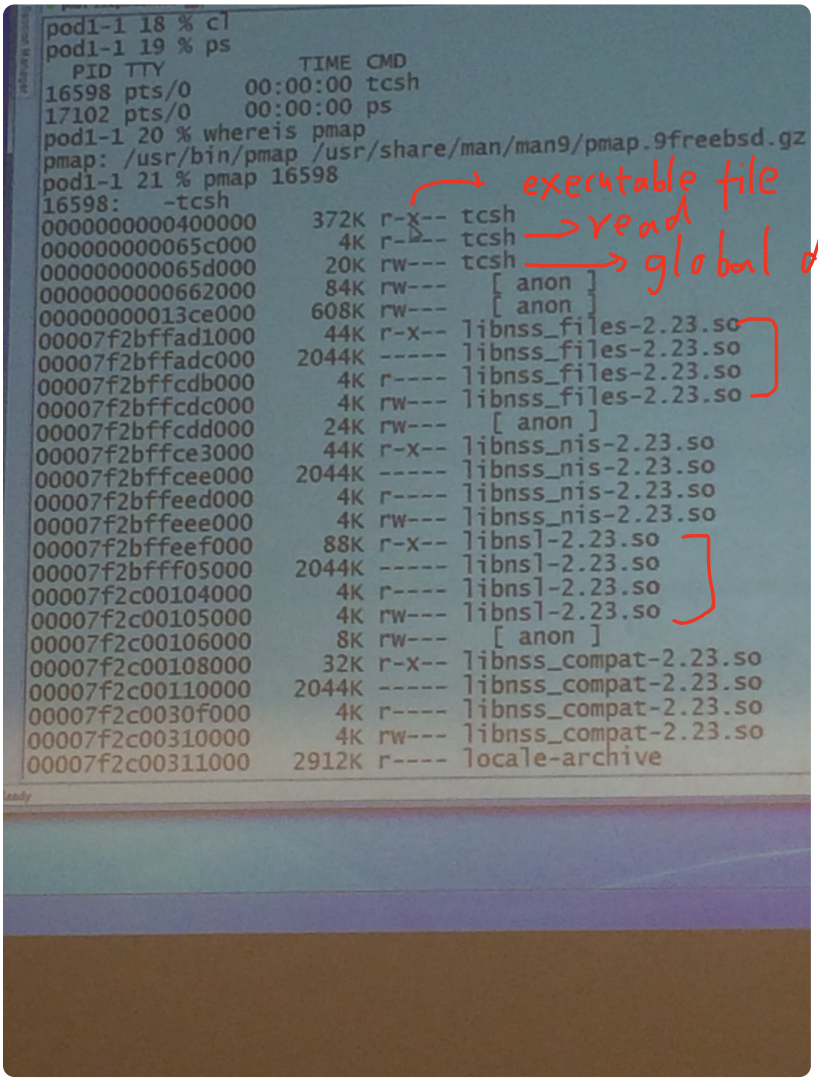
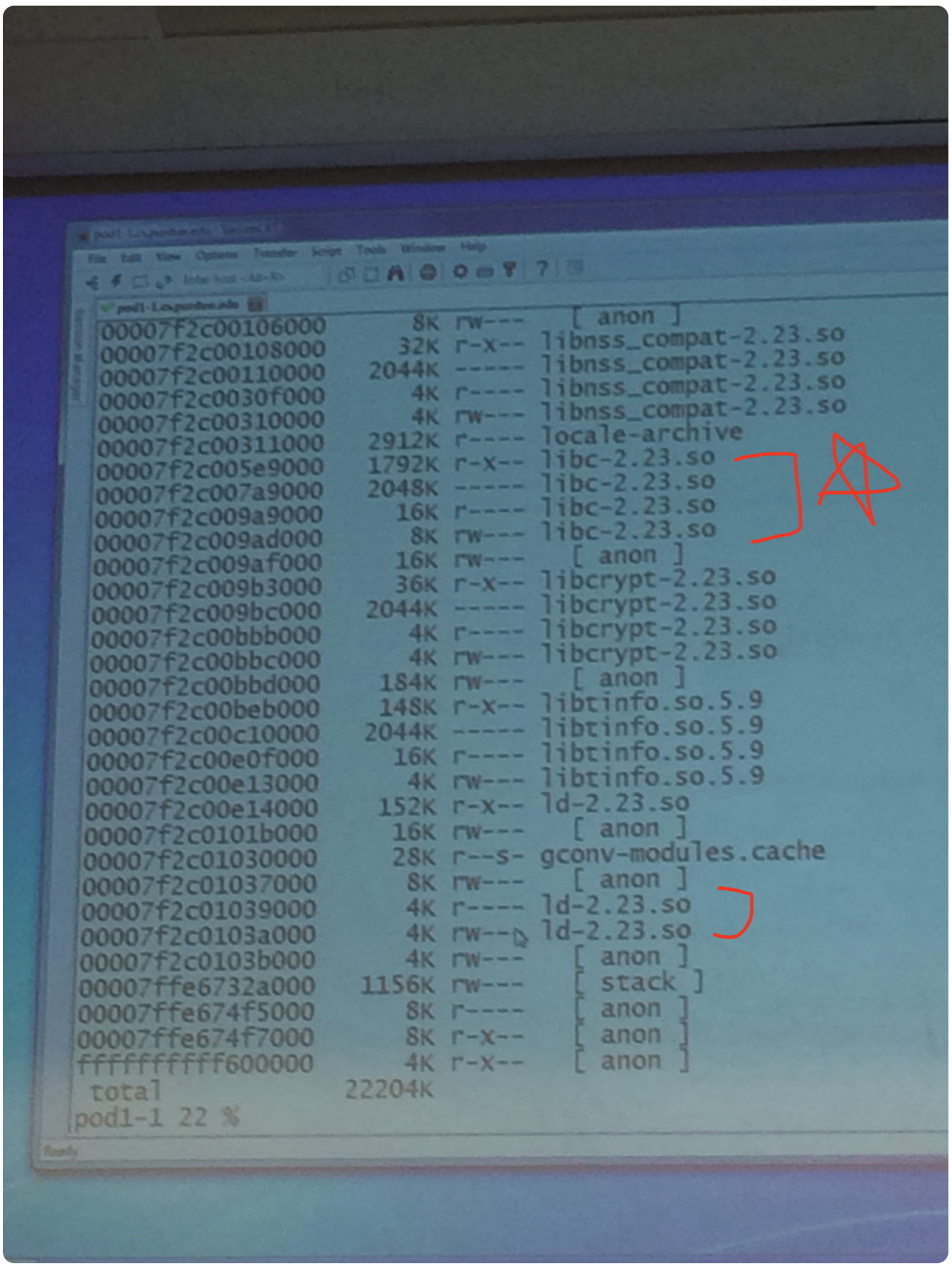
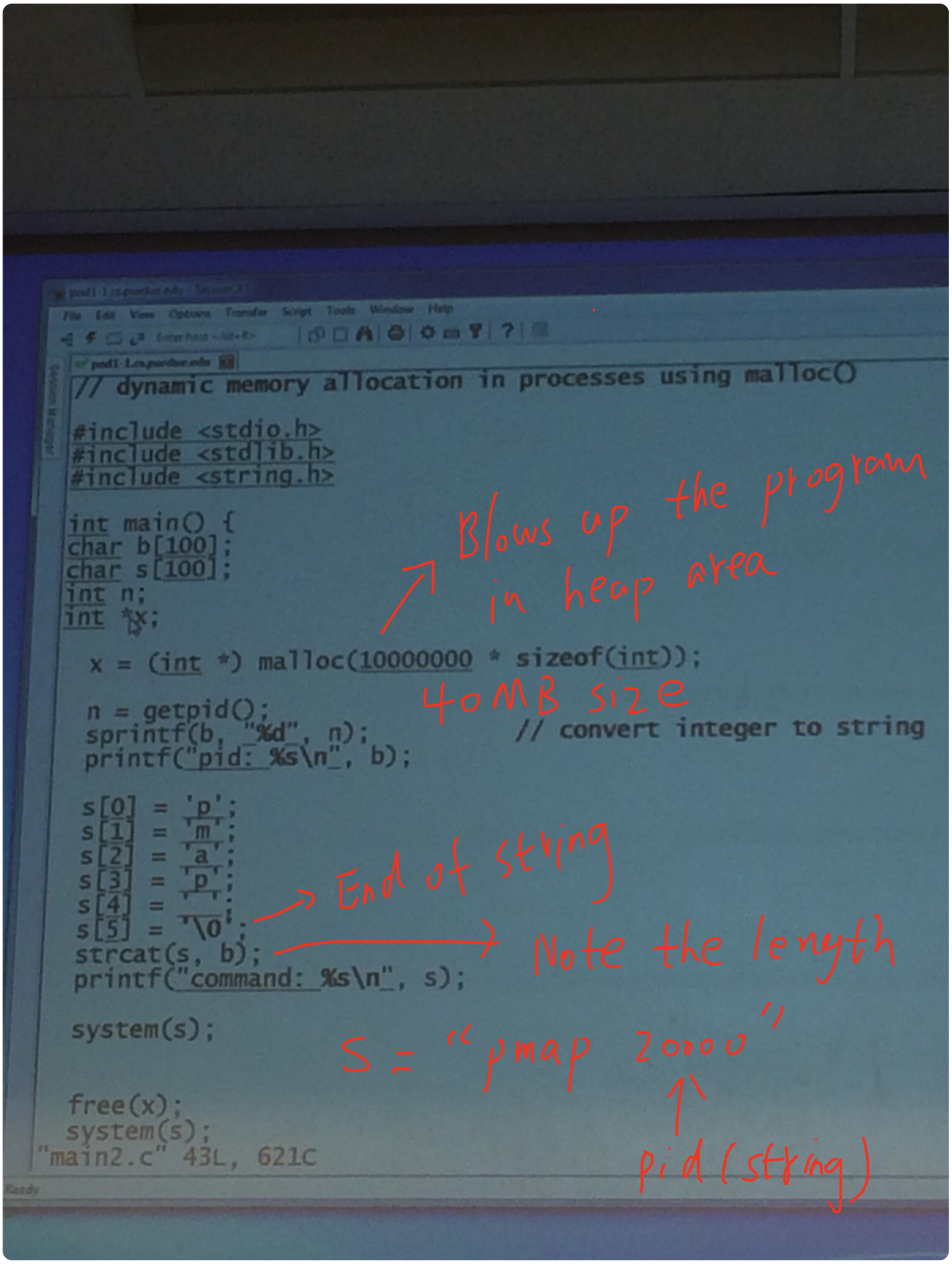
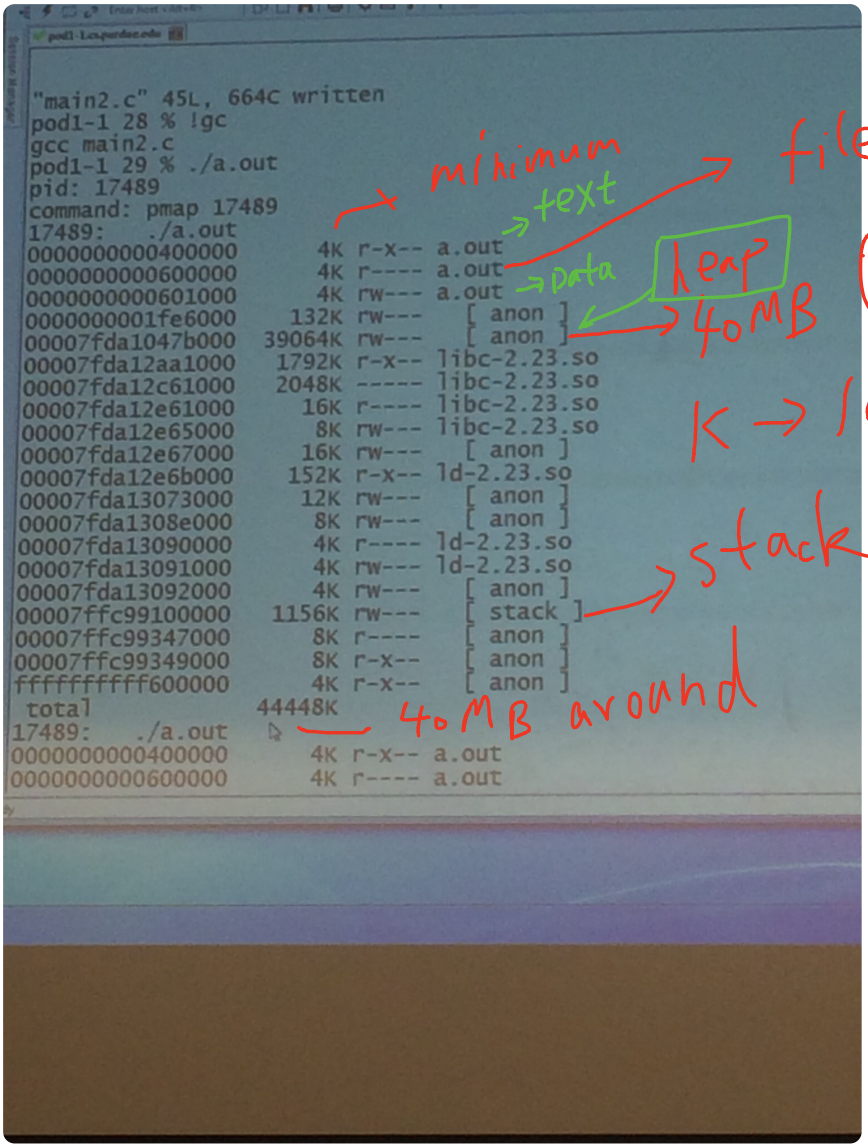
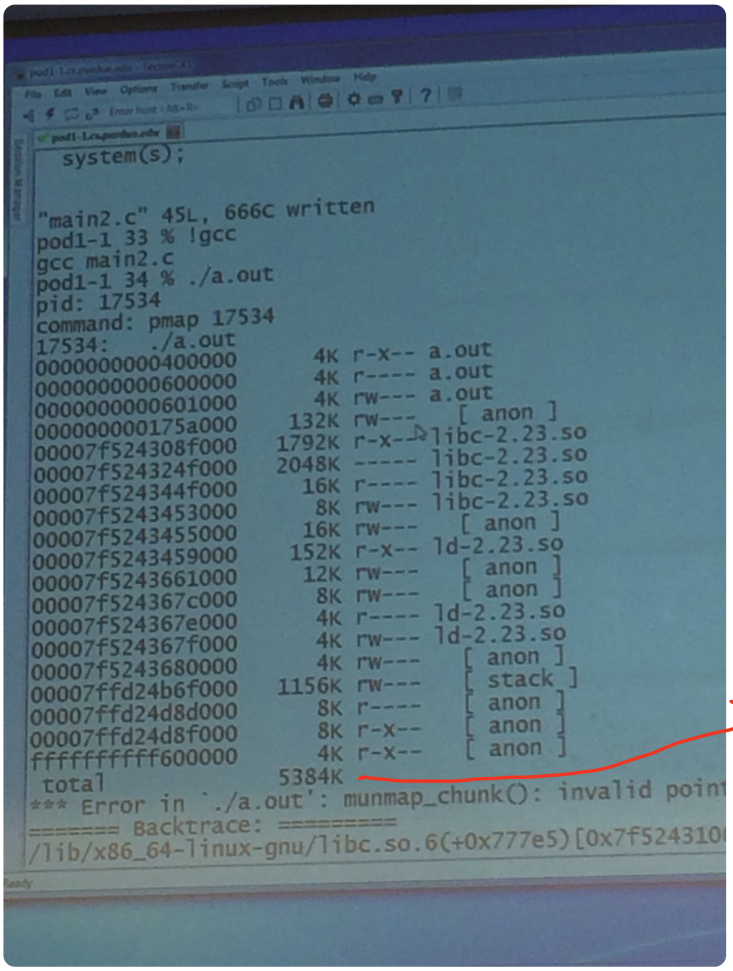
```
pod1-1 19 % ps
  PID TTY          TIME CMD
16598 pts/0    00:00:00 tcsh
17102 pts/0    00:00:00 ps
pod1-1 20 % whereis pmap
pmap: /usr/bin/pmap /usr/share/man/man9/pmap.9freebsd.gz /usr/share/man/man1/pmap.1.gz
pod1-1 21 % pmap 16598
```




00007f2c00106000 8K rw--- [anon]
00007f2c00108000 32K r-x-- libnss_compat-2.23.so
00007f2c00110000 2044K ----- libnss_compat-2.23.so
00007f2c0030f000 4K r---- libnss_compat-2.23.so
00007f2c00310000 4K rw--- libnss_compat-2.23.so
00007f2c00311000 2912K r---- locale-archive
00007f2c005e9000 1792K r-x-- libc-2.23.so
00007f2c007a9000 2048K ----- libc-2.23.so
00007f2c009a9000 16K r---- libc-2.23.so
00007f2c009ad000 8K rw--- libc-2.23.so
00007f2c009af000 16K rw--- [anon]
00007f2c009b3000 36K r-x-- libcrypt-2.23.so
00007f2c009bc000 2044K ----- libcrypt-2.23.so
00007f2c00bbb000 4K r---- libcrypt-2.23.so
00007f2c00bbc000 4K rw--- libcrypt-2.23.so
00007f2c00bbd000 184K rw--- [anon]
00007f2c00beb000 148K r-x-- libtinfo.so.5.9
00007f2c00c10000 2044K ----- libtinfo.so.5.9
00007f2c00e0f000 16K r---- libtinfo.so.5.9
00007f2c00e13000 4K rw--- libtinfo.so.5.9
00007f2c00e14000 152K r-x-- ld-2.23.so
00007f2c0101b000 16K rw--- [anon]
00007f2c01030000 28K r--s- gconv-modules.cache
00007f2c01037000 8K rw--- [anon]
00007f2c01039000 4K r---- ld-2.23.so
00007f2c0103a000 4K rw-- ld-2.23.so
00007f2c0103b000 4K rw--- [anon]
00007ffe6732a000 1156K rw--- [stack]
00007ffe674f5000 8K r---- [anon]
00007ffe674f7000 8K r-x-- [anon]
ffffffffff600000 4K r-x-- [anon]
total 22204K
pod1-1 22 %


// dynamic memory allocation in processes using malloc()
#include <stdio.h>
#include <stdlib.h>
#include <string.h>
int main() {
char b[100];
char s[100];
int n;
int *x;
x = (int *) malloc(10000000 * sizeof(int));
n = getpid();
sprintf(b, "%d", n);
// convert integer to string
printf("pid: %s\n", b);
s[0] = 'p';
s[1] = 'm';
s[2] = 'a';
s[3] = 'p';
s[4] = ' ';
s[5] = '\0';
strcat(s, b);
printf("command: %s\n", s);
system(s);
free(x);
system(s);
"main2.c" 43L, 621C
Blows up the program in heap area
40MB size
End of string
Note the length
s = "pmap 20000"
pid (string)

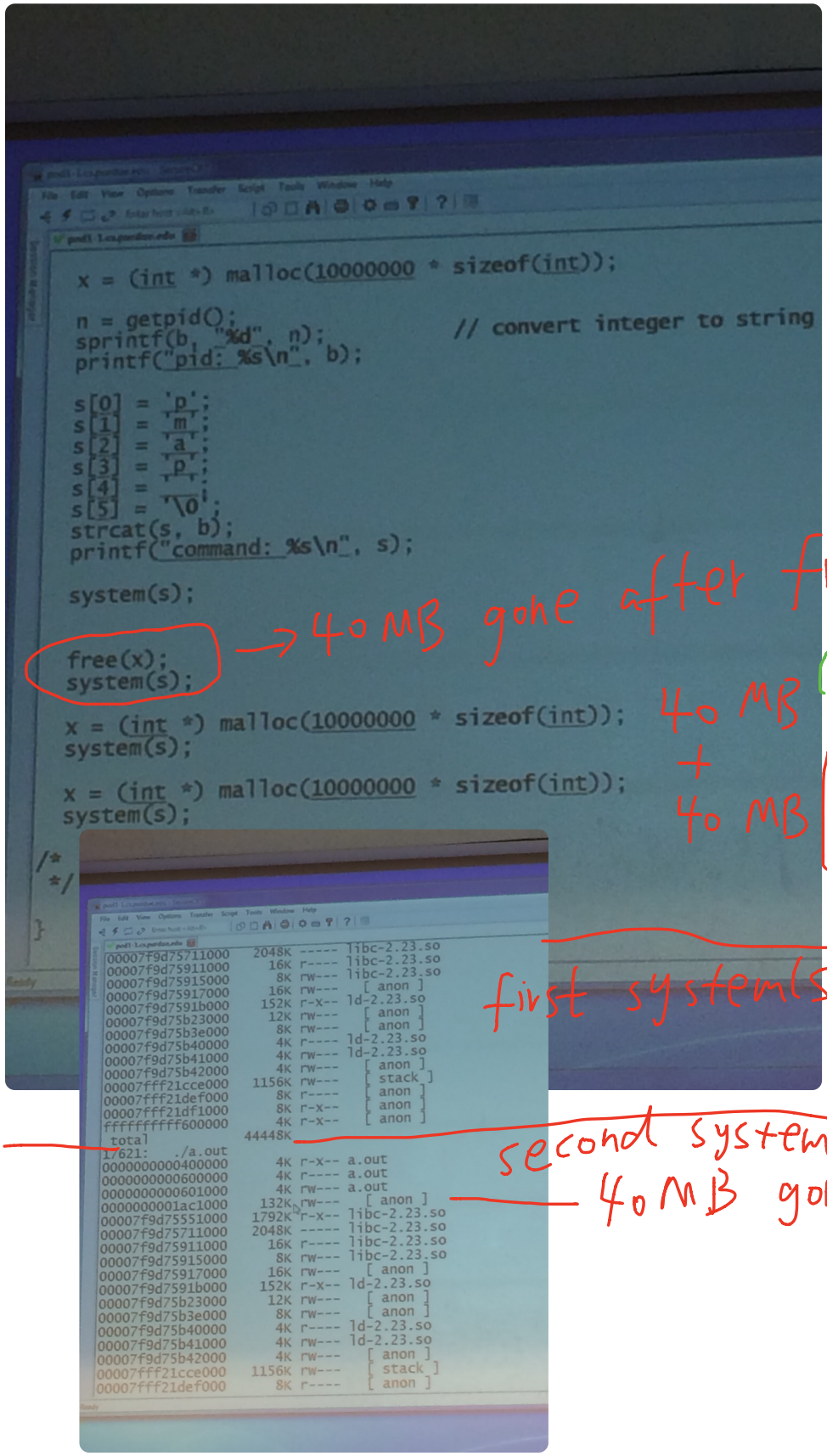

"main2.c" 45L, 664C written
pod1-1 28 % !gc
gcc main2.c
pod1-1 29 % ./a.out
pid: 17489
command: pmap 17489
17489: ./a.out
0000000000400000 4K r-x-- a.out
0000000000600000 4K r---- a.out
0000000000601000 4K rw--- a.out
0000000001fe6000 132K rw--- [anon]
00007fda1047b000 39064K rw--- [anon]
00007fda12aa1000 1792K r-x-- libc-2.23.so
00007fda12c61000 2048K ----- libc-2.23.so
00007fda12e61000 16K r---- libc-2.23.so
00007fda12e65000 8K rw--- libc-2.23.so
00007fda12e67000 16K rw--- [anon]
00007fda12e6b000 152K r-x-- ld-2.23.so
00007fda13073000 12K rw--- [anon]
00007fda1308e000 8K rw--- [anon]
00007fda13090000 4K r---- ld-2.23.so
00007fda13091000 4K rw--- ld-2.23.so
00007fda13092000 4K rw--- [anon]
00007ffc99100000 1156K rw--- [stack]
00007ffc99347000 8K r---- [anon]
00007ffc99349000 8K r-x-- [anon]
ffffffffff600000 4K r-x-- [anon]
total 44448K
17489: ./a.out
0000000000400000 4K r-x-- a.out
0000000000600000 4K r---- a.out
minimum
text
file
data
heap
40MB
(
K → 1024
stack
40MB around

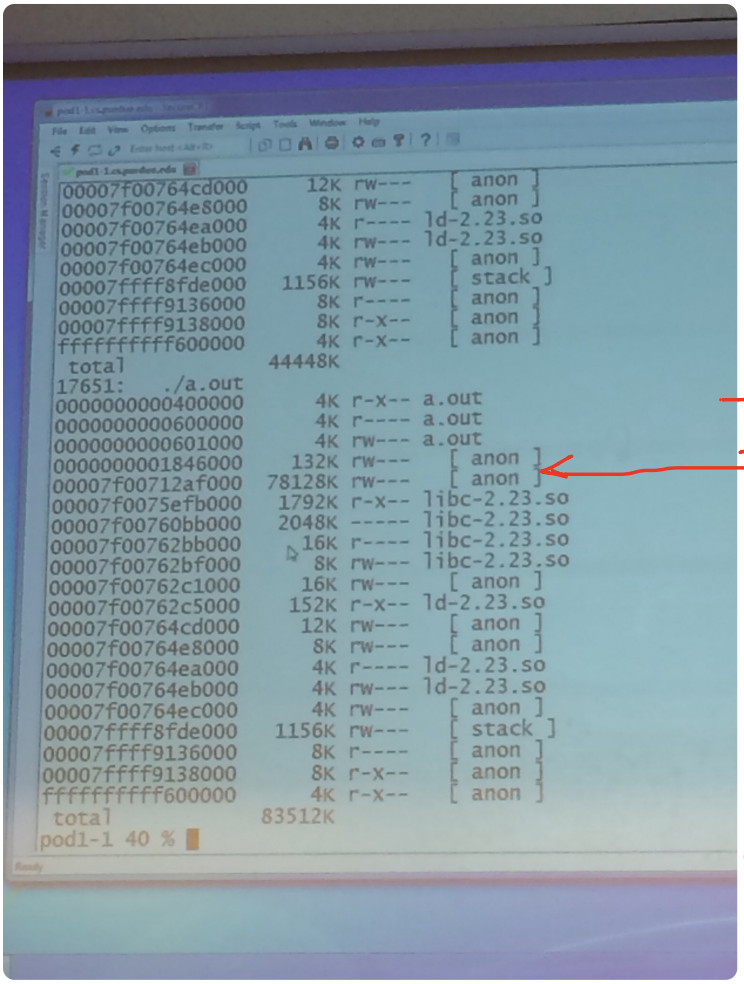


out

comment the heap alloration

No 40 MB memory section any more


x = (int *) malloc(10000000 * sizeof(int));
n = getpid();
sprintf(b, "%d", n);
// convert integer to string
printf("pid: %s\n", b);
s[0] = 'p';
s[1] = 'm';
s[2] = 'a';
s[3] = 'p';
s[4] = ' ';
s[5] = '\0';
strcat(s, b);
printf("command: %s\n", s);
system(s);
free(x);
system(s);
x = (int *) malloc(10000000 * sizeof(int));
system(s);
x = (int *) malloc(10000000 * sizeof(int));
system(s);
/*
*/
}
40 MB gone after free
(Mem Garbage)
40 MB
+
40 MB
store the second 40 MB to the same x, the first 40MB Become garbage
first system(s)
second system(s)
40 MB gone.



↓

lost the track of the first 40 MB, so. can't use it any more, it become garbage.

→ 80 MB

still only have 40 MB in use, even we total have 80 MB, first 40 MB become garbage.