

Ruby trunk - Bug #10460

Segfault instead of stack level too deep

10/30/2014 01:17 PM - plexus (Arne Brasseur)

Status: Open	
Priority: Normal	
Assignee: nobu (Nobuyoshi Nakada)	
Target version:	
ruby -v: ruby 2.2.0dev (2014-10-29 trunk 48188) [x86_64-linux]	Backport: 2.0.0: UNKNOWN, 2.1: UNKNOWN
Description	
The code to trigger this can be found here: https://gist.github.com/mbj/31163a8e712573877268	
Also have a look at the comments there. A lot of different people tried it, in some cases it segfaults, in others it doesn't. It seems to have to do with version of gcc or specific CFLAGS.	
I can reproduce the problem for 2.1.3, 2.1.4, and trunk.	
Related issues:	
Has duplicate Ruby trunk - Bug #10626: BUS error from nesting lambda's and ca...	Open 12/20/2014

History

#1 - 11/04/2014 09:43 AM - plexus (Arne Brasseur)

Did some more testing on current trunk (trunk@48266)

Depending on the optimization level I get different results. -O0 works correctly, -O1 segfaults, -O2 works correctly, -O3 hangs.

strace of the two problematic versions:

- O1: <https://gist.github.com/plexus/15b50dbd31574d6c6657>
- O3: <https://gist.github.com/plexus/173003e04e71492ac430>

I would love to help resolve this but am in way past my comfort zone :) suggestions on how to proceed would be very much appreciated.

#2 - 11/12/2014 04:17 AM - AlamoZ (Adrien Lamothe)

When I run 'strace ./segfault.rb', it segfaults but doesn't hang. strace also shows a file, operating_system.so, that is missing:

```
open("/usr/local/bin/ruby-2.2.0-preview1/lib/ruby/vendor_ruby/2.2.0/x86_64-linux/rubygems/defaults/operating_system.so",
O_RDONLY|O_CLOEXEC) = -1 ENOENT (No such file or directory)
```

Here are the final lines of the strace:

```
lstat("/home/adrien/sandbox/segfault.rb", {st_mode=S_IFREG|0755, st_size=317, ...}) = 0
mmap(NULL, 1052672, PROT_READ|PROT_WRITE, MAP_PRIVATE|MAP_ANONYMOUS, -1, 0) = 0x7f47c8a39000
mmap(NULL, 1052672, PROT_READ|PROT_WRITE, MAP_PRIVATE|MAP_ANONYMOUS|MAP_STACK, -1, 0) = 0x7f47c8938000
mprotect(0x7f47c8938000, 4096, PROT_NONE) = 0
clone(child_stack=0x7f47c8a37fb0,
flags=CLONE_VM|CLONE_FS|CLONE_FILES|CLONE_SIGHAND|CLONE_THREAD|CLONE_SYSVSEM|CLONE_SETTLS|CLONE_PARENT_SET
TID|CLONE_CHILD_CLEARTID, parent_tidptr=0x7f47c8a389d0, tls=0x7f47c8a38700, child_tidptr=0x7f47c8a389d0) = 7540
futextx(0x2600464, FUTEX_WAIT_PRIVATE, 1, NULL./segfault.rb:12: [BUG] vm_call_cfunc - cfp consistency error
ruby 2.2.0preview1 (2014-09-17 trunk 47616) [x86_64-linux]
```

```
+++ killed by SIGSEGV +++
Segmentation fault
```

#3 - 11/18/2014 01:53 PM - plexus (Arne Brasseur)

Was it rude to set this as "Priority: High"? A random segfault seems important but it also seems very few tickets are actually marked as high priority.

#4 - 11/19/2014 07:58 AM - normalperson (Eric Wong)

arne@arnebrasseur.net wrote:

Was it rude to set this as "Priority: High"? A random segfault seems important but it also seems very few tickets are actually marked as

high priority.

I don't think it is rude to set "Priority: High", but I don't care much for "formal" ticket tracking, either. I will work on issues which interest me. (I don't speak for the rest of ruby-core)

To me, segfaults in normal/otherwise-working code are important. However, this issues with stack overflows, your code is still broken even if we avoid segfaults and raise.

Ruby is trying to be nice about reporting the error; but in the end, your code is still broken if it overflows stack.

So we make a minor effort to report small overflows, but (as you can see from this ticket), it is highly sensitive to compiler and platform changes; and big overflows are not caught.

We may increase the size of the guard area; but that costs memory. Right now, on (most) Linux systems, this guard costs 4K (one page) per-thread. Increasing it may help with reporting, but your code is still broken; and you penalize the majority of users who do not overflow stack.

I suspect more users care about memory usage than getting a proper error on broken code.

#5 - 11/19/2014 09:13 PM - plexus (Arne Brasseur)

That makes sense, I agree with your point. Having a nicer error message on broken code isn't a big deal.

There is an actual use case beyond "a nicer error message" though.

Me and others make heavy use of mutation testing with Mutant (<https://github.com/mbj/mutant/>). Mutant changes the ruby code in many different ways, and then checks if your tests fail. The result is you can have much more confidence in your code and your tests. Once you get used to mutation testing it's hard to go without.

Mutant will often generate "broken" code, that's how it works, so endless recursion could be the result. It needs to be able to detect somehow that things go wrong. A segfault is actually not the biggest problem. Mutant forks off workers, so if the worker dies it can assume something went wrong. Sometimes the code in this ticket also causes Ruby to get stuck in a futex. In that case the worker is "stuck" and Mutant becomes unusable.

Maybe not everybody agrees on the usefulness of mutation testing, or if that is a valid use case for MRI. I just wanted to clarify why I filed this ticket. Actually the locking up is more a problem than the segfault.

We may increase the size of the guard area; but that costs memory. Right now, on (most) Linux systems, this guard costs 4K (one page) per-thread.

Could you tell me where in the code I can see this? I would love to investigate this more. Thanks!

#6 - 11/19/2014 09:28 PM - normalperson (Eric Wong)

arne@arnebrasseur.net wrote:

Mutant will often generate "broken" code, that's how it works, so endless recursion could be the result. It needs to be able to detect somehow that things go wrong. A segfault is actually not the biggest problem. Mutant forks off workers, so if the worker dies it can assume something went wrong. Sometimes the code in this ticket also causes Ruby to get stuck in a futex. In that case the worker is "stuck" and Mutant becomes unusable.

The freezing is likely caused by the stack overflow corrupting memory used by a mutex, putting the mutex in an unrecoverable state. You're better off to detecting lockups in the parent process via periodic checks.

We may increase the size of the guard area; but that costs memory. Right now, on (most) Linux systems, this guard costs 4K (one page) per-thread.

Could you tell me where in the code I can see this? I would love to

investigate this more. Thanks!

On GNU/Linux systems, this is done by glibc upon thread creation.

We only set the stack size via `pthread_attr_setstacksize` in `thread_pthread.c`, but we could also call `pthread_attr_setguardsize` in the same place.

#7 - 11/26/2014 10:33 PM - Ajedi32 (Andrew M)

- File `rspec_ruby_segfault.rb` added

- File `sample_output` added

Ran into this issue today when I accidentally created a stack overflow in my RSpec tests:

- ruby 2.1.5p273 (2014-11-13 revision 48405, [i686-linux])
- rspec 2.13.1

Attached is code which (sometimes) reproduces the problem (run with `rspec rspec_ruby_segfault.rb`), and the output I got when the error occurred.

#8 - 11/27/2014 11:23 AM - ko1 (Koichi Sasada)

- Category changed from *YARV* to *core*

- Assignee changed from *ko1* (Koichi Sasada) to *nobu* (Nobuyoshi Nakada)

#9 - 12/03/2014 01:58 PM - vo.x (Vit Ondruch)

I've got similar snippet:

```
describe "SEGV" do
  let(:foo) do
    foo
  end

  it "crashes" do
    foo
  end
end
```

It always fails with ruby 2.1.5p273 (2014-11-13 revision 48405) [x86_64-linux]

It sometimes passes and other time fails with ruby 2.2.0preview2 (2014-11-28 trunk 48628) [x86_64-linux]

#10 - 12/21/2014 01:06 AM - nobu (Nobuyoshi Nakada)

- Has duplicate Bug #10626: *BUS error from nesting lambda's and calls to methods defined with define_method* added

#11 - 02/09/2015 02:17 PM - plexus (Arne Brasseur)

This seems to be fixed, possibly with this commit <https://github.com/ruby/ruby/commit/8fe95fea9d238a6deb70c8953ceb3a28a67f4636>

#12 - 06/26/2015 10:16 AM - gregnavis (Greg Navis)

I think the bug is still there. I'm able to reproduce it on the nightly snapshot (dated 25 June 2015 on the FTP server).

How to Reproduce

Use the following snippet:

```
require 'minitest'
require 'minitest/autorun'

class TestBug < Minitest::Test
  def test_bug
    bang!
  end

  define_method(:bang!) do
    bang!
  end
end
```

It produced the following output:

Run options: --seed 28198

Running:

```
EEE/tmp/ruby/lib/ruby/gems/2.3.0/gems/minitest-5.7.0/lib/minitest.rb:293: [BUG] vm_call_cfunc - cfp consistency error
ruby 2.3.0dev (2015-06-26 trunk 51033) [x86_64-linux]
```

```
-- Control frame information -----
c:0011 p:---- s:0050 e:000049 CFUNC :each
c:0010 p:0008 s:0047 e:000046 BLOCK /tmp/ruby/lib/ruby/gems/2.3.0/gems/minitest-5.7.0/lib/minitest.rb:293
c:0009 p:0034 s:0045 e:000044 METHOD /tmp/ruby/lib/ruby/gems/2.3.0/gems/minitest-5.7.0/lib/minitest.rb:332
c:0008 p:0020 s:0038 E:001468 METHOD /tmp/ruby/lib/ruby/gems/2.3.0/gems/minitest-5.7.0/lib/minitest.rb:319
c:0007 p:0062 s:0032 E:0013a0 METHOD /tmp/ruby/lib/ruby/gems/2.3.0/gems/minitest-5.7.0/lib/minitest.rb:292
c:0006 p:0012 s:0025 e:000024 BLOCK /tmp/ruby/lib/ruby/gems/2.3.0/gems/minitest-5.7.0/lib/minitest.rb:155 [FINISH]
c:0005 p:---- s:0022 e:000021 CFUNC :map
c:0004 p:0036 s:0019 e:000018 METHOD /tmp/ruby/lib/ruby/gems/2.3.0/gems/minitest-5.7.0/lib/minitest.rb:155
c:0003 p:0140 s:0011 e:000010 METHOD /tmp/ruby/lib/ruby/gems/2.3.0/gems/minitest-5.7.0/lib/minitest.rb:129
c:0002 p:0065 s:0005 E:000ae8 BLOCK /tmp/ruby/lib/ruby/gems/2.3.0/gems/minitest-5.7.0/lib/minitest.rb:56 [FINISH]
c:0001 p:0000 s:0002 E:001bf0 (none) [FINISH]
```

```
-- Ruby level backtrace information -----
/tmp/ruby/lib/ruby/gems/2.3.0/gems/minitest-5.7.0/lib/minitest.rb:56:in `block in autorun'
/tmp/ruby/lib/ruby/gems/2.3.0/gems/minitest-5.7.0/lib/minitest.rb:129:in `run'
/tmp/ruby/lib/ruby/gems/2.3.0/gems/minitest-5.7.0/lib/minitest.rb:155:in `__run'
/tmp/ruby/lib/ruby/gems/2.3.0/gems/minitest-5.7.0/lib/minitest.rb:155:in `map'
/tmp/ruby/lib/ruby/gems/2.3.0/gems/minitest-5.7.0/lib/minitest.rb:155:in `block in __run'
/tmp/ruby/lib/ruby/gems/2.3.0/gems/minitest-5.7.0/lib/minitest.rb:292:in `run'
/tmp/ruby/lib/ruby/gems/2.3.0/gems/minitest-5.7.0/lib/minitest.rb:319:in `with_info_handler'
/tmp/ruby/lib/ruby/gems/2.3.0/gems/minitest-5.7.0/lib/minitest.rb:332:in `on_signal'
/tmp/ruby/lib/ruby/gems/2.3.0/gems/minitest-5.7.0/lib/minitest.rb:293:in `block in run'
/tmp/ruby/lib/ruby/gems/2.3.0/gems/minitest-5.7.0/lib/minitest.rb:293:in `each'
```

```
-- C level backtrace information -----
/tmp/ruby/bin/ruby(rb_vm_bugreport+0xc36) [0x7f135c361346] vm_dump.c:695
/tmp/ruby/bin/ruby(rb_bug+0xca) [0x7f135c3cbf6a] error.c:406
/tmp/ruby/bin/ruby(vm_call_cfunc+0x9ab) [0x7f135c34a1db] vm_inshelper.c:1598
/tmp/ruby/bin/ruby(vm_call_method+0x10e) [0x7f135c35cb7e] vm_inshelper.c:1921
/tmp/ruby/bin/ruby(vm_exec_core+0x1310) [0x7f135c34ffb0] insns.def:947
/tmp/ruby/bin/ruby(vm_exec+0x7b) [0x7f135c35526b] vm.c:1486
/tmp/ruby/bin/ruby(invoke_block_from_c+0x71b) [0x7f135c34bbbb] vm.c:857
/tmp/ruby/bin/ruby(vm_invoke_proc+0xcb) [0x7f135c34c04b] vm.c:920
/tmp/ruby/bin/ruby(rb_vm_invoke_proc+0x28) [0x7f135c34c0f8] vm.c:951
/tmp/ruby/bin/ruby(rb_proc_call+0x42) [0x7f135c20a382] proc.c:774
/tmp/ruby/bin/ruby(rb_exec_end_proc+0x131) [0x7f135c202411] eval_jump.c:107
/tmp/ruby/bin/ruby(ruby_finalize_0+0x83) [0x7f135c202543] eval.c:124
/tmp/ruby/bin/ruby(ruby_cleanup+0x1e2) [0x7f135c202a32] eval.c:182
/tmp/ruby/bin/ruby(ruby_run_node+0x36) [0x7f135c202f76] eval.c:314
/tmp/ruby/bin/ruby(main+0x5f) [0x7f135c1fecef] parse.y:8809
```

```
-- Other runtime information -----
* Loaded script: ruby_crash.rb
```

```
* Loaded features:
 0 enumerator.so
 1 rational.so
 2 complex.so
 3 /tmp/ruby/lib/ruby/2.3.0/x86_64-linux/enc/encdb.so
 4 /tmp/ruby/lib/ruby/2.3.0/x86_64-linux/enc/trans/transdb.so
 5 /tmp/ruby/lib/ruby/2.3.0/unicode_normalize.rb
 6 /tmp/ruby/lib/ruby/2.3.0/x86_64-linux/rbconfig.rb
 7 thread.rb
 8 /tmp/ruby/lib/ruby/2.3.0/x86_64-linux/thread.so
 9 /tmp/ruby/lib/ruby/2.3.0/rubygems/compatibility.rb
10 /tmp/ruby/lib/ruby/2.3.0/rubygems/defaults.rb
11 /tmp/ruby/lib/ruby/2.3.0/rubygems/deprecate.rb
12 /tmp/ruby/lib/ruby/2.3.0/rubygems/errors.rb
13 /tmp/ruby/lib/ruby/2.3.0/rubygems/version.rb
14 /tmp/ruby/lib/ruby/2.3.0/rubygems/requirement.rb
```

```

15 /tmp/ruby/lib/ruby/2.3.0/rubygems/platform.rb
16 /tmp/ruby/lib/ruby/2.3.0/rubygems/basic_specification.rb
17 /tmp/ruby/lib/ruby/2.3.0/rubygems/stub_specification.rb
18 /tmp/ruby/lib/ruby/2.3.0/rubygems/util/stringio.rb
19 /tmp/ruby/lib/ruby/2.3.0/rubygems/specification.rb
20 /tmp/ruby/lib/ruby/2.3.0/rubygems/exceptions.rb
21 /tmp/ruby/lib/ruby/2.3.0/rubygems/core_ext/kernel_gem.rb
22 /tmp/ruby/lib/ruby/2.3.0/monitor.rb
23 /tmp/ruby/lib/ruby/2.3.0/rubygems/core_ext/kernel_require.rb
24 /tmp/ruby/lib/ruby/2.3.0/rubygems.rb
25 /tmp/ruby/lib/ruby/2.3.0/rubygems/path_support.rb
26 /tmp/ruby/lib/ruby/2.3.0/rubygems/dependency.rb
27 /tmp/ruby/lib/ruby/2.3.0/optparse.rb
28 /tmp/ruby/lib/ruby/2.3.0/mutex_m.rb
29 /tmp/ruby/lib/ruby/gems/2.3.0/gems/minitest-5.7.0/lib/minitest/parallel.rb
30 /tmp/ruby/lib/ruby/2.3.0/delegate.rb
31 /tmp/ruby/lib/ruby/2.3.0/x86_64-linux/etc.so
32 /tmp/ruby/lib/ruby/2.3.0/fileutils.rb
33 /tmp/ruby/lib/ruby/2.3.0/tmpdir.rb
34 /tmp/ruby/lib/ruby/2.3.0/tempfile.rb
35 /tmp/ruby/lib/ruby/2.3.0/x86_64-linux/stringio.so
36 /tmp/ruby/lib/ruby/gems/2.3.0/gems/minitest-5.7.0/lib/minitest/assertions.rb
37 /tmp/ruby/lib/ruby/gems/2.3.0/gems/minitest-5.7.0/lib/minitest/unit.rb
38 /tmp/ruby/lib/ruby/gems/2.3.0/gems/minitest-5.7.0/lib/minitest/test.rb
39 /tmp/ruby/lib/ruby/gems/2.3.0/gems/minitest-5.7.0/lib/minitest.rb
40 /tmp/ruby/lib/ruby/gems/2.3.0/gems/minitest-5.7.0/lib/minitest/expectations.rb
41 /tmp/ruby/lib/ruby/gems/2.3.0/gems/minitest-5.7.0/lib/minitest/spec.rb
42 /tmp/ruby/lib/ruby/gems/2.3.0/gems/minitest-5.7.0/lib/minitest/mock.rb
43 /tmp/ruby/lib/ruby/gems/2.3.0/gems/minitest-5.7.0/lib/minitest/autorun.rb
44 /tmp/ruby/lib/ruby/gems/2.3.0/gems/minitest-5.7.0/lib/minitest/pride_plugin.rb

```

* Process memory map:

```

7f1344000000-7f1344021000 rw-p 00000000 00:00 0
7f1344021000-7f1348000000 ---p 00000000 00:00 0
7f134c00000000-7f134c021000 rw-p 00000000 00:00 0
7f134c021000-7f1350000000 ---p 00000000 00:00 0
7f1352b8a000-7f1352d87000 r--s 00000000 08:01 269523 /usr/lib64/libc-2.20.so
7f1352d87000-7f1353b77000 r--s 00000000 00:24 203922 /tmp/ruby/bin/ruby
7f1353b77000-7f1353b8d000 r-xp 00000000 08:01 276025 /usr/lib64/libgcc_s-4.9.2-20150212.so
.1
7f1353b8d000-7f1353d8c000 ---p 00016000 08:01 276025 /usr/lib64/libgcc_s-4.9.2-20150212.so
.1
7f1353d8c000-7f1353d8d000 r--p 00015000 08:01 276025 /usr/lib64/libgcc_s-4.9.2-20150212.so
.1
7f1353d8d000-7f1353d8e000 rw-p 00016000 08:01 276025 /usr/lib64/libgcc_s-4.9.2-20150212.so
.1
7f1353d8e000-7f1353d8f000 ---p 00000000 00:00 0
7f1353d8f000-7f1353f90000 rw-p 00000000 00:00 0 [stack:10738]
7f1353f90000-7f1353f91000 ---p 00000000 00:00 0
7f1353f91000-7f1354091000 rw-p 00000000 00:00 0 [stack:10737]
7f1354091000-7f1354099000 r-xp 00000000 00:24 203933 /tmp/ruby/lib/ruby/2.3.0/x86_64-linux
/stringio.so
7f1354099000-7f1354298000 ---p 00008000 00:24 203933 /tmp/ruby/lib/ruby/2.3.0/x86_64-linux
/stringio.so
7f1354298000-7f1354299000 r--p 00007000 00:24 203933 /tmp/ruby/lib/ruby/2.3.0/x86_64-linux
/stringio.so
7f1354299000-7f135429a000 rw-p 00008000 00:24 203933 /tmp/ruby/lib/ruby/2.3.0/x86_64-linux
/stringio.so
7f135429a000-7f13542a0000 r-xp 00000000 00:24 203931 /tmp/ruby/lib/ruby/2.3.0/x86_64-linux
/etc.so
7f13542a0000-7f135449f000 ---p 00006000 00:24 203931 /tmp/ruby/lib/ruby/2.3.0/x86_64-linux
/etc.so
7f135449f000-7f13544a0000 r--p 00005000 00:24 203931 /tmp/ruby/lib/ruby/2.3.0/x86_64-linux
/etc.so
7f13544a0000-7f13544a1000 rw-p 00006000 00:24 203931 /tmp/ruby/lib/ruby/2.3.0/x86_64-linux
/etc.so
7f13544a1000-7f13544a4000 r-xp 00000000 00:24 203935 /tmp/ruby/lib/ruby/2.3.0/x86_64-linux
/thread.so
7f13544a4000-7f13546a3000 ---p 00003000 00:24 203935 /tmp/ruby/lib/ruby/2.3.0/x86_64-linux
/thread.so
7f13546a3000-7f13546a4000 r--p 00002000 00:24 203935 /tmp/ruby/lib/ruby/2.3.0/x86_64-linux
/thread.so
7f13546a4000-7f13546a5000 rw-p 00003000 00:24 203935 /tmp/ruby/lib/ruby/2.3.0/x86_64-linux
/thread.so

```

```

7f13546a5000-7f13546a7000 r-xp 00000000 00:24 175157 /tmp/ruby/lib/ruby/2.3.0/x86_64-linux
/enc/trans/transdb.so
7f13546a7000-7f13548a7000 ---p 00002000 00:24 175157 /tmp/ruby/lib/ruby/2.3.0/x86_64-linux
/enc/trans/transdb.so
7f13548a7000-7f13548a8000 r--p 00002000 00:24 175157 /tmp/ruby/lib/ruby/2.3.0/x86_64-linux
/enc/trans/transdb.so
7f13548a8000-7f13548a9000 rw-p 00003000 00:24 175157 /tmp/ruby/lib/ruby/2.3.0/x86_64-linux
/enc/trans/transdb.so
7f13548a9000-7f13548ab000 r-xp 00000000 00:24 203974 /tmp/ruby/lib/ruby/2.3.0/x86_64-linux
/enc/encdb.so
7f13548ab000-7f1354aaa000 ---p 00002000 00:24 203974 /tmp/ruby/lib/ruby/2.3.0/x86_64-linux
/enc/encdb.so
7f1354aaa000-7f1354aab000 r--p 00001000 00:24 203974 /tmp/ruby/lib/ruby/2.3.0/x86_64-linux
/enc/encdb.so
7f1354aab000-7f1354aac000 rw-p 00002000 00:24 203974 /tmp/ruby/lib/ruby/2.3.0/x86_64-linux
/enc/encdb.so
7f1354aac000-7f135b01f000 r--p 00000000 08:01 279468 /usr/lib/locale/locale-archive
7f135b01f000-7f135b097000 r-xp 00000000 08:01 269065 /usr/lib64/libfreebl3.so
7f135b097000-7f135b296000 ---p 00078000 08:01 269065 /usr/lib64/libfreebl3.so
7f135b296000-7f135b298000 r--p 00077000 08:01 269065 /usr/lib64/libfreebl3.so
7f135b298000-7f135b299000 rw-p 00079000 08:01 269065 /usr/lib64/libfreebl3.so
7f135b299000-7f135b29d000 rw-p 00000000 00:00 0
7f135b29d000-7f135b450000 r-xp 00000000 08:01 269523 /usr/lib64/libc-2.20.so
7f135b450000-7f135b650000 ---p 001b3000 08:01 269523 /usr/lib64/libc-2.20.so
7f135b650000-7f135b654000 r--p 001b3000 08:01 269523 /usr/lib64/libc-2.20.so
7f135b654000-7f135b656000 rw-p 001b7000 08:01 269523 /usr/lib64/libc-2.20.so
7f135b656000-7f135b65a000 rw-p 00000000 00:00 0
7f135b65a000-7f135b761000 r-xp 00000000 08:01 269656 /usr/lib64/libm-2.20.so
7f135b761000-7f135b960000 ---p 00107000 08:01 269656 /usr/lib64/libm-2.20.so
7f135b960000-7f135b961000 r--p 00106000 08:01 269656 /usr/lib64/libm-2.20.so
7f135b961000-7f135b962000 rw-p 00107000 08:01 269656 /usr/lib64/libm-2.20.so
7f135b962000-7f135b969000 r-xp 00000000 08:01 269606 /usr/lib64/libcrypt-2.20.so
7f135b969000-7f135bb68000 ---p 00007000 08:01 269606 /usr/lib64/libcrypt-2.20.so
7f135bb68000-7f135bb69000 r--p 00006000 08:01 269606 /usr/lib64/libcrypt-2.20.so
7f135bb69000-7f135bb6a000 rw-p 00007000 08:01 269606 /usr/lib64/libcrypt-2.20.so
7f135bb6a000-7f135bb98000 rw-p 00000000 00:00 0
7f135bb98000-7f135bb9b000 r-xp 00000000 08:01 269633 /usr/lib64/libdl-2.20.so
7f135bb9b000-7f135bd9a000 ---p 00003000 08:01 269633 /usr/lib64/libdl-2.20.so
7f135bd9a000-7f135bd9b000 r--p 00002000 08:01 269633 /usr/lib64/libdl-2.20.so
7f135bd9b000-7f135bd9c000 rw-p 00003000 08:01 269633 /usr/lib64/libdl-2.20.so
7f135bd9c000-7f135bdb3000 r-xp 00000000 08:01 270055 /usr/lib64/libpthread-2.20.so
7f135bdb3000-7f135bfb2000 ---p 00017000 08:01 270055 /usr/lib64/libpthread-2.20.so
7f135bfb2000-7f135bfb3000 r--p 00016000 08:01 270055 /usr/lib64/libpthread-2.20.so
7f135bfb3000-7f135bfb4000 rw-p 00017000 08:01 270055 /usr/lib64/libpthread-2.20.so
7f135bfb4000-7f135bfb8000 rw-p 00000000 00:00 0
7f135bfb8000-7f135bfd9000 r-xp 00000000 08:01 279457 /usr/lib64/ld-2.20.so
7f135c0d8000-7f135c1d9000 rw-p 00000000 00:00 0
7f135c1d9000-7f135c1da000 r--p 00021000 08:01 279457 /usr/lib64/ld-2.20.so
7f135c1da000-7f135c1db000 rw-p 00022000 08:01 279457 /usr/lib64/ld-2.20.so
7f135c1db000-7f135c1dc000 rw-p 00000000 00:00 0
7f135c1dc000-7f135c4b4000 r-xp 00000000 00:24 203922 /tmp/ruby/bin/ruby
7f135c56a000-7f135c69a000 rw-p 00000000 00:00 0
7f135c6ae000-7f135c6af000 rw-p 00000000 00:00 0
7f135c6af000-7f135c6b0000 ---p 00000000 00:00 0
7f135c6b0000-7f135c6b4000 rw-p 00000000 00:00 0 [stack:10736]
7f135c6b4000-7f135c6b9000 r--p 002d8000 00:24 203922 /tmp/ruby/bin/ruby
7f135c6b9000-7f135c6ba000 rw-p 002dd000 00:24 203922 /tmp/ruby/bin/ruby
7f135c6ba000-7f135c6cc000 rw-p 00000000 00:00 0
7f135daba000-7f135e0a7000 rw-p 00000000 00:00 0 [heap]
7fffdec3f000-7ffffdf43f000 rw-p 00000000 00:00 0 [stack]
7ffffdf512000-7ffffdf514000 r--p 00000000 00:00 0 [vvar]
7ffffdf514000-7ffffdf516000 r-xp 00000000 00:00 0 [vdso]
ffffffff600000-ffffffff601000 r-xp 00000000 00:00 0 [vsyscall]

```

[NOTE]

You may have encountered a bug in the Ruby interpreter or extension libraries.
Bug reports are welcome.
For details: <http://www.ruby-lang.org/bugreport.html>

System Information

```
$ uname -a
```

```
Linux localhost.localdomain 4.0.5-200.fc21.x86_64 #1 SMP Mon Jun 8 16:25:02 UTC 2015 x86_64 x86_64 x86_64 GNU/
```

```
Linux
$ ruby --version
ruby 2.3.0dev (2015-06-26 trunk 51033) [x86_64-linux]
```

Files

rspec_ruby_segfault.rb	233 Bytes	11/26/2014	Ajedi32 (Andrew M)
sample_output	26 KB	11/26/2014	Ajedi32 (Andrew M)