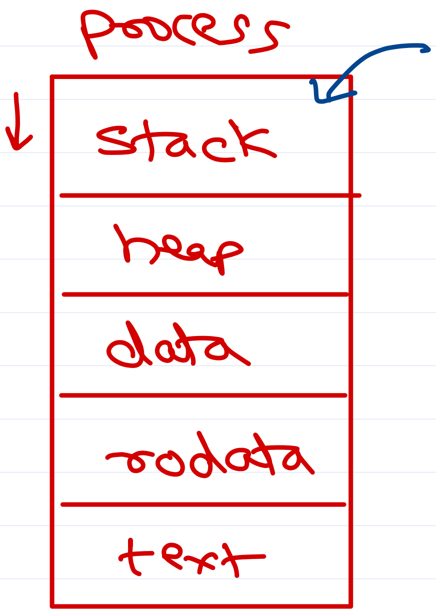
Embedded Operating Systems

Trainer: Nilesh Ghule

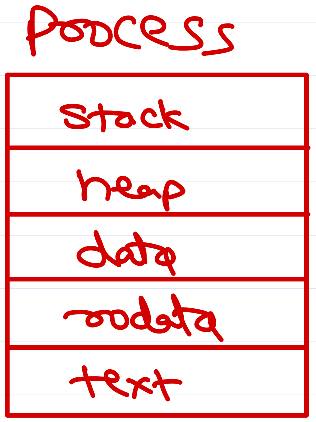
Kernel stack



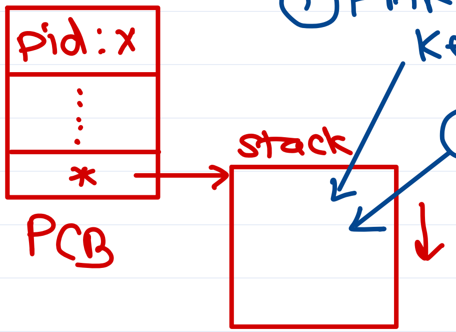
FAR of called fns

↓

user defined fns or lib fns.

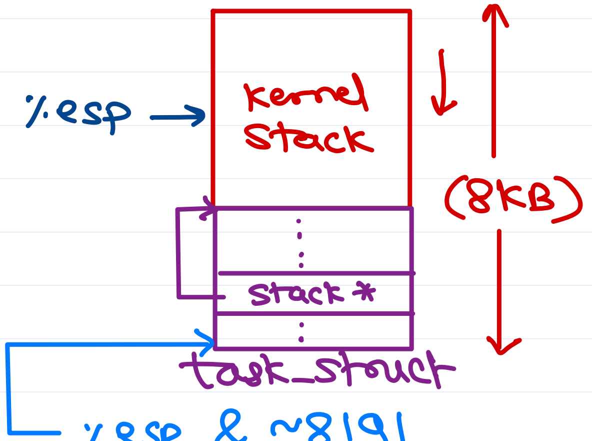


Process
stack
heap
data
rodata
text

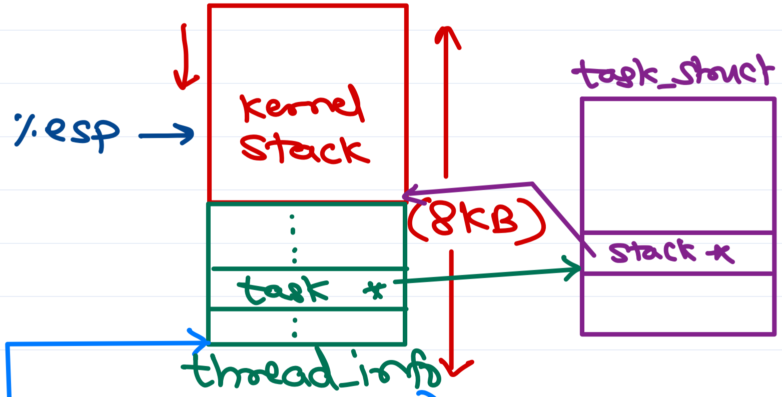


① FAR of called fns
Kernel fns

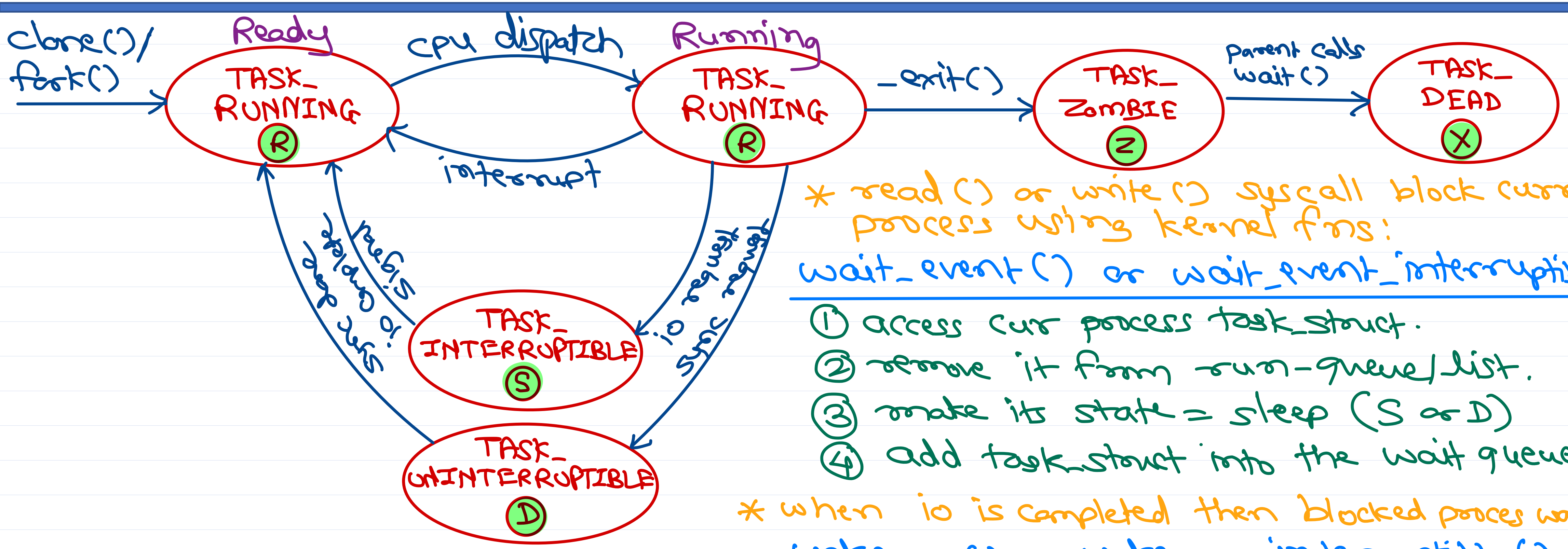
② Store exec ctx
when interrupt
arrives.



%esp & ~8191
(pointer to current
process's task_struct).



(%esp & ~8191)
(%esp & ~8195) → task
(pointer to current
process's task_struct).



* read() or write() syscall block current process using kernel fns:

wait_event() or wait_event_interruptible()

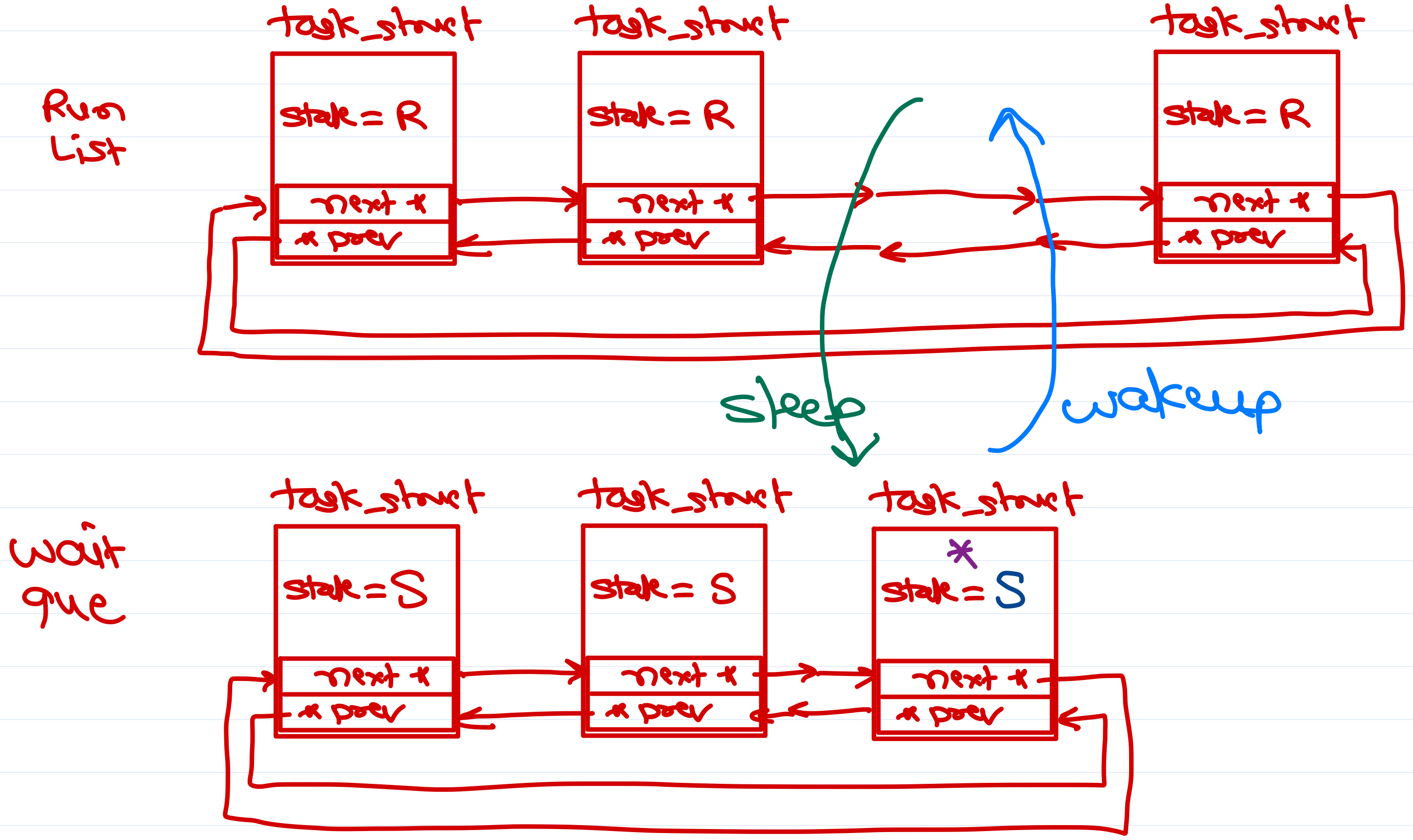
1. access cur process task_struct.
2. remove it from run-queue/list.
3. make its state = sleep (S or D)
4. add task_struct into the wait queue.

* when io is completed then blocked proces wake up

wake_up() or wake_up_interruptible()

1. get task_struct of blocked process (from wait que)
2. remove it from wait_queue.
3. make its state = ready (R).
4. add task_struct into the run queue/list.

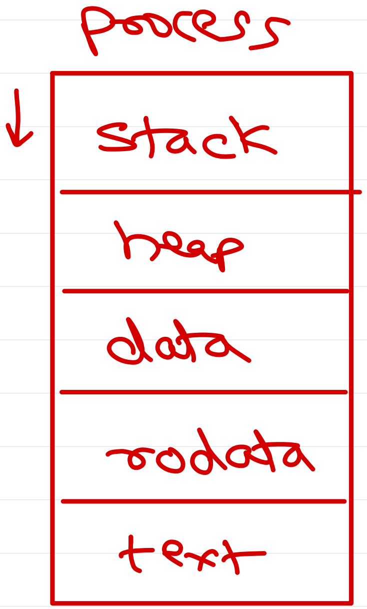
Sleep and Wakeup

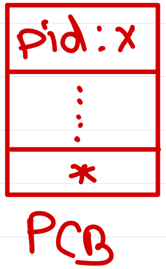


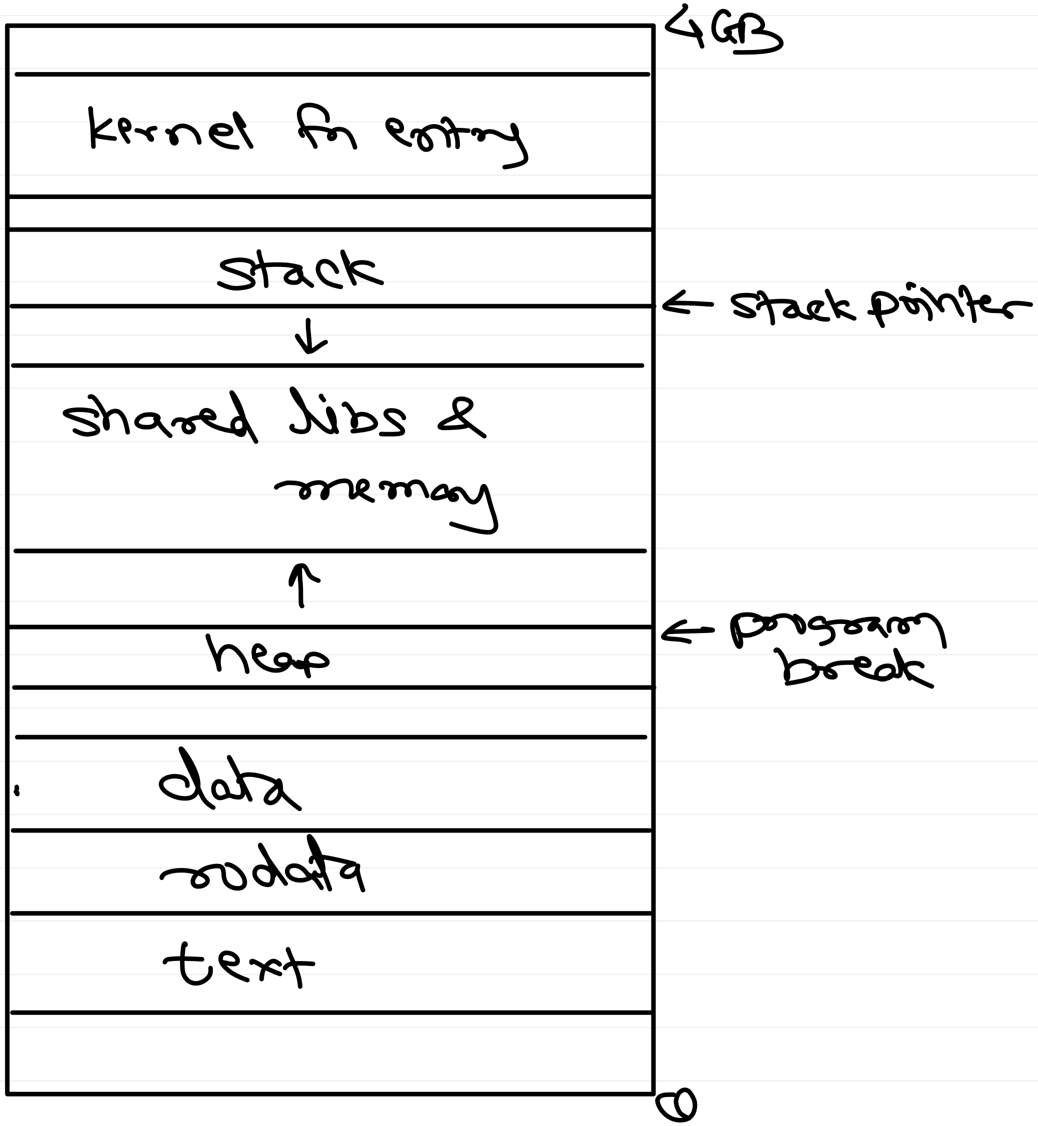
Process sections

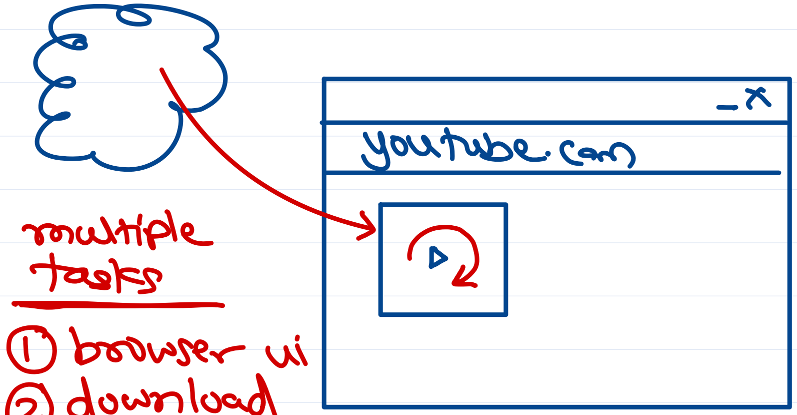
Process memory layout

```
cmd> cat /proc/pid/maps
```







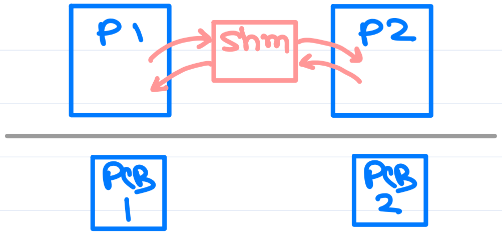


multiple tasks

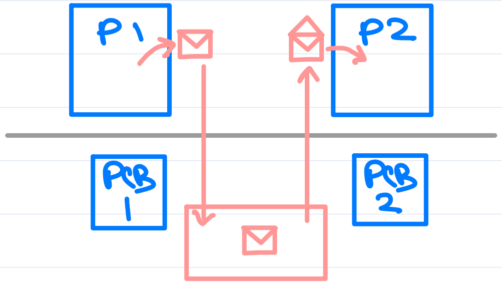
1. browser ui
2. download
3. play

IPC models

1. shared mem model



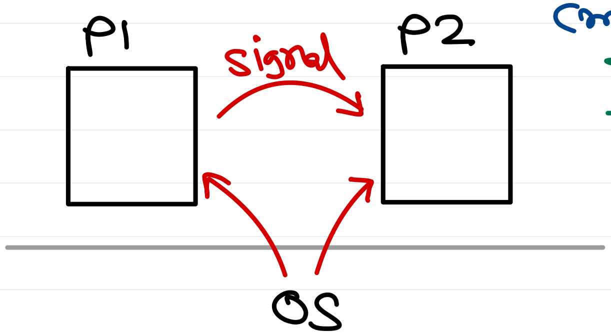
2. message passing model



Linux IPC

1. signals
2. message queue
3. pipe
4. socket
5. shared memory

Signals

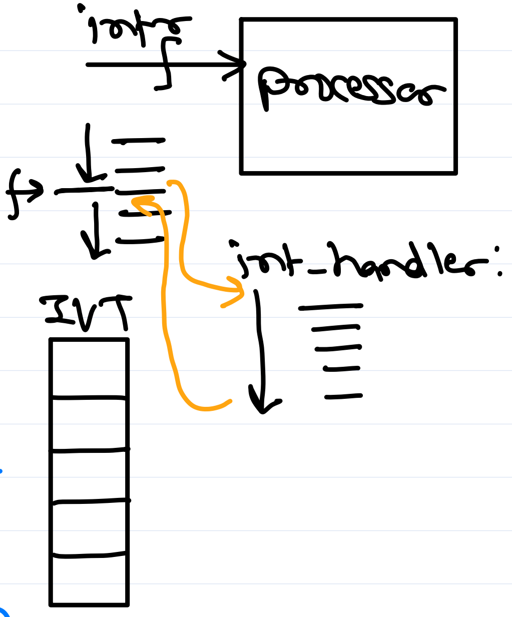


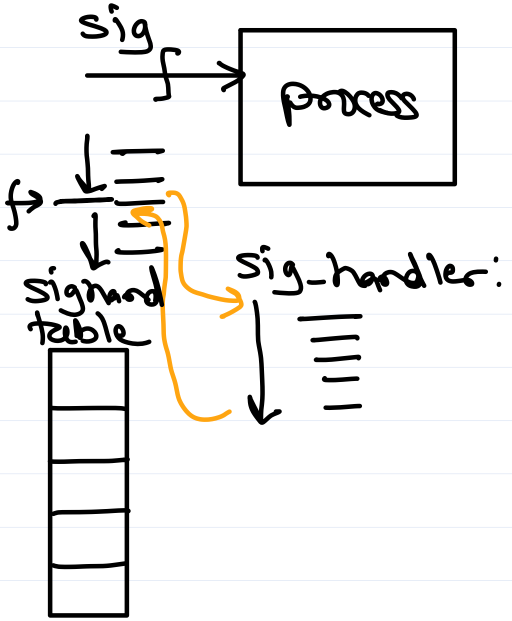
cmd> man 7 signal

To send a signal

```
cmd> kill -sig pid
cmd> pkill -sig proc-name
ret = kill(pid, signum);
```

Signals are software counterparts of hardware interrupts.





Important signals

② SIGINT → ctrl+c
⑮ SIGTERM → during OS shutdown
⑨ SIGKILL →
⑪ SIGSEGV → Seg Fault → ② Core
⑲ SIGSTOP → ctrl+s → ③ Stop
⑱ SIGCONT → ctrl+q → ④ Cont
⑰ SIGCHLD → child term. → ⑤ Ign

signal's default action

① Term
② Core
③ Stop
④ Cont
⑤ Ign

To receive a signal

① implement sig handler
② register sig handler (in sig table).

```
signal(signum, sig_hand_fn);
```

signum ↓ int
sig_hand_fn ↓ fn ptr

Two signals cannot be handled.
ⓐ SIGKILL ⓑ SIGSTOP

Thank you!

Nilesh Ghule <nilesh@sunbeaminfo.com>