

Viewing Mapped Memory Regions

COMP 321

Dave Johnson



COMP 321

Copyright © 2025 David B. Johnson

Page 1

1

The Magic of the “/proc” Filesystem

A “pseudo-filesystem” that exports data from the kernel

- It ***looks like*** it contains regular directories and regular files
- Some system-wide examples
 - cat /proc/sys/kernel/ostype ⇒ “Linux”
 - cat /proc/sys/kernel/osrelease ⇒ “5.14.0-503.21.1.el9_5.x86_64”
- “/proc” also contains a directory named after existing numeric pid, such as
 - cat /proc/12345/cmdline ⇒ That process’s command line arguments
 - cat /proc/12345/environ ⇒ That process’s environment variables
- Also “***/proc/self***” as a synonym for your own pid’s /proc (e.g., /proc/12345)
- Reading from a /proc file creates the file’s contents ***on the fly***
 - Basically, the kernel does printf() from kernel data into the read() buffer

COMP 321

Copyright © 2025 David B. Johnson

Page 2

2

The File `/proc/12345/maps` (For Each Process)

A file in `/proc` for each process pid (such as, e.g., 12345)

- Shows the **current** memory mappings for that process, including
 - text, data, bss, heap, stack
 - mappings created by calls to `mmap()`
 - shared library mappings
- For each current memory mapping, shows information similar to what would have been needed by `mmap()` to create it
- Like the rest of `/proc`, the information is up to date as of when you read() it

3

Review: Address Space

A simplified example

```
int a;  
int b = 2;
```

```
main()  
{
```

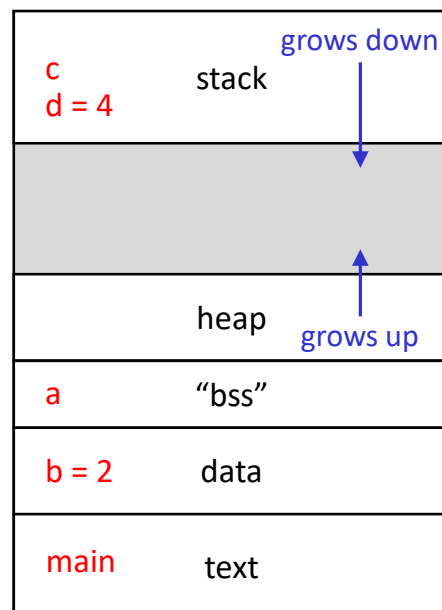
```
    int c;  
    int d = 4;  
}
```

Allocated with malloc

Uninitialized global/static

Initialized global/static

CPU instructions



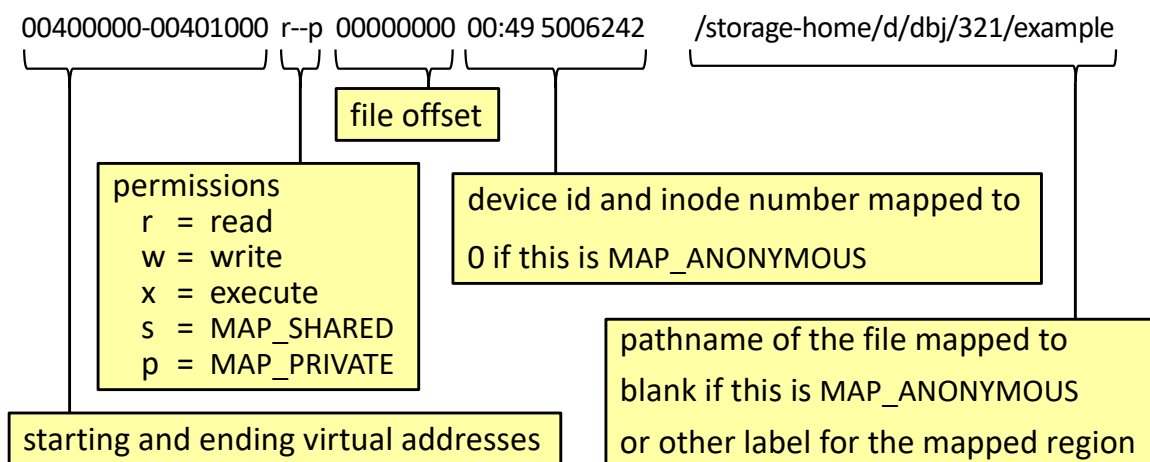
4

Some Details Missing From This Simple Example

- Combining some/all of the bss into the data
 - Data size must be rounded up to the page size, must be stored in the file and mapped into memory
 - That extra space is used by the linker for some/all of the bss
- Read-only data, also some control/header data that gets loaded
- Other memory mapped with mmap()
- Shared libraries
- Optimizations for certain kernel calls
- Stacks for additional threads
- Address space layout randomization (ASLR)
 - Makes return-oriented programming attacks harder

The General Format of /proc/12345/maps

The file is a sequence of lines, each showing one mapped region



A Very Simple Example Program

```
extern char etext;    // imaginary variable: first byte after the text
extern char edata;    // imaginary variable: first byte after the data
extern char end;      // imaginary variable: first byte after the bss

int
main(void)
{
    printf("&etext %p  &edata %p  &end %p  sbrk(0) %p\n",
           &etext, &edata, &end, sbrk(0));

    kill(getpid(), SIGSTOP);

    exit(0);
}
```

COMP 321

Copyright © 2025 David B. Johnson

Page 7

7

maps From This Example When Statically Linked

00400000-00401000 r--p 00000000 00:49 5006242	/storage-home/d/dbj/321/example-static
00401000-00486000 r-xp 00001000 00:49 5006242	/storage-home/d/dbj/321/example-static
00486000-004ae000 r--p 00086000 00:49 5006242	/storage-home/d/dbj/321/example-static
004ae000-004b2000 r--p 000ad000 00:49 5006242	/storage-home/d/dbj/321/example-static
004b2000-004b5000 rw-p 000b1000 00:49 5006242	/storage-home/d/dbj/321/example-static
004b5000-004ba000 rw-p 00000000 00:00 0	[heap]
004ba000-004dc000 rw-p 00000000 00:00 0	[heap]
7fff7ff9000-7fff7ffd000 r--p 00000000 00:00 0	[vvar]
7fff7ffd000-7fff7fff000 r-xp 00000000 00:00 0	[vdso]
7ffffffde000-7fffffff000 rw-p 00000000 00:00 0	[stack]
ffffffff600000-ffffffff601000 --xp 00000000 00:00 0	[vsyscall]

```
&etext 0x4859d5  &edata 0x4b4178  &end 0x4b9ae0  sbrk(0) 0x4dc000
```

COMP 321

Copyright © 2025 David B. Johnson

Page 8

8

maps From This Example When Statically Linked

00400000-00401000 r--p 00000000 00:49 5006242	/storage-home/d/dbj/321/example-static
00401000-00486000 r-xp 00001000 00:49 5006242	/storage-home/d/dbj/321/example-static
00486000-004ae000 r--p 00086000 00:49 5006242	/storage-home/d/dbj/321/example-static
004ae000-004b2000 r--p 000ad000 00:49 5006242	/storage-home/d/dbj/321/example-static
004b2000-004b5000 rw-p 000b1000 00:49 5006242	/storage-home/d/dbj/321/example-static
004b5000-004ba000 rw-p 00000000 00:00 0	[heap]
004ba000-004dc000 rw-p 00000000 00:00 0	[heap]
7fff7ff9000-7fff7ffd000 r--p 00000000 00:00 0	[vvar]
7fff7ffd000-7fff7fff000 r-xp 00000000 00:00 0	[vdso]
7ffffffde000-7fffffff000 rw-p 00000000 00:00 0	[stack]
ffffffff600000-ffffffff601000 --xp 00000000 00:00 0	[vsyscall]

&etext 0x4859d5 **&edata 0x4b4178** **&end 0x4b9ae0** sbrk(0) 0x4dc000

maps From This Example When Statically Linked

00400000-00401000 r--p 00000000 00:49 5006242	/storage-home/d/dbj/321/example-static
00401000-00486000 r-xp 00001000 00:49 5006242	/storage-home/d/dbj/321/example-static
00486000-004ae000 r--p 00086000 00:49 5006242	/storage-home/d/dbj/321/example-static
004ae000-004b2000 r--p 000ad000 00:49 5006242	/storage-home/d/dbj/321/example-static
004b2000-004b5000 rw-p 000b1000 00:49 5006242	/storage-home/d/dbj/321/example-static
004b5000-004ba000 rw-p 00000000 00:00 0	[heap]
004ba000-004dc000 rw-p 00000000 00:00 0	[heap]
7fff7ff9000-7fff7ffd000 r--p 00000000 00:00 0	[vvar]
7fff7ffd000-7fff7fff000 r-xp 00000000 00:00 0	[vdso]
7ffffffde000-7fffffff000 rw-p 00000000 00:00 0	[stack]
ffffffff600000-ffffffff601000 --xp 00000000 00:00 0	[vsyscall]

&etext 0x4859d5 **&edata 0x4b4178** **&end 0x4b9ae0** sbrk(0) 0x4dc000

maps From This Example When Statically Linked

```
00400000-00401000 r--p 00000000 00:49 5006242 /storage-home/d/dbj/321/example-static
00401000-00486000 r-xp 00001000 00:49 5006242 /storage-home/d/dbj/321/example-static
00486000-004ae000 r--p 00086000 00:49 5006242 /storage-home/d/dbj/321/example-static
004ae000-004b2000 r--p 000ad000 00:49 5006242 /storage-home/d/dbj/321/example-static
004b2000-004b5000 rw-p 000b1000 00:49 5006242 /storage-home/d/dbj/321/example-static
004b5000-004ba000 rw-p 00000000 00:00 0 [heap]
004ba000-004dc000 rw-p 00000000 00:00 0 [heap]
7fff7ff9000-7fff7ffd000 r--p 00000000 00:00 0 [vvar]
7fff7ffd000-7fff7fff000 r-xp 00000000 00:00 0 [vdso]
7fffffde000-7fffffff000 rw-p 00000000 00:00 0 [stack]
ffffffff600000-ffffffff601000 --xp 00000000 00:00 0 [vsyscall]
```

```
&etext 0x4859d5 &edata 0x4b4178 &end 0x4b9ae0 sbrk(0) 0x4dc000
```

11

maps From This Example When Statically Linked

```
00400000-00401000 r--p 00000000 00:49 5006242 /storage-home/d/dbj/321/example-static
00401000-00486000 r-xp 00001000 00:49 5006242 /storage-home/d/dbj/321/example-static
00486000-004ae000 r--p 00086000 00:49 5006242 /storage-home/d/dbj/321/example-static
004ae000-004b2000 r--p 000ad000 00:49 5006242 /storage-home/d/dbj/321/example-static
004b2000-004b5000 rw-p 000b1000 00:49 5006242 /storage-home/d/dbj/321/example-static
004b5000-004ba000 rw-p 00000000 00:00 0 [heap]
004ba000-004dc000 rw-p 00000000 00:00 0 [heap]
7fff7ff9000-7fff7ffd000 r--p 00000000 00:00 0 [vvar]
7fff7ffd000-7fff7fff000 r-xp 00000000 00:00 0 [vdso]
7fffffde000-7fffffff000 rw-p 00000000 00:00 0 [stack]
ffffffff600000-ffffffff601000 --xp 00000000 00:00 0 [vsyscall]
```

```
&etext 0x4859d5 &edata 0x4b4178 &end 0x4b9ae0 sbrk(0) 0x4dc000
```

12

maps From This Example When Statically Linked

00400000-00401000 r--p 00000000 00:49 5006242	/storage-home/d/dbj/321/example-static
00401000-00486000 r-xp 00001000 00:49 5006242	/storage-home/d/dbj/321/example-static
00486000-004ae000 r--p 00086000 00:49 5006242	/storage-home/d/dbj/321/example-static
004ae000-004b2000 r--p 000ad000 00:49 5006242	/storage-home/d/dbj/321/example-static
004b2000-004b5000 rw-p 000b1000 00:49 5006242	/storage-home/d/dbj/321/example-static
004b5000-004ba000 rw-p 00000000 00:00 0	[heap]
004ba000-004dc000 rw-p 00000000 00:00 0	[heap]
7ffff7ff9000-7ffff7ffd000 r--p 00000000 00:00 0	[vvar]
7ffff7ffd000-7ffff7fff000 r-xp 00000000 00:00 0	[vdso]
7ffffffde000-7fffffff0000 rw-p 00000000 00:00 0	[stack]
ffffffff600000-ffffffff601000 --xp 00000000 00:00 0	[vsyscall]

Optimization for certain kernel calls, such as `gettimeofday()` or `getcpu()`

- Becomes a procedure call rather than a kernel call

maps From This Example When Statically Linked

00400000-00401000 r--p 00000000 00:49 5006242	/storage-home/d/dbj/321/example-static
00401000-00486000 r-xp 00001000 00:49 5006242	/storage-home/d/dbj/321/example-static
00486000-004ae000 r--p 00086000 00:49 5006242	/storage-home/d/dbj/321/example-static
004ae000-004b2000 r--p 000ad000 00:49 5006242	/storage-home/d/dbj/321/example-static
004b2000-004b5000 rw-p 000b1000 00:49 5006242	/storage-home/d/dbj/321/example-static
004b5000-004ba000 rw-p 00000000 00:00 0	[heap]
004ba000-004dc000 rw-p 00000000 00:00 0	[heap]
7ffff7ff9000-7ffff7ffd000 r--p 00000000 00:00 0	[vvar]
7ffff7ffd000-7ffff7fff000 r-xp 00000000 00:00 0	[vdso]
7ffffffde000-7fffffff0000 rw-p 00000000 00:00 0	[stack]
ffffffff600000-ffffffff601000 --xp 00000000 00:00 0	[vsyscall]

Compatible emulation of the *old* way of optimizing certain kernel calls

maps From This Example When Dynamically Linked

```
00400000-00401000 r--p 00000000 00:49 5006245 /storage-home/d/dbj/321/example-dynamic
00401000-00402000 r-xp 00001000 00:49 5006245 /storage-home/d/dbj/321/example-dynamic
00402000-00403000 r--p 00002000 00:49 5006245 /storage-home/d/dbj/321/example-dynamic
00403000-00404000 r--p 00002000 00:49 5006245 /storage-home/d/dbj/321/example-dynamic
00404000-00405000 rw-p 00003000 00:49 5006245 /storage-home/d/dbj/321/example-dynamic
00405000-00426000 rw-p 00000000 00:00 0 [heap]
```

...

maps From This Example When Dynamically Linked

```
...
7fff7c0000-7fff7c28000 r--p 00000000 fd:02 421 /usr/lib64/libc.so.6
7fff7c28000-7fff7d9d000 r-xp 00028000 fd:02 421 /usr/lib64/libc.so.6
7fff7d9d000-7fff7df5000 r--p 0019d000 fd:02 421 /usr/lib64/libc.so.6
7fff7df5000-7fff7df9000 r--p 001f5000 fd:02 421 /usr/lib64/libc.so.6
7fff7df9000-7fff7dfb000 rw-p 001f9000 fd:02 421 /usr/lib64/libc.so.6
7fff7dfb000-7fff7e08000 rw-p 00000000 00:00 0
7fff7fa7000-7fff7fab000 rw-p 00000000 00:00 0
```

...

The entire standard C library linked in as a shared library

maps From This Example When Dynamically Linked

...

```
7fff7c00000-7fff7c28000 r--p 00000000 fd:02 421 /usr/lib64/libc.so.6
7fff7c28000-7fff7d9d000 r-xp 00028000 fd:02 421 /usr/lib64/libc.so.6
7fff7d9d000-7fff7df5000 r--p 0019d000 fd:02 421 /usr/lib64/libc.so.6
7fff7df5000-7fff7df9000 r--p 001f5000 fd:02 421 /usr/lib64/libc.so.6
7fff7df9000-7fff7dfb000 rw-p 001f9000 fd:02 421 /usr/lib64/libc.so.6
7fff7dfb000-7fff7e08000 rw-p 00000000 00:00 0
7fff7fa7000-7fff7fab000 rw-p 00000000 00:00 0
```

...

The entire standard C library linked in as a shared library

Each shared library has its own separate data and bss

maps From This Example When Dynamically Linked

...

```
7fff7fc1000-7fff7fc5000 r--p 00000000 00:00 0 [vvar]
7fff7fc5000-7fff7fc7000 r-xp 00000000 00:00 0 [vdso]
7fff7fc7000-7fff7fc9000 r--p 00000000 fd:02 417 /usr/lib64/ld-linux-x86-64.so.2
7fff7fc9000-7fff7ff0000 r-xp 00002000 fd:02 417 /usr/lib64/ld-linux-x86-64.so.2
7fff7ff0000-7fff7ffb000 r--p 00029000 fd:02 417 /usr/lib64/ld-linux-x86-64.so.2
7fff7ffb000-7fff7ffd000 r--p 00034000 fd:02 417 /usr/lib64/ld-linux-x86-64.so.2
7fff7ffd000-7fff7fff000 rw-p 00036000 fd:02 417 /usr/lib64/ld-linux-x86-64.so.2
7fffffde000-7ffffffffff000 rw-p 00000000 00:00 0 [stack]
ffffffff600000-ffffffff601000 --xp 00000000 00:00 0 [vsyscall]
```

The Linux dynamic linker/loader

maps From This Example When Dynamically Linked

...

7fff7fc1000-7fff7fc5000 r--p 00000000 00:00 0	[vvar]
7fff7fc5000-7fff7fc7000 r-xp 00000000 00:00 0	[vdso]
7fff7fc7000-7fff7fc9000 r--p 00000000 fd:02 417	/usr/lib64/ld-linux-x86-64.so.2
7fff7fc9000-7fff7ff0000 r-xp 00002000 fd:02 417	/usr/lib64/ld-linux-x86-64.so.2
7fff7ff0000-7fff7ffb000 r--p 00029000 fd:02 417	/usr/lib64/ld-linux-x86-64.so.2
7fff7ffb000-7fff7ffd000 r--p 00034000 fd:02 417	/usr/lib64/ld-linux-x86-64.so.2
7fff7ffd000-7fff7fff000 rw-p 00036000 fd:02 417	/usr/lib64/ld-linux-x86-64.so.2
7fffffde000-7ffffffffff000 rw-p 00000000 00:00 0	[stack]
ffffffff600000-ffffffff601000 -xp 00000000 00:00 0	[vsyscall]

The Linux dynamic linker/loader

Each shared library has its own separate data and bss