

```

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

```

```

pod1-1 18 % cl
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
pod1-1 21 % pmap 16598
16598: -tcsh
0000000000400000  372K r-x-- tcsh
000000000065c000  4K r-- tcsh
000000000065d000  20K rw--- tcsh
0000000000662000  84K rw--- [ anon ]
000000000013ce000 608K rw--- [ anon ]
00007f2bfffad1000 44K r-x-- libnss_files-2.23.so
00007f2bfffadc000 2044K ----- libnss_files-2.23.so
00007f2bffffdb000  4K r---- libnss_files-2.23.so
00007f2bffffcd000  4K rw--- libnss_files-2.23.so
00007f2bffffcdd000 24K rw--- [ anon ]
00007f2bffffce3000 44K r-x-- libnss_nis-2.23.so
00007f2bffffcee000 2044K ----- libnss_nis-2.23.so
00007f2bffffeed000  4K r---- libnss_nis-2.23.so
00007f2bffffeee000  4K rw--- libnss_nis-2.23.so
00007f2bffffef000  88K r-x-- libnsl-2.23.so
00007f2bfffff05000 2044K ----- libnsl-2.23.so
00007f2c00104000  4K r---- libnsl-2.23.so
00007f2c00105000  4K rw--- libnsl-2.23.so
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

```

executable file

→ read

global data

dynamic share  
library

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 ]	
ffffffffffff600000	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] = '\0';
    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

40 MB size

End of string

Note the length

S = "pmap 2000"

↑  
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
00000000001fe6000  132K r-w-- [ anon ]
00007fda1047b000 39064K r-w-- [ anon ]
00007fda12aa1000 1792K r-x-- libc-2.23.so
00007fda12c61000 2048K ----- libc-2.23.so
00007fda12e61000   16K r---- libc-2.23.so
00007fda12e65000   8K r-w-- libc-2.23.so
00007fda12e67000   16K r-w-- [ anon ]
00007fda12e6b000 152K r-x-- ld-2.23.so
00007fda13073000   12K rw--- [ anon ]
00007fda1308e000   8K r-w-- [ anon ]
00007fda13090000   4K r---- ld-2.23.so
00007fda13091000   4K rw--- ld-2.23.so
00007fda13092000   4K r-w-- [ anon ]
00007ffc99100000 1156K r-w-- 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
```

Annotations:

- minimum file (red arrow)
- text (red arrow)
- Data (green arrow)
- Heap (green box)
- 40 MB (green arrow)
- K → 1024 (red)
- stack (red arrow)
- 40 MB around (red arrow)

```
pod1-Linux-pod1: ~ (root) ~
File Edit View Options Transfer Script Tools Window Help
4 f o? Enter host [Alt-R]
pod1-Linux-pod1: ~ (root) ~
system(s);

"main2.c" 45L, 666C written
pod1-1 33 % !gcc
gcc main2.c
pod1-1 34 % ./a.out
pid: 17534
command: pmap 17534
17534: ./a.out
0000000000400000    4K r-x-- a.out
0000000000600000    4K r---- a.out
0000000000601000    4K rw--- a.out
0000000000175a000   132K rw--- [ anon ]
00007f524308f000   1792K r-x-- libc-2.23.so
00007f524324f000   2048K ----- libc-2.23.so
00007f524344f000   16K r---- libc-2.23.so
00007f5243453000   8K rw--- libc-2.23.so
00007f5243455000   16K rw--- [ anon ]
00007f5243459000   152K r-x-- ld-2.23.so
00007f5243661000   12K rw--- [ anon ]
00007f524367c000   8K rw--- [ anon ]
00007f524367e000   4K r---- ld-2.23.so
00007f524367f000   4K rw--- ld-2.23.so
00007f5243680000   4K rw--- [ anon ]
00007ffd24b6f000   1156K rw--- stack
00007ffd24d8d000   8K r---- [ anon ]
00007ffd24d8f000   8K r-x-- [ anon ]
ffffffffff600000   4K r-x-- [ anon ]
total           5384K
*** Error in './a.out': munmap_chunk(): invalid pointer
==== Backtrace: =====
/lib/x86_64-linux-gnu/libc.so.6(+0x777e5)[0x7f524310]
```

out  
Comment the  
→ heap allocation  
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] = '\0';
s[5] = '\0';
strcat(s, b);
printf("command: %s\n", s);
system(s);

free(x);
system(s);

```

→ 40 MB gone after f

x = (int \*) malloc(10000000 \* sizeof(int));      40 MB  
 system(s);      +  
 x = (int \*) malloc(10000000 \* sizeof(int));      40 MB  
 system(s);

```
free(x);  
system(s);
```

→ 40 MB gone after free

(Mem Garbage)

Store the second 40 MB to the same X,  
the first 40 MB become garbage

first system(s)

second system(s)

```
File Edit View Options Transfer Script Tools Windows Help  
File Edit View Options Transfer Script Tools Windows Help  
[pid: 1] Lwpd [LogcatReader] 2048K ----- libc-2.23.so  
000007fd7597110000 16K r----- libc-2.23.so  
000007fd759110000 8K rwm--- libc-2.23.so  
000007fd759110000 16K rwm--- [ anon ]  
000007fd759110000 152K rwx-- 1d-2.23.so  
000007fd7591bb000 12K rw---- [ anon ]  
000007fd75b23000 8K rw---- [ anon ]  
000007fd75b3e000 4K r---- 1d-2.23.so  
000007fd75b40000 4K rwm--- 1d-2.23.so  
000007fd75b41000 4K rwm--- [ anon ]  
000007fd75b42000 4K rwm--- [ stack ]  
00007fffff21cce000 1156K rw---- [ anon ]  
00007fff21def000 8K r---- [ anon ]  
00007fff21df1000 8K rwx-- [ anon ]  
ffffffffff60000000 4K rwx-- [ anon ]  
total]  
LWP: 621: ./a.out  
0000000000040000 4K r-x-- a.out  
0000000000060000 4K r---- a.out  
00000000000601000 4K rwm--- a.out  
000000000001ac1000 132K rwm--- [ anon ]  
000007fd75551000 1792K rwx-- 1d-2.23.so  
000007fd75711000 2048K ----- libc-2.23.so  
000007fd759110000 16K r---- libc-2.23.so  
000007fd759110000 8K rwm--- libc-2.23.so  
000007fd759170000 16K rwm--- [ anon ]  
000007fd7591bb000 152K rwx-- 1d-2.23.so  
000007fd75b23000 12K rw---- [ anon ]  
000007fd75b3e000 8K rw---- [ anon ]  
000007fd75b40000 4K r---- 1d-2.23.so  
000007fd75b41000 4K rwm--- 1d-2.23.so  
000007fd75b42000 4K rwm--- [ anon ]  
000007ff721cce000 1156K rw---- [ stack ]  
000007ff21def000 8K r---- [ anon ]
```

↙

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

```
pod1-1:~$ ./a.out
0000000000400000    12K rw--- [ anon ]
0000000000600000    8K rw--- [ anon ]
0000000000601000    4K r---- [d-2.23.so]
0000000001846000    4K rw--- [ anon ]
00007f00712af000    132K rw--- [ anon ]
00007f0075efb000    78128K rw--- [ anon ] ←
00007f00760bb000    1792K r-x-- [ libc-2.23.so ]
00007f00762bb000    2048K ---- [ libc-2.23.so ]
00007f00762bf000    16K r---- [ libc-2.23.so ]
00007f00762c1000    8K rw--- [ libc-2.23.so ]
00007f00762c5000    16K rw--- [ anon ]
00007f00764cd000    152K r-x-- [d-2.23.so]
00007f00764e8000    12K rw--- [ anon ]
00007f00764ea000    8K rw--- [ anon ]
00007f00764eb000    4K r---- [d-2.23.so]
00007f00764ec000    4K rw--- [ anon ]
00007ffff8fde000    1156K rw--- [ stack ]
00007ffff9136000    8K r---- [ anon ]
00007ffff9138000    8K r-x-- [ anon ]
ffffffffff600000    4K r-x-- [ anon ]
total                44448K
17651: ./a.out
0000000000400000    4K r-x-- a.out
0000000000600000    4K r---- a.out
0000000000601000    4K rw--- a.out
0000000001846000    132K rw--- [ anon ]
00007f00712af000    78128K rw--- [ anon ] → 80 MB
00007f0075efb000    1792K r-x-- [ libc-2.23.so ]
00007f00760bb000    2048K ---- [ libc-2.23.so ]
00007f00762bb000    16K r---- [ libc-2.23.so ]
00007f00762bf000    8K rw--- [ libc-2.23.so ]
00007f00762c1000    16K rw--- [ anon ]
00007f00762c5000    152K r-x-- [d-2.23.so]
00007f00764cd000    12K rw--- [ anon ]
00007f00764e8000    8K rw--- [ anon ]
00007f00764ea000    4K r---- [d-2.23.so]
00007f00764eb000    4K rw--- [d-2.23.so]
00007f00764ec000    4K rw--- [ anon ]
00007ffff8fde000    1156K rw--- [ stack ]
00007ffff9136000    8K r---- [ anon ]
00007ffff9138000    8K r-x-- [ anon ]
ffffffffff600000    4K r-x-- [ anon ]
total                83512K
pod1-1 40 %
```

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