

Ahmet Miles Putun
Project 1 Report
Dr. Urgaonkar
06/26/2021

Prog1

1) Stack, Heap and System Calls

- a) In address 1 section that is being recursively printing the new addresses, the addresses extend towards the 0x7ffe00000000, leaning towards 0x0000 direction. Address 1 refers to local variables and the data structure stored in is stack.
In address 2 section that is being recursively printing the new addresses, the addresses go towards the 0x16ff, growing towards 0xffff direction. Address 2 refers to dynamically allocated variables and the data structured stored in is heap.

```
~/Desktop -- ssh azp5611@e5-cse-204-12.cse.psu.edu -- 109x24
[e5-cse-204-12.cse.psu.edu 205% ls
Makefile prog1 prog1.c
[e5-cse-204-12.cse.psu.edu 206% ./prog1
Address 1 = 0x7ffe07360f0      Address 2 = 0x16fb010
Address 1 = 0x7ffe0705b50      Address 2 = 0x16fb010
Address 1 = 0x7ffe06d55b0      Address 2 = 0x16fb010
Address 1 = 0x7ffe06a5010      Address 2 = 0x16fb010
Address 1 = 0x7ffe0674470      Address 2 = 0x16fb010
Address 1 = 0x7ffe06444d0      Address 2 = 0x16fb010
Address 1 = 0x7ffe0613f30      Address 2 = 0x16fb010
Address 1 = 0x7ffe05e3990      Address 2 = 0x16fb010
Address 1 = 0x7ffe05b33f0      Address 2 = 0x16fb010
Address 1 = 0x7ffe0582e50      Address 2 = 0x16fb010
Enter anyxx key to exit
x
```

- b) For this question, while running the program in a separate terminal, do pidof prog1, and get pid, then display process details with /proc/pid/smaps
Stack size is 2140 KB.

```
~/Desktop -- ssh azp5611@e5-cse-204-12.cse.psu.edu -- 173x31
[Shared_Clean: 0 kB
Shared_Dirty: 0 kB
Private_Clean: 0 kB
Private_Dirty: 4 kB
Referenced: 4 kB
Anonymous: 4 kB
AnonHugePages: 0 kB
Swap: 0 kB
KernelPageSize: 4 kB
MMUPageSize: 4 kB
Locked: 0 kB
VmFlags: rd wr mr mp ms ac sd
7ffdbe355800-7ffdbe5ca000 r-xp 00000000 00:00 0 [stack]
Size: 2140 kB
Rss: 72 kB
Pss: 72 kB
Shared_Clean: 0 kB
Shared_Dirty: 0 kB
Private_Clean: 0 kB
Private_Dirty: 72 kB
Referenced: 72 kB
Anonymous: 72 kB
AnonHugePages: 0 kB
Swap: 0 kB
KernelPageSize: 4 kB
MMUPageSize: 4 kB
Locked: 0 kB
VmFlags: rd wr mr mp ms gd ac
7ffdbe5ca000-7ffdbe5ca000 r-xp 00000000 00:00 0 [vds0]
Size: 8 kB
Rss: 4 kB]
```

c) Heap size is 132 KB.

```
-/Desktop - ssh azp5611@e5-cse-204-12.cse.psu.edu - 173x31
Shared_Clean:      0 kB
Shared_Dirty:      0 kB
Private_Clean:     0 kB
Private_Dirty:     4 kB
Referenced:        4 kB
Anonymous:         4 kB
AnonHugePages:     0 kB
Swap:              0 kB
KernelPageSize:    4 kB
MMUPageSize:       4 kB
Locked:             0 kB
VmFlags: rd wr mr mp me dw ac sd
00b36000-00b57000 rw-p 00000000 00:00 0 [heap]
Size:           132 kB
Rss:            8 kB
Pss:            8 kB
Shared_Clean:     0 kB
Shared_Dirty:      0 kB
Private_Clean:     0 kB
Private_Dirty:     8 kB
Referenced:        8 kB
Anonymous:         8 kB
AnonHugePages:     0 kB
Swap:              0 kB
KernelPageSize:    4 kB
MMUPageSize:       4 kB
Locked:             0 kB
VmFlags: rd wr mr mp me ac sd
7fc84c46000-7fc84c20a000 r-xp 00000000 fd:00 537238551
Size:           1988 kB
```

d) Limits -> Stack: 7ffd5e355000 - 7ffd5e56c000

-> Heap: 00b36000 - 00b57000

```
[e5-cse-204-12.cse.psu.edu 218% cat /proc/21321/limits
cat: /proc/21321/limits: No such file or directory
[e5-cse-204-12.cse.psu.edu 219% pidof prog1
22228
[e5-cse-204-12.cse.psu.edu 220% cat /proc/22228/limits
limits                                Soft Limit          Hard Limit          Units
Max CPU time                            unlimited          unlimited          seconds
Max file size                           unlimited          unlimited          bytes
Max data size                           unlimited          unlimited          bytes
Max stack size                          8388608          unlimited          bytes
Max core file size                     0                unlimited          bytes
Max resident set                       unlimited          unlimited          bytes
Max processes                          4096             63052            processes
Max open files                         1024             4096             files
Max locked memory                     65536            65536            bytes
Max address space                     unlimited          unlimited          bytes
Max file locks                        unlimited          unlimited          locks
Max pending signals                  63052            63052            signals
Max pseudoterminals                   819200           819200           bytes
Max nice priority                     0                0
Max realtime priority                 0                0
Max realtime timeout                  unlimited          unlimited          us
[e5-cse-204-12.cse.psu.edu 221% cat /proc/22228/maps
00490000-004a1000 r-xp 00000000 00:29 11141180
00600000-00601000 r--p 00000000 00:29 11141180
00601000-00602000 rw-p 00001000 00:29 11141180
00b36000-00b57000 rw-p 00000000 00:00 0 [heap]
7fc84c46000-7fc84c20a000 r-xp 00000000 fd:00 537238551
7fc84c20a000-7fc84c469000 ---p 001c4000 fd:00 637238551
7fc84c469000-7fc84c48d000 r--p 001c3000 fd:00 537238551
7fc84c48d000-7fc84c48f000 rw-p 001c7000 fd:00 537238551
7fc84c48f000-7fc84c414000 rw-p 00000000 00:00 0
7fc84c414000-7fc84c436000 r-xp 00000000 fd:00 537240869
7fc84c51f000-7fc84c602000 rw-p 00000000 00:00 0
7fc84c532000-7fc84c635000 rw-p 00000000 00:00 0
7fc84c535000-7fc84c636000 r--p 00021000 fd:00 537240869
7fc84c636000-7fc84c637000 rw-p 00022000 fd:00 537240869
7fc84c637000-7fc84c638000 rw-p 00000000 00:00 0
7ffdb5e35000-7ffdb5e56c000 rw-p 00000000 00:00 0 [stack]
7ffdb5e56000-7ffdb5e5ca000 r-xp 00000000 00:00 0 [vds0]
ffffffffff600000-ffffffffff601000 r-xp 00000000 00:00 0 [vsyscall]
[e5-cse-204-12.cse.psu.edu 222%
```

```
[e5-cse-204-12.cse.psu.edu 221% cat /proc/22228/maps
00490000-004a1000 r-xp 00000000 00:29 11141180
00600000-00601000 r--p 00000000 00:29 11141180
00601000-00602000 rw-p 00001000 00:29 11141180
00b36000-00b57000 rw-p 00000000 00:00 0 [heap]
7fc84c46000-7fc84c20a000 r-xp 00000000 fd:00 537238551
7fc84c20a000-7fc84c469000 ---p 001c4000 fd:00 637238551
7fc84c469000-7fc84c48d000 r--p 001c3000 fd:00 537238551
7fc84c48d000-7fc84c48f000 rw-p 001c7000 fd:00 537238551
7fc84c48f000-7fc84c414000 rw-p 00000000 00:00 0
7fc84c414000-7fc84c436000 r-xp 00000000 fd:00 537240869
7fc84c51f000-7fc84c602000 rw-p 00000000 00:00 0
7fc84c532000-7fc84c635000 rw-p 00000000 00:00 0
7fc84c535000-7fc84c636000 r--p 00021000 fd:00 537240869
7fc84c636000-7fc84c637000 rw-p 00022000 fd:00 537240869
7fc84c637000-7fc84c638000 rw-p 00000000 00:00 0
7ffdb5e35000-7ffdb5e56c000 rw-p 00000000 00:00 0 [stack]
7ffdb5e56000-7ffdb5e5ca000 r-xp 00000000 00:00 0 [vds0]
ffffffffff600000-ffffffffff601000 r-xp 00000000 00:00 0 [vsyscall]
[e5-cse-204-12.cse.psu.edu 222%
```

e) Strace command

- According to man strace command, strace intercepts and records the system calls which are called by a process and the signals which are received by a process

Execve: executes the program “./prog1, [“prog1”]

Brk: it is a call to change the location of the program break. Apparently, if you do increase it, it has an effect of allocating more memory to the given process, the deallocation for decreasement. First it is defined to be NULL as it starts.

Mmap: it is a system call that maps files or devices into memory. And according to Wikipedia, “it implements demand paging because file contents are not read from disk directly and initially do not use physical RAM at all”.

Open: Allocates resources associated with the file descriptor and returns a handle that the process will use to refer to that file.

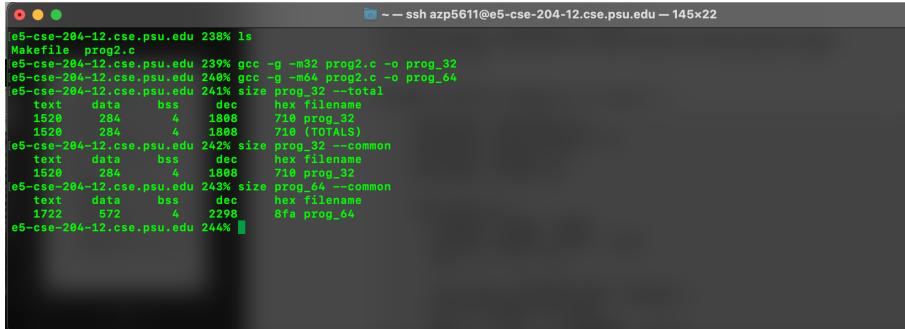
Stat: It returns the information about a file. Fstat is similar to retrieving information about a file.

Access: checks whether the calling process can access the file path.

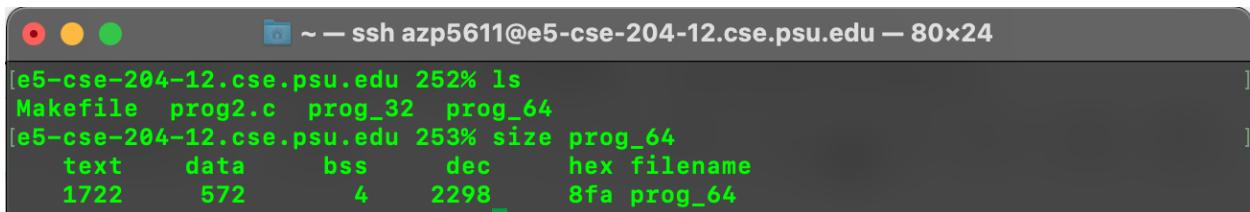
Close: closes a file descriptor

2) Debugging Refresher

- a) i) For prog_32 (32 bits exec), size of compiled code in “text” is 1520 and size of compiled code for prog_64 (64 bits exec), size of compiled code in “text” is 1722.



```
e5-cse-204-12.cse.psu.edu 238% ls
Makefile prog2.c
e5-cse-204-12.cse.psu.edu 239% gcc -g -m32 prog2.c -o prog_32
e5-cse-204-12.cse.psu.edu 240% gcc -g -m64 prog2.c -o prog_64
e5-cse-204-12.cse.psu.edu 241% size prog_32 --total
text    data    bss    dec    hex filename
1520     284      4   1888    738 prog_32
1520     284      4   1888    738 (TOTALS)
e5-cse-204-12.cse.psu.edu 242% size prog_32 --common
text    data    bss    dec    hex filename
1520     284      4   1888    738 prog_32
e5-cse-204-12.cse.psu.edu 243% size prog_64 --common
text    data    bss    dec    hex filename
1722     572      4   2298    8fa prog_64
e5-cse-204-12.cse.psu.edu 244%
```



```
[e5-cse-204-12.cse.psu.edu 252% ls
Makefile prog2.c prog_32 prog_64
[e5-cse-204-12.cse.psu.edu 253% size prog_64
text    data    bss    dec    hex filename
1722     572      4   2298    8fa prog_64]
```

- ii) For prog_32, size of code during run time, total is 935k, stack is 7040k. Please see the screenshot below. For prog_64, total size during run time is 11432K and stack is 7040k.



```
[e5-cse-204-12.cse.psu.edu 244% pidof prog_32
20169
[e5-cse-204-12.cse.psu.edu 245% pgrep prog_32
20169
[e5-cse-204-12.cse.psu.edu 246% pmap 20169
20169: /home/grads/azp5611/cmpsc473/PA1/prog2/prog_32
00000000004b0000 4K r-- prog_32
00000000004c0000 4K r-- prog_32
00000000004d0000 4K r-- prog_32
00000000004e0000 304K rw--- [ anon ]
0000000077dd0000 4K rw--- [ anon ]
0000000077dd0000 1808K r-- libc-2.17.so
0000000077790000 4K r-- libc-2.17.so
00000000775a0000 4K r-- libc-2.17.so
0000000077520000 4K r-- libc-2.17.so
0000000077530000 12K rw--- [ anon ]
00000000775d0000 4K rw--- [ anon ]
00000000775d0000 4K r-- libc-2.17.so
00000000777d0000 136K r-- ld-2.17.so
0000000077fc0000 4K r---- ld-2.17.so
0000000077fd0000 4K rw--- ld-2.17.so
00000000ff91e000 7048K rw--- [ stack ]
total           9352K
e5-cse-204-12.cse.psu.edu 247%
```

```

~ - ssh azp5611@e5-cse-204-12.cse.psu.edu - 80x24
[e5-cse-204-12.cse.psu.edu 256% pmap 27324 | grep "total"
total 11432K
[e5-cse-204-12.cse.psu.edu 257% pmap 27324
27324: /home/ugrads/azp5611/cmpsc473/PA1/prog2/prog_64
0000000004000000 4K r-x--- prog_64
0000000006000000 4K r----- prog_64
0000000006010000 4K rw---- prog_64
0000000006020000 384K rw---- [ anon ]
00007ffff7a0d000 1808K r-x--- libc-2.17.so
00007ffff7bd1000 2044K ----- libc-2.17.so
00007ffff7dd0000 16K r----- libc-2.17.so
00007ffff7dd4000 8K rw---- libc-2.17.so
00007ffff7dd6000 20K rw---- [ anon ]
00007ffff7ddb000 136K r-x--- ld-2.17.so
00007ffff7fc4000 12K rw---- [ anon ]
00007ffff7ff8000 8K rw---- [ anon ]
00007ffff7ffa000 8K r-x--- [ anon ]
00007ffff7ffc000 4K r----- ld-2.17.so
00007ffff7ffd000 4K rw---- ld-2.17.so
00007ffff7ffe000 4K rw---- [ anon ]
00007fffff91f000 7040K rw---- [ stack ]
ffffffffff600000 4K r-x--- [ anon ]
total 11432K
e5-cse-204-12.cse.psu.edu 258%

```

iii) For prog_32, Library sizes (libc-2.17.so, ld-2.17.so ...), total is 1968 K. See the screenshot below for details

```

~ - ssh azp5611@e5-cse-204-12.cse.psu.edu - 146x24
[e5-cse-204-12.cse.psu.edu 246% pmap 28169
20169: /home/ugrads/azp5611/cmpsc473/PA1/prog2/prog_32
0000000004000000 4K r-x--- prog_32
0000000006000000 4K r----- prog_32
0000000006040000 4K rw---- prog_32
0000000008040000 384K rw---- [ anon ]
00000000077d0000 4K rw---- [ anon ]
00000000077d0b000 1888K r-x--- libc-2.17.so
00000000077d0c000 4K r----- libc-2.17.so
00000000077fa0000 4K r----- libc-2.17.so
00000000077fa2000 4K rw---- libc-2.17.so
00000000077fa3000 12K rw---- [ anon ]
00000000077fd7000 8K rw---- [ anon ]
00000000077fd9000 4K r-x--- [ anon ]
00000000077fd9000 136K r-x--- ld-2.17.so
00000000077fc0000 4K r----- ld-2.17.so
00000000077fd0000 4K rw---- ld-2.17.so
00000000077fd1000 7040K rw---- [ stack ]
total 1968K
e5-cse-204-12.cse.psu.edu 247% pmap 28169 | grep "total"
Unmatched ".
e5-cse-204-12.cse.psu.edu 248% pmap 28169 | grep "total"
total 9352K
e5-cse-204-12.cse.psu.edu 249%

```

For prog_64, Library, library size 3884 K (adding up libc-2.17.so, ld-2.17.so ...). See screenshot.

```

~ - ssh azp5611@e5-cse-204-12.cse.psu.edu - 80x24
[e5-cse-204-12.cse.psu.edu 256% pmap 27324 | grep "total"
total 11432K
[e5-cse-204-12.cse.psu.edu 257% pmap 27324
27324: /home/ugrads/azp5611/cmpsc473/PA1/prog2/prog_64
0000000004000000 4K r-x--- prog_64
0000000006000000 4K r----- prog_64
0000000006010000 4K rw---- prog_64
0000000006020000 384K rw---- [ anon ]
00007ffff7a0d000 1808K r-x--- libc-2.17.so
00007ffff7bd1000 2044K ----- libc-2.17.so
00007ffff7dd0000 16K r----- libc-2.17.so
00007ffff7dd4000 20K rw---- libc-2.17.so
00007ffff7dd6000 134K r-x--- ld-2.17.so
00007ffff7dd8000 12K rw---- [ anon ]
00007ffff7fc0000 4K r----- ld-2.17.so
00007ffff7fc8000 4K rw---- ld-2.17.so
00007ffff7fe0000 4K rw---- [ anon ]
00007fffff91f000 7040K rw---- [ stack ]
ffffffffff600000 4K r-x--- [ anon ]
total 11432K
e5-cse-204-12.cse.psu.edu 258%

```

b) and c)

gdb to find the program statement that caused the error, explain the cause of this error.

```
C = malloc(300);
```

```
Int x[300000];
```

Size of each frame:

(Stack Frame 5 at - Stack Frame 4 at)

-> 0xffed7ed0 - 0xffdb2f20 = 124FB0 (1200048 in decimal)

X exceeds the bounds of the stack when reached for, so overflow.

```
~/Desktop — ssh azp5611@e5-cse-204-12.cse.psu.edu — 112x24
#3 0x80484e6 in allocate (count=7) at prog2.c:13
#4 0x80484e6 in allocate (count=8) at prog2.c:13
#5 0x80484e6 in allocate (count=9) at prog2.c:13
#6 0x80484e6 in allocate (count=10) at prog2.c:13
#7 0x8048511 in main (argc=1, argv=0xffffcf44) at prog2.c:21
(gdb) info frame 4
Stack frame at 0xffdb2f20:
  eip = 0x80484e6 in allocate (prog2.c:13); saved eip 0x80484e6
  called by frame at 0xffed7ed0, caller of frame at 0xffc8df70
  source language c.
  Arglist at 0xffdb2f18, args: count=8
  Locals at 0xffdb2f18, Previous frame's sp is 0xffdb2f20
  Saved registers:
    ebp at 0xffdb2f18, eip at 0xffdb2fic
(gdb) info frame 5
Stack frame at 0xffed7ed0:
  eip = 0x80484e6 in allocate (prog2.c:13); saved eip 0x80484e6
  called by frame at 0xfffffce80, caller of frame at 0xffdb2f20
  source language c.
  Arglist at 0xffed7ec8, args: count=9
  Locals at 0xffed7ec8, Previous frame's sp is 0xffed7ed0
  Saved registers:
    ebp at 0xffed7ec8, eip at 0xffed7ecc
(gdb) 
```

```
[e5-cse-204-12.cse.psu.edu 109% pmap 12753
12753: /home/ugrads/azp5611/cmpsc473/PA1/prog2/prog_32
0000000000004a8000 4K r-x-- prog_32
0000000000004a9000 4K r---- prog_32
0000000000004aa000 4K rw--- prog_32
0000000000004ab000 384K rw--- [ anon ]
00000000000077da000 4K rw--- [ anon ]
00000000000077db000 1808K r-x-- libc-2.17.so
00000000000077f9000 4K ----- libc-2.17.so
00000000000077fa0000 8K r---- libc-2.17.so
00000000000077fa2000 4K rw--- libc-2.17.so
00000000000077fa3000 12K rw--- [ anon ]
00000000000077fd7000 8K rw--- [ anon ]
00000000000077fd9000 4K r-x-- [ anon ]
00000000000077fd9000 136K r-x-- ld-2.17.so
00000000000077ffc000 4K r---- ld-2.17.so
0000000000007ffffd000 4K rw--- ld-2.17.so
0000000000ff91e000 7848K rw--- [ stack ]
total 9352K -
```

d) It seems like it is invoked 7 times. I am not sure about the last invocation, meaning the 7th, since it goes back to main with argv, it may mean it fails the 7th time so 6 invocations could be the correct answer as well. But my count starts from 4.

```
~ - ssh azp5611@e5-cse-204-12.cse.psu.edu - 80x24

Stack Address = 0xffffe8df8c      Heap Address = 0x8059a78
Stack Address = 0xffffb68fdc      Heap Address = 0x8060fb0
Stack Address = 0xffffa4402c      Heap Address = 0x80684e8
Stack Address = 0xffff91f07c      Heap Address = 0x806fa20

Program received signal SIGSEGV, Segmentation fault.
allocate (count=4) at prog2.c:11
11          c = malloc (30000);
Missing separate debuginfos, use: debuginfo-install glibc-2.17-324.el7_9.i686
[(gdb) backtrace
#0  allocate (count=4) at prog2.c:11
#1  0x000484e6 in allocate (count=5) at prog2.c:13
#2  0x000484e6 in allocate (count=6) at prog2.c:13
#3  0x000484e6 in allocate (count=7) at prog2.c:13
#4  0x000484e6 in allocate (count=8) at prog2.c:13
#5  0x000484e6 in allocate (count=9) at prog2.c:13
#6  0x000484e6 in allocate (count=10) at prog2.c:13
#7  0x00048511 in main (argc=1, argv=0xfffffc44) at prog2.c:21
(gdb) ]
```

e) Size of each frame:

(Stack Frame 5 at - Stack Frame 4 at)

-> 0xffffed7ed0 - 0xffffdb2f20 = 124FB0 (12.000.48 bytes).

```
((gdb) frame  
#1 0x080484e6 in allocate (count=8) at prog2.c:13  
13         allocate(count - 1);  
(gdb) 
```

It has the information about saved registers, local variables, the caller and callee of the frames, argument lists, displaying the contents of the frame, and gives details about it.

```
(gdb) info frame 5
Stack frame at 0xffffed7ed0;
  eip = 0x80484e6 in allocate (prog2.c:13); saved eip 0x80484e6
  called by frame at 0xfffffc80, caller of frame at 0xffffdb2f20
  source language c.
  Arglist at 0xffffed7ec0, args: count=9
  Locals at 0xffffed7ec8, Previous frame's sp is 0xffffed7ed0
  Saved registers:
    ebp at 0xffffed7ec8, eip at 0xffffed7ecc
(gdb) 
```

3)

```
[e5-cse-204-12.cse.psu.edu 129% cat Makefile
all: prog3

prog3: prog3.c
        gcc -g -std=gnu99 prog3.c -o prog3 -lm
clean:
        rm -rf prog3
[e5-cse-204-12.cse.psu.edu 130% gcc -g -m32 -std=c99 prog3.c -o prog3_32
/tmp/ccI5UBvH.o: In function `allocate':
/home/ugrads/azp5611/cmpsc473/PA1/prog3/prog3.c:13: undefined reference to `pow'
collect2: error: ld returned 1 exit status
[e5-cse-204-12.cse.psu.edu 131% gcc -g -m32 -std=gnu99 prog3.c -o prog3_32
/tmp/ccjtCoRU.o: In function `allocate':
/home/ugrads/azp5611/cmpsc473/PA1/prog3/prog3.c:13: undefined reference to `pow'
collect2: error: ld returned 1 exit status
[e5-cse-204-12.cse.psu.edu 132% gcc -g -m32 -std=c99 prog3.c -o prog_32
/tmp/ccXEWVcw.o: In function `allocate':
/home/ugrads/azp5611/cmpsc473/PA1/prog3/prog3.c:13: undefined reference to `pow'
collect2: error: ld returned 1 exit status
[e5-cse-204-12.cse.psu.edu 133% gcc -g -m32 -std=c99 prog3.c -o prog_32 -lm
[e5-cse-204-12.cse.psu.edu 134% gcc -g -m64 -std=c99 prog3.c -o prog_64 -lm
[e5-cse-204-12.cse.psu.edu 135% ls
Makefile prog_32 prog3.c prog_64
e5-cse-204-12.cse.psu.edu 136%
```

- a) i) For prog_32 (32 bits exec) of prog3, size of compiled code in “text” is 1759 and size of compiled code for prog_64 (64 bits exec), size of compiled code in “text” is 2017.

```
[e5-cse-204-12.cse.psu.edu 145% ls
Makefile prog_32 prog3.c prog_64
[e5-cse-204-12.cse.psu.edu 146% size prog_32
  text    data     bss     dec     hex filename
 1759      296       4   2059     80b prog_32
[e5-cse-204-12.cse.psu.edu 147% size prog_64
  text    data     bss     dec     hex filename
 2017      596       4   2617     a39 prog_64
e5-cse-204-12.cse.psu.edu 148%
```

ii) For prog_32, size of code during run time, total is 437552K, stack is 132K. Please see the screenshot below. For prog_64, total size during run time is 4413212K and stack is 132K with read and write. See the screenshots below. Linked libraries for the 32 bit executable prog_32 (if it is only libc and libm) is total 2088K (libc+libm value). Its value is $(136+4+4) = 144$ K Linked libraries for the 64 bit executable prog_64 is (libc_limb value) 6956K. Its value is $(136+4+4) = 144$ K.

```
ssh azp5611@e5-cse-204-12.cse.psu.edu -t
[e5-cse-204-12.cse.psu.edu 146% pidof prog_32
26598
[e5-cse-204-12.cse.psu.edu 147% pgrep prog2
pgrep: Command not found.
[e5-cse-204-12.cse.psu.edu 148% pgrep prog_32
26598
[e5-cse-204-12.cse.psu.edu 149% pmap 26598
26598: /home/ugrads/azp5611/cmpsc473/PA1/prog3/prog_32
00000000008048000 4K r-x-- prog_32
00000000008049000 4K r---- prog_32
0000000000804a000 4K rw--- prog_32
0000000000804b000 132K rw--- [ anon ]
000000000d480000 132K rw--- [ anon ]
000000000d421000 892K ----- [ anon ]
000000000d5c6000 433996K rw--- [ anon ]
000000000f7d9000 1808K r-x-- libc-2.17.so
000000000f7f5d000 4K ----- libc-2.17.so
000000000f7f5e000 8K r---- libc-2.17.so
000000000f7f60000 4K rw--- libc-2.17.so
000000000f7f61000 12K rw--- [ anon ]
000000000f7f64000 256K r-x-- libm-2.17.so
000000000f7fa4000 4K r---- libm-2.17.so
000000000f7fa5000 4K rw--- libm-2.17.so
000000000f7fd7000 8K rw--- [ anon ]
000000000f7fd9000 4K r-x-- [ anon ]
000000000f7fd9000 136K r-x-- ld-2.17.so
000000000f7ffc000 4K r---- ld-2.17.so
000000000f7ffd000 4K rw--- ld-2.17.so
000000000fffd000 132K rw--- [ stack ]
total 437552K
[e5-cse-204-12.cse.psu.edu 150% pmap 26598 | grep "total"
total 437552K
e5-cse-204-12.cse.psu.edu 151%
```

```
ssh azp5611@e5-cse-204-12.cse.psu.edu -t
[e5-cse-204-12.cse.psu.edu 153% ls
Makefile prog_32 prog3.c prog_64
[e5-cse-204-12.cse.psu.edu 154% size prog_64
text data bss dec hex filename
2017 596 4 2617 a39 prog_64
e5-cse-204-12.cse.psu.edu 155% pgrep prog_64
27193
[e5-cse-204-12.cse.psu.edu 156% pmap 27193 | grep "total"
total 4413212K
[e5-cse-204-12.cse.psu.edu 157% pmap 27193
27193: /home/ugrads/azp5611/cmpsc473/PA1/prog3/prog_64
0000000000400000 4K r-x-- prog_64
0000000000601000 4K r---- prog_64
0000000000602000 4K rw--- prog_64
0000000000602900 132K rw--- [ anon ]
00007ffff80000000 132K rw--- [ anon ]
00007ffff80210000 65604K ----- [ anon ]
00007ffff8ec88000 4339852K rw--- [ anon ]
00007ffff77800000 1688K r-x-- libc-2.17.so
00007ffff78c10000 2644K ----- libc-2.17.so
00007ffff7ac00000 16K r---- libc-2.17.so
00007ffff7ad20000 8K rw--- libc-2.17.so
00007ffff7ad40000 20K rw--- [ anon ]
00007ffff7ad60000 1628K r-x-- libm-2.17.so
00007ffff7bd80000 2644K ----- libm-2.17.so
00007ffff7dd00000 4K r---- libm-2.17.so
00007ffff7dd20000 4K rw--- libm-2.17.so
00007ffff7dd40000 136K r-x-- id-2.17.so
00007ffff7dd60000 404K rw--- [ anon ]
00007ffff7f600000 8K rw--- [ anon ]
00007ffff7f610000 8K r-x-- [ anon ]
00007ffff7f620000 4K r---- id-2.17.so
00007ffff7fd00000 4K rw--- id-2.17.so
00007ffff7fc0000 4K r---- [ anon ]
00007ffff7fc0000 132K rw--- [ stack ]
fffffffffffd00000 4K r-x-- [ anon ]
total 4413212K
e5-cse-204-12.cse.psu.edu 158%
```

```

Stack Address = 0x7fffffffdb10      Heap Address = 0x602010
Stack Address = 0x7fffffffdb940      Heap Address = 0x602040
Stack Address = 0x7fffffffdb770      Heap Address = 0x6021e0
Stack Address = 0x7fffffffdb5a0      Heap Address = 0x603190
Stack Address = 0x7fffffffdb3d0      Heap Address = 0x7fffff7f62010
Stack Address = 0x7fffffffdb200      Heap Address = 0x7fffff733a010
Stack Address = 0x7fffffffdb030      Heap Address = 0x7fffff4d14010
Stack Address = 0x7fffffffcc60      Heap Address = 0x7fffdcf9b010
Stack Address = 0x7fffffffcc90      Heap Address = 0x7ffeee8e8010

Program received signal SIGSEGV, Segmentation fault.
0x00007fff779aa06 in __memset_sse2 () from /lib64/libc.so.6
Missing separate debuginfos, use: debuginfo-install glibc-2.17-324.el7_9.x86_64
(gdb) 
```

- b) According to google, SigSegV is a signal that is received when there is a memory access violation while trying to read or write from/to a memory area that your process does not have access to.

```

[e5-cse-204-12.cse.psu.edu:144% valgrind prog_64]
==3092== Memcheck, a memory error detector
==3092== Copyright (C) 2002-2017, and GNU GPL'd, by Julian Seward et al.
==3092== Using Valgrind-3.15.0 and LibVEX; rerun with -H for copyright info
==3092== Command: prog_64
==3092== 
==3092== Entering Function
Stack Address = 0x1ffe00000000      Heap Address = 0x5507040
Stack Address = 0x1ffe00000000      Heap Address = 0x55070b0
Stack Address = 0x1ffe00000000      Heap Address = 0x5507280
Stack Address = 0x1ffe00000000      Heap Address = 0x5508260
Stack Address = 0x1ffe00000000      Heap Address = 0x5511ee0
Stack Address = 0x1ffe00000000      Heap Address = 0x5907040
Stack Address = 0x1ffe00000000      Heap Address = 0x5d07040
==3092== Warning: set address range perms: large range [0x832d040, 0x200a6440] (undefined)
Stack Address = 0x1ffe00000000      Heap Address = 0x832d040
==3092== Warning: set address range perms: large range [0x59ea0000, 0x148861840] (undefined)
Stack Address = 0x1ffe00000000      Heap Address = 0x59ea0000
==3092== Invalid write of size 1
==3092==   at 0x4C30FAD: memset (vg_replace_strmem.c:1253)

```

From the screenshot above, it seems that there is invalid write of size 1 which apparently is the size of the written data and in this case it is 1 byte, size of a character.

```
    b = malloc(pow(10,r)*sizeof(int));
    for (int i = 0 ;i<sizeof(b) ; i++)
    {
        char *ch1;
        ch1 = &b[i];
        memset(ch1,'*',sizeof(b[0])+i);
    }

    printf("Stack Address = %p      Heap Address = %p  \n",
allocate(count-1,r);
```

There is a memset error which is because we allocated memory and tried accessing its addresses that exceeded the range that was allocated.

Valgrind gives details about the referring locations starting with 0x4C30FA8 and then refers to the lines, as line 22 in prog3.c: “allocate (count-1,r); line 18: **memset(ch1,’*’,sizeof(b[0]+i))** and line 31 that corresponds to function main, “allocate(count,r)”.

- c) This bug is caused by trying to reach memory it was not supposed due to allocation of the memory. Prog3 is accessing invalid memory range and prog2 stack being overflowed.

4)

- a) The program frees the memory conditionally except for the allocate2 function.
The allocation of the memory seems absurd because the for loop may allocate more than it should have, or it is trying to overwrite where it was allocated before with “if conditions” or switch , memory leak could happen.
The if statements bothered me while following code, I am not exactly sure what I would do to fix the allocation-deallocation of the memory itself but I would remove the if statements and after it finishes the first execution, I would change it to free it immediately.

```
==9602== Copyright (C) 2002-2017, and GNU GPL'd, by Julian Seward et al.
==9602== Using Valgrind-3.15.0 and LibVEX; rerun with -h for copyright info
==9602== Command: prog4 --leak-check=full
==9602==
Executing the code .....
Program execution successful
==9602==
==9602== HEAP SUMMARY:
==9602==     in use at exit: 1,843,002,000 bytes in 921,501 blocks
==9602==   total heap usage: 1,009,999 allocs, 88,498 frees, 2,039,998,000 bytes allocated
==9602==
==9602== LEAK SUMMARY:
==9602==     definitely lost: 1,842,954,000 bytes in 921,478 blocks
==9602==     indirectly lost: 0 bytes in 0 blocks
==9602==     possibly lost: 46,000 bytes in 23 blocks
==9602==     still reachable: 0 bytes in 0 blocks
==9602==           suppressed: 0 bytes in 0 blocks
==9602== Rerun with --leak-check=full to see details of leaked memory
==9602==
==9602== For lists of detected and suppressed errors, rerun with: -s
==9602== ERROR SUMMARY: 0 errors from 0 contexts (suppressed: 0 from 0)
```

- b) User CPU time is the time spent executing the user program, it is on the processor running your program's code (or code in libraries). System CPU time is the time spent executing the code in the operating system kernel on behalf of your program.

(Reference for this question 4b.

[https://stackoverflow.com/questions/4310039/user-cpu-time-vs-system-cpu-time\)](https://stackoverflow.com/questions/4310039/user-cpu-time-vs-system-cpu-time)

The User CPU time is 1.099468 seconds, and 0.498523 seconds System CPU time.

```
● ● ● ~ — ssh azp5611@e5-cse-204-12.cse.psu.edu — 97x28
&start, &end));
^
prog4.c: At top level:
prog4.c:75:3: error: expected identifier or '(' before 'return'
    return 0;
^
prog4.c:76:1: error: expected identifier or '(' before ')' token
}
^
make: *** [prog4] Error 1
[e5-cse-204-12.cse.psu.edu 173% vim prog4.c
[e5-cse-204-12.cse.psu.edu 174% make
gcc -g -std=gnu99 prog4.c check.o -o prog4 -lm
prog4.c:75:3: error: expected identifier or '(' before 'return'
    return 0;
^
prog4.c:76:1: error: expected identifier or '(' before ')' token
}
^
make: *** [prog4] Error 1
[e5-cse-204-12.cse.psu.edu 175% vim prog4.c
[e5-cse-204-12.cse.psu.edu 176% make
gcc -g -std=gnu99 prog4.c check.o -o prog4 -lm
[e5-cse-204-12.cse.psu.edu 177% ./prog4
Executing the code .....
Program execution successfull
CPU TIME: 1.099468 seconds user, 0.498523 seconds system
e5-cse-204-12.cse.psu.edu 178%
```