운영체제

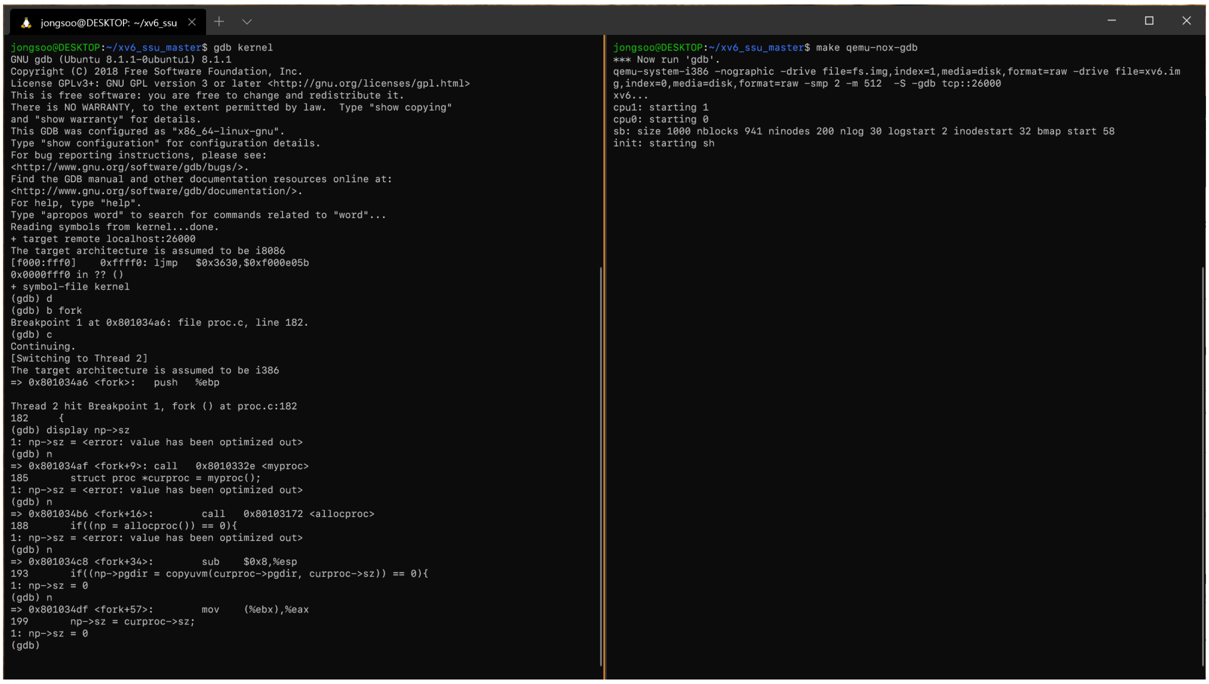
HW#3

Get the Process Size with GDB

학　과 : 스마트시스템소프트웨어학과

이　름 : 20170404 한종수

제출일 : 2021. 03. 22



```
jongsoo@DESKTOP:~/xv6_ssu_master$ gdb kernel
GNU gdb (Ubuntu 8.1.1-0ubuntu1) 8.1.1
Copyright (C) 2018 Free Software Foundation, Inc.
License GPLv3+: GNU GPL version 3 or later <http://gnu.org/licenses/gpl.html>
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.  Type "show copying"
and "show warranty" for details.
This GDB was configured as "x86_64-linux-gnu".
Type "show configuration" for configuration details.
For bug reporting instructions, please see:
<http://www.gnu.org/software/gdb/bugs/>.
Find the GDB manual and other documentation resources online at:
<http://www.gnu.org/software/gdb/documentation/>.
For help, type "help".
Type "apropos word" to search for commands related to "word"...
Reading symbols from kernel...done.
+ target remote localhost:26000
The target architecture is assumed to be i8086
[f000:fff0]    0xffff0: ljmp   $0x3630,$0xf000e05b
0x0000fff0 in ?? ()
+ symbol-file kernel
(gdb) d
(gdb) b fork
Breakpoint 1 at 0x801034a6: file proc.c, line 182.
(gdb) c
Continuing.
[Switching to Thread 2]
The target architecture is assumed to be i386
=> 0x801034a6 <fork>:   push   %ebp

Thread 2 hit Breakpoint 1, fork () at proc.c:182
182     {
(gdb) display np->sz
1: np->sz = <error: value has been optimized out>
(gdb) n
=> 0x801034af <fork+9>: call   0x8010332e <myproc>
185       struct proc *curproc = myproc();
1: np->sz = <error: value has been optimized out>
(gdb) n
=> 0x801034b6 <fork+16>:        call   0x80103172 <allocproc>
188       if((np = allocproc()) == 0){
1: np->sz = <error: value has been optimized out>
(gdb) n
=> 0x801034c8 <fork+34>:        sub    $0x8,%esp
193       if((np->pgdir = copyuvm(curproc->pgdir, curproc->sz)) == 0){
1: np->sz = 0
(gdb) n
=> 0x801034df <fork+57>:        mov    (%ebx),%eax
199       np->sz = curproc->sz;
1: np->sz = 0
(gdb)
```

```
jongsoo@DESKTOP:~/xv6_ssu_master$ make qemu-nox-gdb
*** Now run 'gdb'.
qemu-system-i386 -nographic -drive file=fs.img,index=1,media=disk,format=raw -drive file=xv6.im
g,index=0,media=disk,format=raw -smp 2 -m 512  -S -gdb tcp::26000
xv6...
cpu1: starting 1
cpu0: starting 0
sb: size 1000 nblocks 941 ninodes 200 nlog 30 logstart 2 inodestart 32 bmap start 58
init: starting sh
```

Screenshot GDB