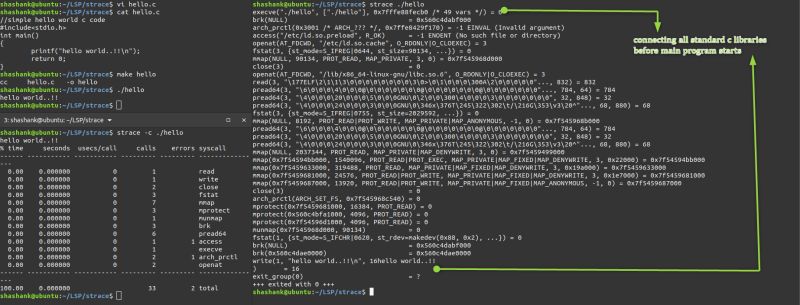
**strace in linux:**   
strace stands for system call tracer. It is a debugging tool used to monitor the system calls used by a program and all the signals it receives.  
  
**What strace does?**1. Learn which system calls a program makes  
2. Finding those system calls which fails with error code  
3. Finding which files a program opens  
4. Finding out what system calls a running program is making.  
  
**Usage:**   
There are couple of ways to use strace  
Method:1  
# **strace <program\_name>**Ex: strace ls or strace pwd  
Method:2  
# **strace -p <Pid\_of\_the\_running\_process>**Ex: strace -p 22145  
  
calls between execve() and write():  
They take care of connecting all standard c libraries before main program starts. They basically setup a runtime.   
  
Generating statistics for system calls:  
sometimes we want to look only at what system calls were made by the program and identify the most commonly used system calls by the program.  
  
We can do it by using the -c option of strace which provides the summary info on executing program.  
**Usage:   
# strace -c <executable\_name>**



Using **strace -e** option we can also specify which system calls to be traced.  
  
for example to trace only open() and close() syscalls we can use the command as  
# **strace -e trace='open, close' <executable\_name>**  
to not trace specific system calls we can use negation  
# strace -e trace='!open,close' <executable\_name>  
  
Track by specific system call groups:  
  
# **strace -e trace=ipc => to track the communication between process**  
**# strace -e trace=network => to track network syscalls**  
**# strace -e trace=memory => to track memory related syscalls  
# strace -e trace=process => track process related calls**

