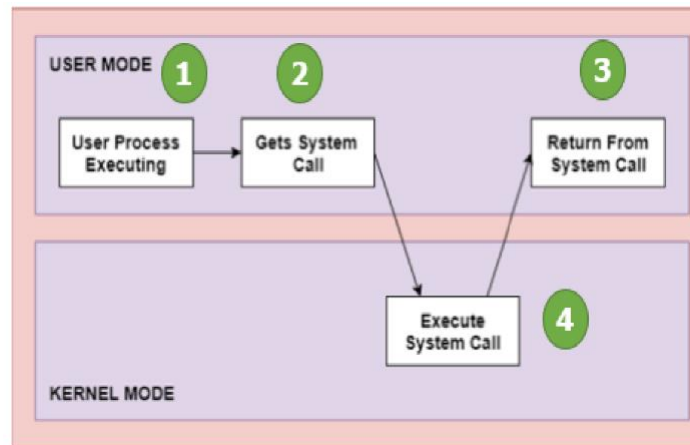
System Calls

A system call is a mechanism that provides the interface between a process and the operating system. It is a programmatic method in which a computer program requests a service from the kernel of the OS. System call offers the services of the operating system to the user programs via API (Application Programming Interface). System calls are the only entry points for the kernel system.



Architecture of System Calls

Given System Call example diagram.



Step 1) The processes executed in the user mode till the time a system call interrupts it.

Step 2) After that, the system call is executed in the kernel-mode on a priority basis.

Step 3) Once system call execution is over, control returns to the user mode.

Step 4) The execution of user processes resumed in Kernel mode.

Types of System Calls

Here are the five types of System Calls in OS:

1. Process Control.
2. File Management.
3. Device Management.
4. Information Maintenance.
5. Communications.

Process Control

This system calls perform the task of process creation, process termination, etc.

Functions

1. End & Abort.
2. Load & Execute.
3. Create process & Terminate process.
4. Wait & Signal event.
5. Allocate & Free memory.

File Management

File management system calls handle file manipulation jobs like creating a file, reading and writing, etc.

Functions

1. Create a file.
2. Delete a file.
3. Open & Close a file
4. Read, Write & Reposition.
5. Get & Set file attributes.

Device Management Device management does the job of device manipulation like reading from device buffers, writing into device buffers, etc. Functions <ol style="list-style-type: none"> 1. Request & Release device. 2. Logically attach/detach device. 3. Get & Set device attributes. 	Information Maintenance It handles information and its transfer between The OS and the user program. Functions <ol style="list-style-type: none"> 1. Get or Set time & date. 2. Get process & device attributes.
Communication These types of system calls are specially used for inter-process communications. Functions <ol style="list-style-type: none"> 1. Create, delete communication connections. 2. Send, receive messages. 3. Help OS to transfer status information. 4. Attach or detach remote devices. 	

Summary of System Calls

CATEGORIES	WINDOWS	UNIX/LINUX
Process Control	CreateProcess() ExitProcess() WaitForSingleObject()	fork() exit() wait()
Device Manipulation	SetConsoleMode() ReadConsole() WriteConsole()	ioctl() read() write()
File Manipulation	CreateFile() Read File() WriteFile() CloseHandle()	Open() Read() write() close()
Information Maintenance	GetCurrentProcessID() SetTimer() Sleep()	getpid() alarm() sleep()
Communication	CreatePipe() CreateFileMapping() MapViewOfFile()	Pipe() shm_open() mmap()
Protection	SetFileSecurity() IntializeSecurityDescriptor() SetSecurityDescriptorGroup()	Chmod() Umask() Chown()

System Calls Related to Process

There are a lot many Linux system calls available inbuilt for the users. A system call is as good as a function in C Programming Language. It can be compared with 'printf' function in C. The reason that it is often called system call rather than functions is that functions are limited to programming while system calls are specific for operating systems. These system calls perform the task of process creation, process termination, etc. The Linux System calls under this are fork() , exit() , exec().

1. Fork System Call()

In Linux, process is created by duplicating parent process. This is called forking. You invoke the fork system call with fork() function.

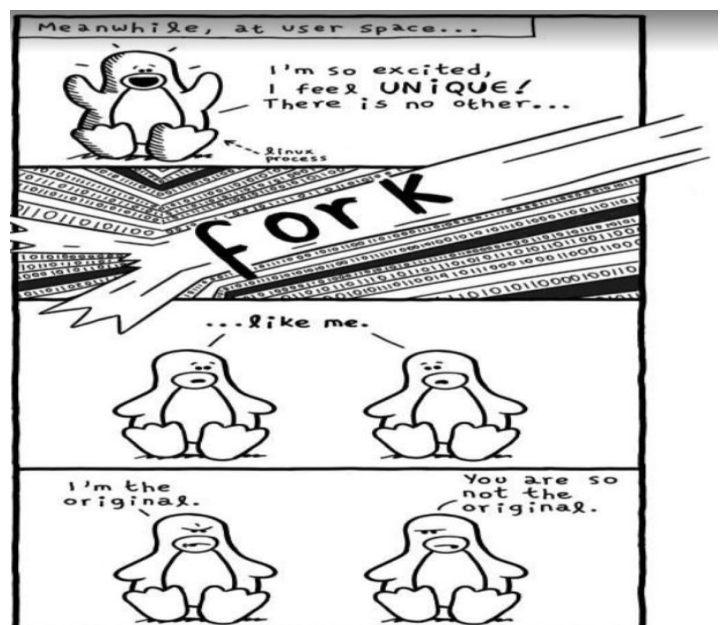
Usually A new process is created by the fork() system call. Process may be created with fork () without a new program being run-the new sub-process simply continues to execute exactly the same program that the first (parent) process was running. It is one of the most widely used system calls under process management.

It is a system call that creates a new process under Linux operating system. It takes no argument. The purpose of fork() is to create a new process which becomes the child process to the caller. After the new child process is created, both processes will execute next instruction following the fork system call, therefore we have to distinguish the parent process from the child which can be done by evaluating the returned value of fork() function.

By examining the returned value of fork function, we can determine the current process is parent or child process. following are the returned value and their meaning. If the returned value is negative, it means that the child process creation was unsuccessful. If the returned value is zero, the child process is created with pid = 0. If the returned value is positive, the child process is created with the process with a process ID to the parent process. The returned process ID is of type pid_t defined in sys.type.h). Normally this process ID is an integer.

After the system call to fork() is issued, a simple test can tell which process is the child. Note that Linux will make an exact copy of the parent address space and give it to the child. Therefore, the parent and child processes have separate address space. Consider the following C language program:

```
1#include<stdio.h>
2#include<sys/types.h>
3#include<unistd.h>
4
5int main() {
6printf("Before Forking \n");
7printf("Creating Child Process\n");
8int i=fork(); //child process will be created & it will execute
9             //the program after fork.
10 if(i==0)
11 {
12printf("Iam Child Process\n");
13}
14 else
15 {
16printf("Iam Parent Process\n");
17}
18
19printf("After Forking\n");
20return 0;
```



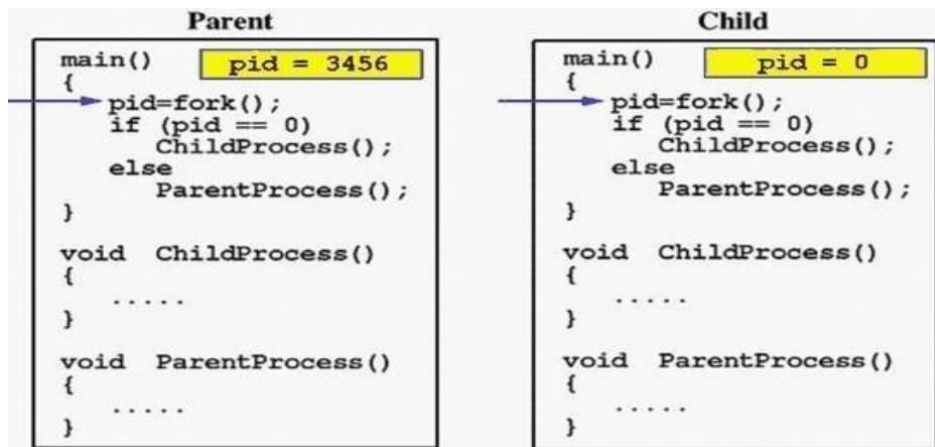
Implementing the above code and check the output.

```
gcc code.c -o out
```

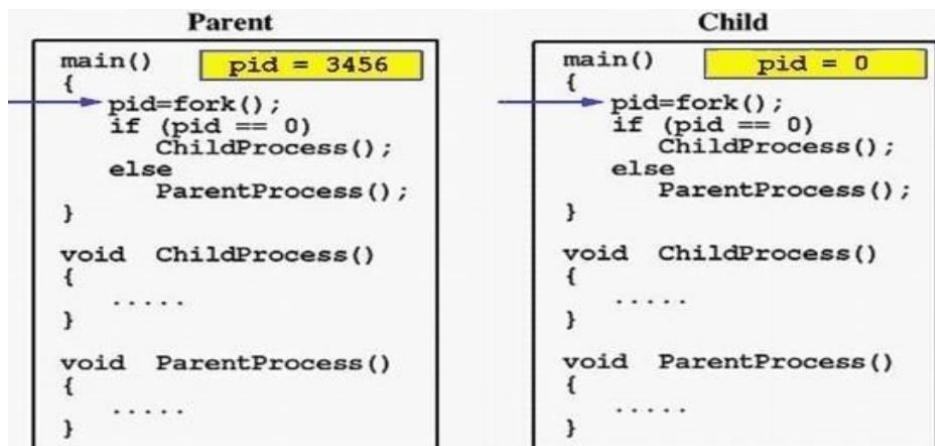
```
./out
```

```
sameer@virtual-machine:~/Desktop/lab04$ gcc code.c -o out
sameer@virtual-machine:~/Desktop/lab04$ ./out
Before Forking
Creating Child Process
Iam Parent Process
After Forking
Iam Child Process
After Forking
sameer@virtual-machine:~/Desktop/lab04$
```

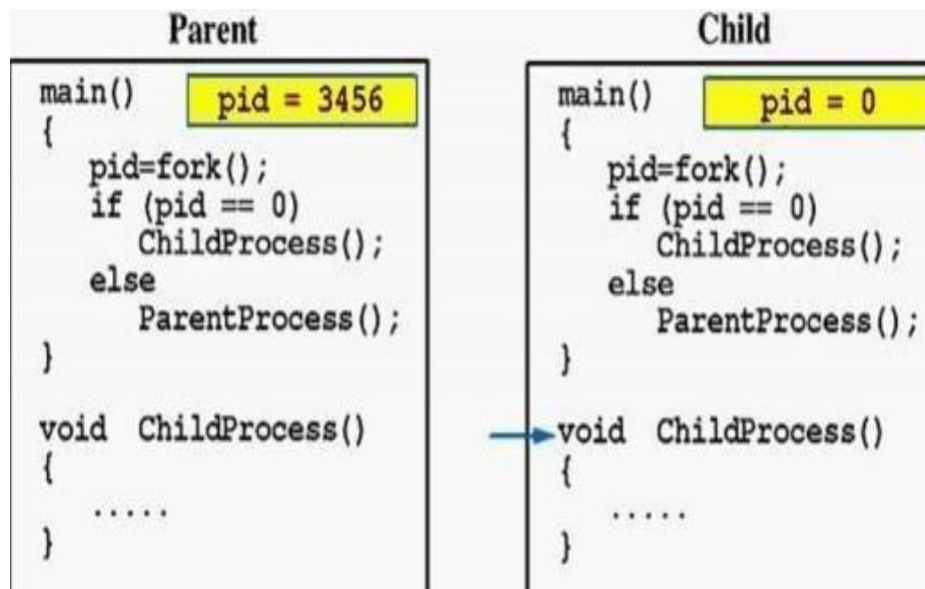
When the main program executes `fork()`, an identical copy of its address space, including the program and all data, is created. System call `fork()` returns the child process ID to the parent and returns 0 to the child process. The images below will diagrammatically show the above code execution of forking:



Now both programs (i.e. the parent and the child) will execute independent of each other starting at the next statement.



In the above image, the fork function is called, which creates a new process and assign value of pid in parent process and assign 0 in child process. During if condition, it checked if the pid is zero or not to distinguish between parent and child process and invoke the functions of each process respectively.



Due to the fact that the CPU scheduler will assign a time quantum to each process, the parent or the child process will run for some time before the control is switched to the other and the running process will print some lines before you can see any line printed by the other process. The following codes distinguishes parent and child process working on variable in shared and separate address spaces: Even though the variable name remain same in child process yet due to separate address of process the variable is considered a new variable in process.

```
#include<stdio.h>
#include <sys/types.h>
#include<unistd.h>
void parent_process(int cvar);
void child_process(int pvar);

int y=10;
int main() {
int x=0;
printf("before forking \n");
printf("creating child process\n");
int i= fork();
if (i==0)
{
child_process(x);
}
else
{
parent_process(x);
}
printf("after forking \n");
return 0;
}
void child_process(int a){
y+=2;
a=3;
printf("the value of child process variable= %d\n",a);
printf("In child process: y=%d\n",y);
}
void parent_process(int b){
b=2;
y+=5;
printf("the value of parent process variable= %d\n",b);
printf("In Parent process: y=%d\n",y); }
```


Implementing the above code and check the output.

```
gcc code1.c -o out1
```

```
./out1
```

```
sameer@virtual-machine:~/Desktop/lab04$ gedit code1.c
sameer@virtual-machine:~/Desktop/lab04$ gcc code1.c -o out1
sameer@virtual-machine:~/Desktop/lab04$ ./out1
Before Forking
Creating Child Process
The value of parent process variable= 2
In parent process: y= 15
After Forking
The value of child process variable= 3
In child process: y= 12
After Forking
sameer@virtual-machine:~/Desktop/lab04$ |
```

System Call to Get Process ID

There are two system calls (functions) which can get the Process ID one is to get the process ID of the current process and another one to get the ID of its parent process. These are:

1. **getpid():** Returns process id of the current process.
2. **getppid():** Returns process id of the parent process.

Class Task: In the above example print the process ID of parent and child process and their parent processes plus child process should also print his/her grandparent process id.

Multiple Child Processes

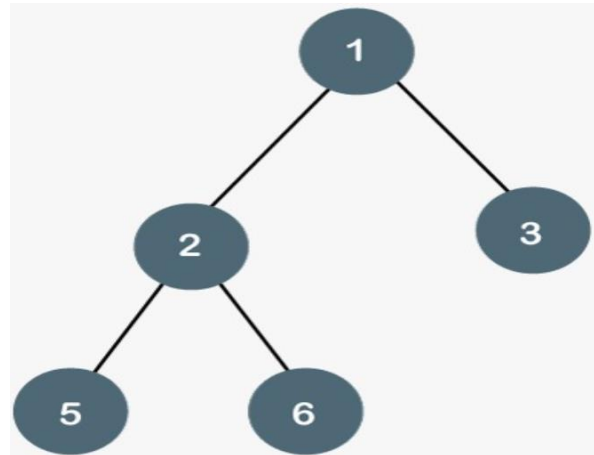
In the following example multiple child are created . The execution sequence may be different in your system as compare to the commented sequence of print.

Let's execute the program and verify the creation of multiple children. Understand the tree.

```
#include<stdio.h>
#include<unistd.h>
int main()
{
    printf("node:1 , pid = %d, ppid =%d\n",getpid(),getppid());
    int i = fork();
    if(i==0){
        printf("node:3 , pid = %d, ppid =%d\n",getpid(),getppid());
    }
    else{
        i = fork();
        if(i==0){
            printf("node:2 , pid = %d, ppid =%d\n",getpid(),getppid());
            i=fork();
            if(i==0){
                printf("node:6 , pid = %d, ppid =%d\n",getpid(),getppid());
            }
            else{
                i=fork();
                if(i==0){
                    printf("node:5 , pid = %d, ppid =%d\n",getpid(),getppid());
                }
            }
        }
    }
}
return 0;
```



```
Node 1, pid =397, ppid=15
Node 3, pid=398, ppid=397
Node 2, pid=399, ppid=14
monis@LAPTOP-CMQQNPQF:~$ Node 6, pid=400, ppid=399
Node 5, pid=401, ppid=399
```



Different Kinds of Child Processes

- **Zombie Process**

Reaping Child Processes

■ Idea

- When process terminates, it still consumes system resources
 - Examples: Exit status, various OS tables
- Called a “zombie”
 - Living corpse, half alive and half dead

■ Reaping

- Performed by parent on terminated child (using `wait` or `waitpid`)
- Parent is given exit status information
- Kernel then deletes zombie child process

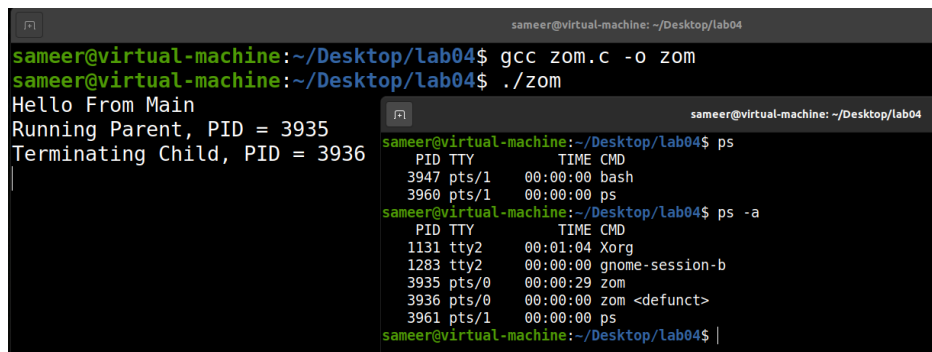
■ What if parent doesn't reap?

- If any parent terminates without reaping a child, then the orphaned child will be reaped by **init** process (`pid == 1`)
- So, only need explicit reaping in long-running processes
 - e.g., shells and servers

Implement the below program and check the output by opening two terminals. In one terminal, you need to execute your zom.c program and in second terminal execute `ps -a` to check the status of child process. As given below.

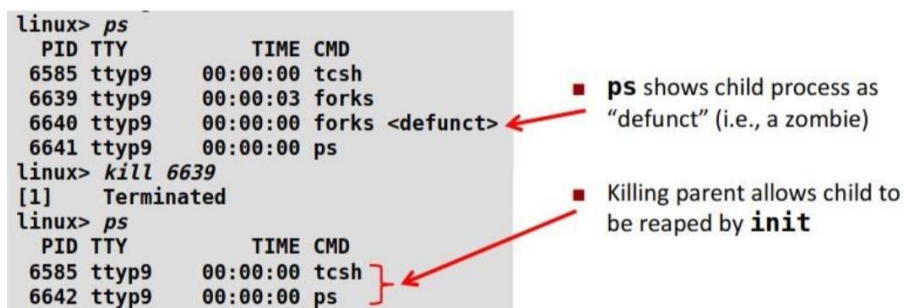
Then find the parent process id and kill the child process.

```
1#include<stdio.h>
2#include<unistd.h>
3#include<sys/types.h>
4#include<stdlib.h>
5
6void forking(){
7    if(fork()==0){
8        /* Child */
9        printf("Terminating Child, PID = %d\n", getpid());
10       exit(0);
11    }
12
13    else{
14        printf("Running Parent, PID = %d\n", getpid());
15        while(1); //Infinite Loop
16    }
17    exit(0);
18 }
19
20
21
22int main(){
23    printf("Hello From Main\n");
24    forking();
25    return 0;
26 }
```



```
sameer@virtual-machine: ~/Desktop/lab04
sameer@virtual-machine:~/Desktop/lab04$ gcc zom.c -o zom
sameer@virtual-machine:~/Desktop/lab04$ ./zom
Hello From Main
Running Parent, PID = 3935
Terminating Child, PID = 3936

sameer@virtual-machine:~/Desktop/lab04$ ps
  PID TTY          TIME CMD
 3947 pts/1        00:00:00 bash
 3960 pts/1        00:00:00 ps
sameer@virtual-machine:~/Desktop/lab04$ ps -a
  PID TTY          TIME CMD
 1131 tty2        00:01:04 Xorg
 1283 tty2        00:00:00 gnome-session-b
 3935 pts/0        00:00:29 zom
 3936 pts/0        00:00:00 zom <defunct>
 3961 pts/1        00:00:00 ps
sameer@virtual-machine:~/Desktop/lab04$
```

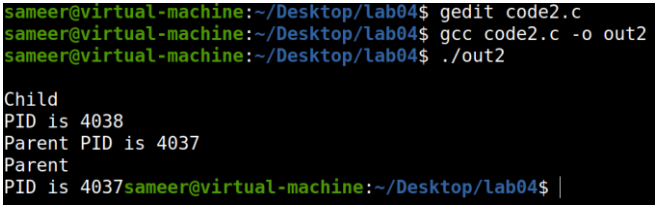
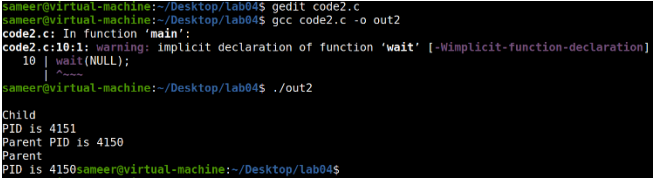


```
linux> ps
  PID TTY          TIME CMD
 6585 ttyp9        00:00:00 tcsh
 6639 ttyp9        00:00:03 forks
 6640 ttyp9        00:00:00 forks <defunct>
 6641 ttyp9        00:00:00 ps
linux> kill 6639
[1]  Terminated
linux> ps
  PID TTY          TIME CMD
 6585 ttyp9        00:00:00 tcsh
 6642 ttyp9        00:00:00 ps

■ ps shows child process as "defunct" (i.e., a zombie)
■ Killing parent allows child to be reaped by init
```

Solutions to Avoid Creation of Zombie Processes

Using wait() system call we can avoid the creation of zombie process. The below changes to the above code will force the parent to wait:

Parent without WAIT();	Parent with WAIT();
<pre>1#include<stdio.h> 2#include<sys/types.h> 3#include<unistd.h> 4 5int main(){ 6 7int pid=fork(); 8 9if(pid>0){ 10sleep(10); 11printf("\nParent"); 12printf("\nPID is %d", getpid()); 13} 14 15if(pid==0){ 16printf("\nChild"); 17printf("\nPID is %d", getpid()); 18printf("\nParent PID is %d", getppid()); 19} 20 21return 0; 22}</pre>  <pre>sameer@virtual-machine:~/Desktop/lab04\$ gedit code2.c sameer@virtual-machine:~/Desktop/lab04\$ gcc code2.c -o out2 sameer@virtual-machine:~/Desktop/lab04\$./out2 Child PID is 4038 Parent PID is 4037 Parent PID is 4037sameer@virtual-machine:~/Desktop/lab04\$ </pre> <p>Parent will sleep for 10 seconds and then it will get executed.</p>	<pre>1#include<stdio.h> 2#include<sys/types.h> 3#include<unistd.h> 4 5int main(){ 6 7int pid=fork(); 8 9if(pid>0){ 10wait(NULL); 11sleep(10); 12printf("\nParent"); 13printf("\nPID is %d", getpid()); 14} 15 16if(pid==0){ 17printf("\nChild"); 18printf("\nPID is %d", getpid()); 19printf("\nParent PID is %d", getppid()); 20} 21 22return 0; 23}</pre>  <pre>sameer@virtual-machine:~/Desktop/lab04\$ gedit code2.c sameer@virtual-machine:~/Desktop/lab04\$ gcc code2.c -o out2 code2.c: In function 'main': code2.c:10:1: warning: implicit declaration of function 'wait' [-Wimplicit-function-declaration] 10 wait(NULL); ~~~ sameer@virtual-machine:~/Desktop/lab04\$./out2 Child PID is 4151 Parent PID is 4150 Parent PID is 4150sameer@virtual-machine:~/Desktop/lab04\$</pre> <p>The parent process waits for the child process to terminate. The wait() system call suspends the execution of the parent process until any of its child processes terminate.</p>

What happens when the main make-zombie program ends when the parent process exits, without ever calling wait? Does the zombie process stay around? No—try running ps again, and note that both of the make-zombie processes are gone.

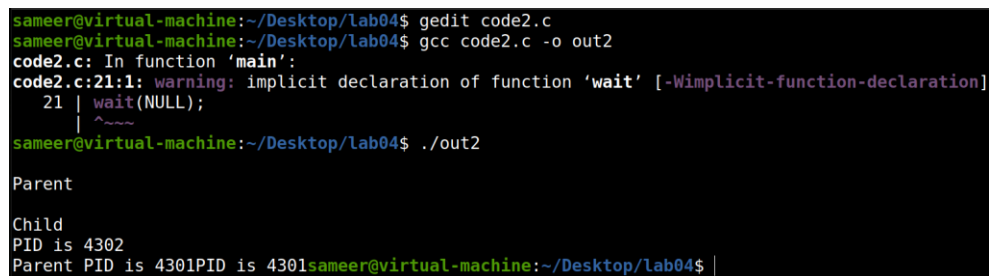
When a program exits, its children are inherited by a special process, the init program, which always runs with process ID of 1 (it's the first process started when Linux boots). The init process automatically cleans up any zombie child processes that it inherits. Implement the above program and check the output.

Orphan Process

In general English terms, orphan is someone who lost parents. Same is the story here. If the parent process has finished execution and exited, but at the same time if the child process remains UN-executed, the child is then termed to be an orphan. This is done by making the child process sleep for sometimes. By that time of child's sleep, parent process will complete its execution and will exit. Since, parent process is no more there, child is referred to be an orphan now.

```
1#include<stdio.h>
2#include<sys/types.h>
3#include<unistd.h>
4
5int main(){
6
7int pid=fork();
8
9if(pid>0){
10sleep(1);
11printf("\nParent");
12printf("\nPID is %d", getpid());
13}
14
15if(pid==0){
16sleep(5)
17printf("\nChild");
18printf("\nPID is %d", getpid());
19printf("\nParent PID is %d", getppid());
20}
21wait(NULL);
22return 0;
23}
```

Implement the given below program and check the child process with `ps -al` command.



```
sameer@virtual-machine:~/Desktop/lab04$ gedit code2.c
sameer@virtual-machine:~/Desktop/lab04$ gcc code2.c -o out2
code2.c: In function 'main':
code2.c:21:1: warning: implicit declaration of function 'wait' [-Wimplicit-function-declaration]
 21 | wait(NULL);
    | ^~~~~
sameer@virtual-machine:~/Desktop/lab04$ ./out2

Parent

Child
PID is 4302
Parent PID is 4301PID is 4301sameer@virtual-machine:~/Desktop/lab04$ |
```

2. Execute System Call `exec()`

Fork allow you to create a process by duplicating the process of the current program, that is from whom it is called.

However, limitation arises when you wish to execute a different program and this is where execute system call come in handy!

The **exec()** family of functions creates a new process image from a regular, executable file. This file is either an executable object file, or an interpreter script. There is no return from a successful call to an `exec()` function, because the calling process is functionally replaced by the new process.

In other words A new program will start executing after a call to `exec()`. Running a new program does not require that a new process be created first: any process may call `exec()` at any time. The currently running

program is immediately terminated, and the new program starts executing in the context of the existing process.

The arguments specified by a program with an `exec()` function are passed on to the new process image in the corresponding `main()` arguments.

`int execl(const char *path, const char *arg0, ..., const char *argn, (char *)0);`

path: Specifies the path name of the new process image file.

arg0, ..., argn: Point to null-terminated character strings. These strings constitute the argument list for the new process image. The list is terminated by a NULL pointer. The argument `arg0` should point to a file name that is associated with the process being started by the `exec()` function.

Last argument: is passed null as the function passes string.

The `exit()` system call is used by a program to terminate its execution. The operating system reclaims resources that were used by the process after the `exit()` system call.

```
1#include<stdio.h>
2#include<sys/types.h>
3#include<unistd.h>
4
5int main(){
6execl("/bin/ls", "ls", (char*)0);
7/* We can only reach this code
8if execl returned with an error */
9
10perror("execl");
11
12return 0;
13}
```

By executing the above code, you should get output of current directory files.

```
sameer@virtual-machine:~/Desktop/lab04$ touch exec.c
sameer@virtual-machine:~/Desktop/lab04$ gedit exec.c
sameer@virtual-machine:~/Desktop/lab04$ gcc exec.c -o ex
sameer@virtual-machine:~/Desktop/lab04$ ./ex
code1.c code2.c code.c ex exec.c out out1 out2 zom zom.c
sameer@virtual-machine:~/Desktop/lab04$
```

To avoid the replacement of current process, we can use fork and create child process which will be executing the other execution units.

```
#include <sys/types.h>
#include <unistd.h>
#include <stdio.h>
#include <stdlib.h>

int main(void) {
    int PID;
    char cmd[256];
    Printf("Press e if you want to terminate\n");
    while (1) {
        printf("cmd: ");
        scanf("%s",cmd);
        if ( strcmp(cmd,"e")==0) /* loop terminates if type 'e'*/
            exit(0);
        /* creates a new process. Parent gets the process ID. Child gets 0 */
        if ((PID=fork()) > 0)
            wait(NULL);
        else if (PID == 0) /* child process */
        {
            execlp (cmd,cmd,NULL);
            /* exec cannot return. If so do the following */
            fprintf (stderr, "Cannot execute %s\n", cmd);
            exit(1); /* exec failed */
        }
        else if ( PID == -1)
        {
            fprintf (stderr, "Cannot create a new process\n");
            exit (2);
        }
    }
}
```

Execute the above example and find the output, understand how it works.