To trace Api calls and behaviour of files:

I have used remnux to trace api calls.

Remnux is used for malware analysis. It includes a variety of tools that can be used for tracing API calls in an application. To trace API calls in remnux you can use Strace tool. Strace is a command line tool that is used for tracing system calls and signals made by a program.

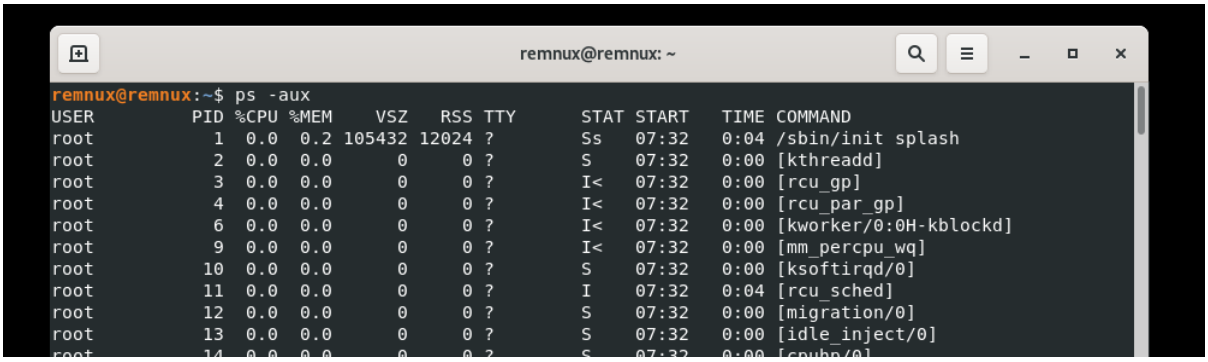
To use the command, first install the command:

sudo apt-get install strace

Identify the pid that you want to trace. To do that you need to type ps- aux to get all the processes that are running in the system.

We are considering to trace the Firefox application. To get the pid of the Firefox application we use pgrep Firefox.

Pic-1.0



The pid of the Firefox application is 29680.

Once the process Id is known you should run the strace command using -p to attach to the process.

We have to type:

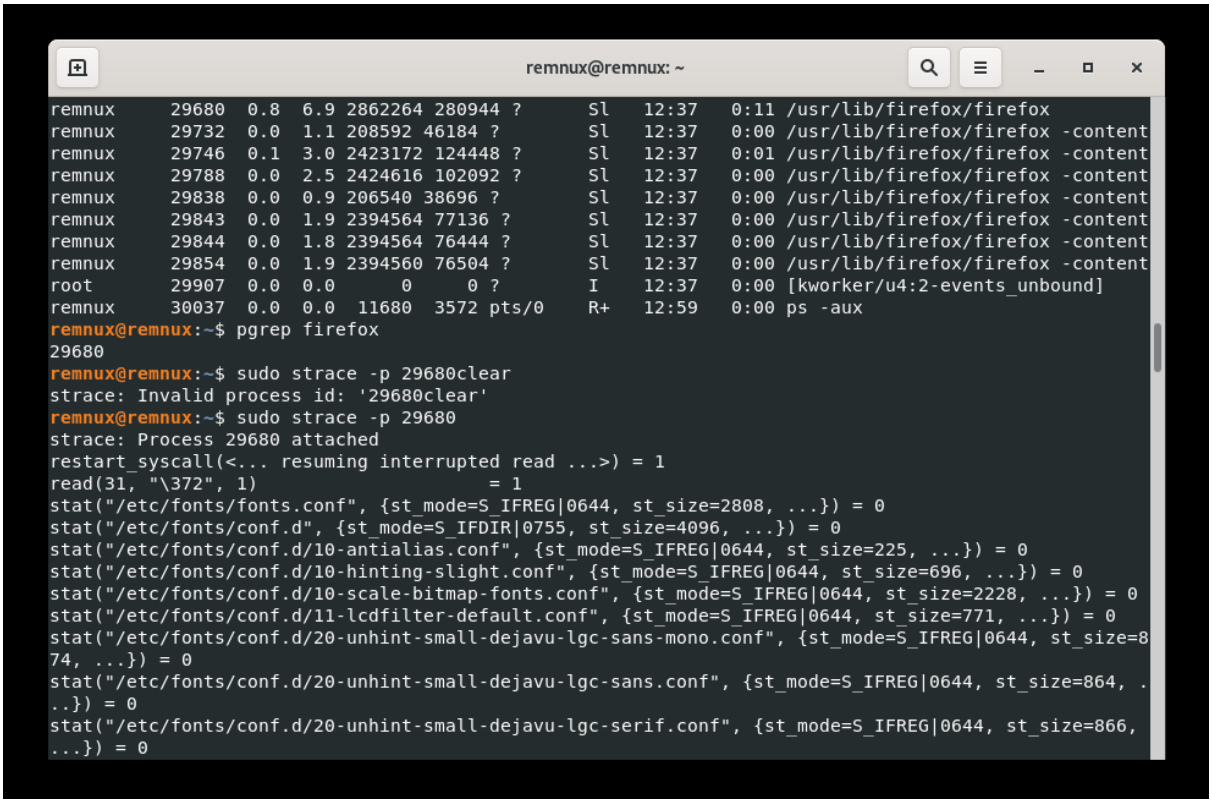
strace -p <pid of the application>

for the firefox it is 29680.

strace -p 29680

when we run this command, the tracing starts and continues till you interrupt or keeps giving the trace data.

Pic-1.1


remnux@remnux: ~
remnux 29680 0.8 6.9 2862264 280944 ? Sl 12:37 0:11 /usr/lib/firefox/firefox
remnux 29732 0.0 1.1 208592 46184 ? Sl 12:37 0:00 /usr/lib/firefox/firefox -content
remnux 29746 0.1 3.0 2423172 124448 ? Sl 12:37 0:01 /usr/lib/firefox/firefox -content
remnux 29788 0.0 2.5 2424616 102092 ? Sl 12:37 0:00 /usr/lib/firefox/firefox -content
remnux 29838 0.0 0.9 206540 38696 ? Sl 12:37 0:00 /usr/lib/firefox/firefox -content
remnux 29843 0.0 1.9 2394564 77136 ? Sl 12:37 0:00 /usr/lib/firefox/firefox -content
remnux 29844 0.0 1.8 2394564 76444 ? Sl 12:37 0:00 /usr/lib/firefox/firefox -content
remnux 29854 0.0 1.9 2394560 76504 ? Sl 12:37 0:00 /usr/lib/firefox/firefox -content
root 29907 0.0 0.0 0 0 ? I 12:37 0:00 [kworker/u4:2-events_unbound]
remnux 30037 0.0 0.0 11680 3572 pts/0 R+ 12:59 0:00 ps -aux
remnux@remnux:~$ pgrep firefox
29680
remnux@remnux:~$ sudo strace -p 29680clear
strace: Invalid process id: '29680clear'
remnux@remnux:~$ sudo strace -p 29680
strace: Process 29680 attached
restart_syscall(<... resuming interrupted read ...>) = 1
read(31, "\372", 1) = 1
stat("/etc/fonts/fonts.conf", {st_mode=S_IFREG|0644, st_size=2808, ...}) = 0
stat("/etc/fonts/conf.d", {st_mode=S_IFDIR|0755, st_size=4096, ...}) = 0
stat("/etc/fonts/conf.d/10-antialias.conf", {st_mode=S_IFREG|0644, st_size=225, ...}) = 0
stat("/etc/fonts/conf.d/10-hinting-slight.conf", {st_mode=S_IFREG|0644, st_size=696, ...}) = 0
stat("/etc/fonts/conf.d/10-scale-bitmap-fonts.conf", {st_mode=S_IFREG|0644, st_size=2228, ...}) = 0
stat("/etc/fonts/conf.d/11-lcdfilter-default.conf", {st_mode=S_IFREG|0644, st_size=771, ...}) = 0
stat("/etc/fonts/conf.d/20-unhint-small-dejavu-lgc-sans-mono.conf", {st_mode=S_IFREG|0644, st_size=8
74, ...}) = 0
stat("/etc/fonts/conf.d/20-unhint-small-dejavu-lgc-sans.conf", {st_mode=S_IFREG|0644, st_size=864, .
..}) = 0
stat("/etc/fonts/conf.d/20-unhint-small-dejavu-lgc-serif.conf", {st_mode=S_IFREG|0644, st_size=866,
...}) = 0