

Ruby - Bug #633

dl segfaults on x86_64-linux systems

10/11/2008 08:06 AM - floering (Benjamin Floering)

Status:	Closed	
Priority:	Normal	
Assignee:	takano32 (Mitsuhiro TAKANO)	
Target version:	1.9.1 Release Candidate	
ruby -v:		
Description		Backport:
=begin Tested systems: RHEL3_64, RHEL4_64, and RHEL5_64. All segfault running tests in ext/dl/test. Confirmed that this is not as big an issue on 32bit (no segfault, but two errors). \$ ruby test_all.rb Loaded suite test_all Started .../ruby/ext/dl/test/test_dl2.rb:78: [BUG] Segmentation fault ruby 1.9.0 (2008-10-11 revision 19752) [x86_64-linux] -- control frame ----- c:0020 p:---- s:0074 b:0074 l:000073 d:000073 CFUNC :call c:0019 p:0101 s:0070 b:0070 l:000380 d:000380 METHOD /ruby/ext/dl/test/test_dl2.rb:78 c:0018 p:0051 s:0064 b:0064 l:000063 d:000063 METHOD /ruby19/lib/ruby/1.9.0/test/unit/testcase.rb:81 c:0017 p:0017 s:0059 b:0059 l:000052 d:000058 BLOCK /ruby19/lib/ruby/1.9.0/test/unit/testsuite.rb:34 c:0016 p:---- s:0058 b:0058 l:000057 d:000057 FINISH :inherited c:0015 p:---- s:0056 b:0056 l:000055 d:000055 CFUNC :each c:0014 p:0032 s:0053 b:0053 l:000052 d:000052 METHOD /ruby19/lib/ruby/1.9.0/test/unit/testsuite.rb:33 c:0013 p:0017 s:0048 b:0048 l:000041 d:000047 BLOCK /ruby19/lib/ruby/1.9.0/test/unit/testsuite.rb:34 c:0012 p:---- s:0047 b:0047 l:000046 d:000046 FINISH :(null) c:0011 p:---- s:0045 b:0045 l:000044 d:000044 CFUNC :each c:0010 p:0032 s:0042 b:0042 l:000041 d:000041 METHOD /ruby19/lib/ruby/1.9.0/test/unit/testsuite.rb:33 c:0009 p:0146 s:0037 b:0037 l:000ac8 d:000ac8 METHOD /ruby19/lib/ruby/1.9.0/test/unit/ui/testrunnermediator.rb:46 c:0008 p:0010 s:0028 b:0028 l:000027 d:000027 METHOD /ruby19/lib/ruby/1.9.0/test/unit/ui/console/testrunner.rb:67 c:0007 p:0029 s:0025 b:0025 l:000024 d:000024 METHOD /ruby19/lib/ruby/1.9.0/test/unit/ui/console/testrunner.rb:41 c:0006 p:0028 s:0022 b:0022 l:000021 d:000021 METHOD /ruby19/lib/ruby/1.9.0/test/unit/ui/testrunnerutilities.rb:29 c:0005 p:0062 s:0017 b:0017 l:000016 d:000016 METHOD /ruby19/lib/ruby/1.9.0/test/unit/autorunner.rb:213 c:0004 p:0080 s:0013 b:0013 l:000012 d:000012 METHOD		

/ruby19/lib/ruby/1.9.0/test/unit/autorunner.rb:12

c:0003 p:0046 s:0005 b:0004 l:001bc8 d:000003 BLOCK

/ruby19/lib/ruby/1.9.0/test/unit.rb:278

c:0002 p:---- s:0004 b:0004 l:000003 d:000003 FINISH :inherited

c:0001 p:0000 s:0002 b:0002 l:000001 d:000001 TOP

```
DBG> : "/ruby/ext/dl/test/test_dl2.rb:78:in call" DBG> : "/ruby/ext/dl/test/test_dl2.rb:78:in test_callback"
DBG> : "/ruby19/lib/ruby/1.9.0/test/unit/testcase.rb:81:in run" DBG> : "/ruby19/lib/ruby/1.9.0/test/unit/testsuite.rb:34:in block in run"
DBG> : "/ruby19/lib/ruby/1.9.0/test/unit/testsuite.rb:33:in each" DBG> : "/ruby19/lib/ruby/1.9.0/test/unit/testsuite.rb:33:in run"
DBG> : "/ruby19/lib/ruby/1.9.0/test/unit/testsuite.rb:34:in block in run" DBG> : "/ruby19/lib/ruby/1.9.0/test/unit/testsuite.rb:33:in each"
DBG> : "/ruby19/lib/ruby/1.9.0/test/unit/testsuite.rb:33:in run" DBG> : "/ruby19/lib/ruby/1.9.0/test/unit/ui/testrunnermediator.rb:46:in
run_suite"
DBG> : "/ruby19/lib/ruby/1.9.0/test/unit/ui/console/testrunner.rb:67:in start_mediator" DBG> :
"/ruby19/lib/ruby/1.9.0/test/unit/ui/console/testrunner.rb:41:in start"
DBG> : "/ruby19/lib/ruby/1.9.0/test/unit/ui/testrunnerutilities.rb:29:in run" DBG> : "/ruby19/lib/ruby/1.9.0/test/unit/autorunner.rb:213:in
run"
DBG> : "/ruby19/lib/ruby/1.9.0/test/unit/autorunner.rb:12:in run" DBG> : "/ruby19/lib/ruby/1.9.0/test/unit.rb:278:in block in <top
(required)>"
: 884 segmentation fault (core dumped) ruby test_all.rb

dl 64 bit was working in 1.8. Are we dropping support for 64 bit in 1.9?
=end
```

Associated revisions

Revision 0781d24aaa41d87802592f325ccf8ccfe9bad04b - 12/28/2008 08:10 AM - takano32 (Mitsuhiro TAKANO)

Sun Dec 28 17:10:13 2008 TAKANO Mitsuhiro (takano32) tak@no32.tk

```
* ext/dl/test/test_dl2.rb: modify strncpy, strcpy, qsort, types.
Bug #633 [ruby-core:19289]
* ext/dl/test/test_base.rb: /lib/libc.so is x86_64 binary in x86_64 architecture.
```

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/trunk@21110 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

Revision 0781d24aaa41d87802592f325ccf8ccfe9bad04b - 12/28/2008 08:10 AM - takano32 (Mitsuhiro TAKANO)

Sun Dec 28 17:10:13 2008 TAKANO Mitsuhiro (takano32) tak@no32.tk

```
* ext/dl/test/test_dl2.rb: modify strncpy, strcpy, qsort, types.
Bug #633 [ruby-core:19289]
* ext/dl/test/test_base.rb: /lib/libc.so is x86_64 binary in x86_64 architecture.
```

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/trunk@21110 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

Revision 0781d24a - 12/28/2008 08:10 AM - takano32 (Mitsuhiro TAKANO)

Sun Dec 28 17:10:13 2008 TAKANO Mitsuhiro (takano32) tak@no32.tk

```
* ext/dl/test/test_dl2.rb: modify strncpy, strcpy, qsort, types.
Bug #633 [ruby-core:19289]
* ext/dl/test/test_base.rb: /lib/libc.so is x86_64 binary in x86_64 architecture.
```

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/trunk@21110 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

Revision b78fe145f3072174fe02eba714baa220bc58dbb9 - 12/29/2008 07:18 AM - yugui (Yuki Sonoda)

merges r21110, r21111 and r21140 from trunk into ruby_1_9_1.

```
* ext/dl/test/test_dl2.rb: modify strncpy, strcpy, qsort, types.
Bug #633 [ruby-core:19289]
* ext/dl/test/test_base.rb: /lib/libc.so is x86_64 binary in x86_64 architecture.
```

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/branches/ruby_1_9_1@21151 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

Revision b78fe145f3072174fe02eba714baa220bc58dbb9 - 12/29/2008 07:18 AM - yugui (Yuki Sonoda)

merges r21110, r21111 and r21140 from trunk into ruby_1_9_1.

```
* ext/dl/test/test_dl2.rb: modify strncpy, strcpy, qsort, types.
Bug #633 [ruby-core:19289]
* ext/dl/test/test_base.rb: /lib/libc.so is x86_64 binary in x86_64 architecture.
```

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/branches/ruby_1_9_1@21151 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

Revision b78fe145 - 12/29/2008 07:18 AM - yugui (Yuki Sonoda)

merges r21110, r21111 and r21140 from trunk into ruby_1_9_1.

* ext/dl/test/test_dl2.rb: modify strncpy, strcpy, qsort, types.

Bug #633 [ruby-core:19289]

* ext/dl/test/test_base.rb: /lib/libc.so is x86_64 binary in x86_64 architecture.

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/branches/ruby_1_9_1@21151 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

Revision d0ed5a93786881e2ddda99d0c83e4d1a216a3ca8 - 12/29/2008 02:54 PM - ko1 (Koichi Sasada)

- ext/dl/test/test_base.rb: add libc search logic.
this patch is written by Takehiro Kubo.
[ruby-core:20963] [Bug #932]
- ext/dl/dl.h: Add "...". as the last argument.
this patch is written by Takehiro Kubo.
Bug #633 [ruby-core:19289]
- ext/dl/lib/dl/stack.rb: add add_padding() to calculate alignment. this patch is written by Takehiro Kubo.
Bug #633 [ruby-core:19289]
- ext/dl/test/test_func.rb: atof()'s return value is double.
this patch is written by Takehiro Kubo.
Bug #633 [ruby-core:19289]
- ext/dl/test/test_import.rb:
 - atof()'s return value is double.
 - The types of qsort's second and third argument are size_t.
 - fprintf()'s return value is int.this patch is written by Takehiro Kubo.
Bug #633 [ruby-core:19289]

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/trunk@21182 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

Revision d0ed5a93786881e2ddda99d0c83e4d1a216a3ca8 - 12/29/2008 02:54 PM - ko1 (Koichi Sasada)

- ext/dl/test/test_base.rb: add libc search logic.
this patch is written by Takehiro Kubo.
[ruby-core:20963] [Bug #932]
- ext/dl/dl.h: Add "...". as the last argument.
this patch is written by Takehiro Kubo.
Bug #633 [ruby-core:19289]
- ext/dl/lib/dl/stack.rb: add add_padding() to calculate alignment. this patch is written by Takehiro Kubo.
Bug #633 [ruby-core:19289]
- ext/dl/test/test_func.rb: atof()'s return value is double.
this patch is written by Takehiro Kubo.
Bug #633 [ruby-core:19289]
- ext/dl/test/test_import.rb:
 - atof()'s return value is double.
 - The types of qsort's second and third argument are size_t.
 - fprintf()'s return value is int.this patch is written by Takehiro Kubo.
Bug #633 [ruby-core:19289]

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/trunk@21182 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

Revision d0ed5a93 - 12/29/2008 02:54 PM - ko1 (Koichi Sasada)

- ext/dl/test/test_base.rb: add libc search logic.
this patch is written by Takehiro Kubo.
[ruby-core:20963] [Bug #932]
- ext/dl/dl.h: Add "...". as the last argument.
this patch is written by Takehiro Kubo.
Bug #633 [ruby-core:19289]
- ext/dl/lib/dl/stack.rb: add add_padding() to calculate alignment. this patch is written by Takehiro Kubo.
Bug #633 [ruby-core:19289]
- ext/dl/test/test_func.rb: atof()'s return value is double.
this patch is written by Takehiro Kubo.
Bug #633 [ruby-core:19289]
- ext/dl/test/test_import.rb:

- atof()'s return value is double.
- The types of qsort's second and third argument are size_t.
- fprintf()'s return value is int.
this patch is written by Takehiro Kubo.
Bug #633 [ruby-core:19289]

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/trunk@21182 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

Revision e8f6d8493678a828ae345f86c680601d2661442a - 12/30/2008 10:32 AM - yugui (Yuki Sonoda)

merges r21177 and r21182 from trunk into ruby_1_9_1.

- ext/dl/test/test_base.rb: add x86_64-linux's case again. #932
--
- ext/dl/test/test_base.rb: add libc search logic.
this patch is written by Takehiro Kubo.
[ruby-core:20963] [Bug #932]
- ext/dl/dl.h: Add "... " as the last argument.
this patch is written by Takehiro Kubo.
Bug #633 [ruby-core:19289]
- ext/dl/lib/dl/stack.rb: add add_padding() to calculate
alignment. this patch is written by Takehiro Kubo.
Bug #633 [ruby-core:19289]
- ext/dl/test/test_func.rb: atof()'s return value is double.
this patch is written by Takehiro Kubo.
Bug #633 [ruby-core:19289]
- ext/dl/test/test_import.rb:
 - atof()'s return value is double.
 - The types of qsort's second and third argument are size_t.
 - fprintf()'s return value is int.
this patch is written by Takehiro Kubo.
Bug #633 [ruby-core:19289]

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/branches/ruby_1_9_1@21195 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

Revision e8f6d8493678a828ae345f86c680601d2661442a - 12/30/2008 10:32 AM - yugui (Yuki Sonoda)

merges r21177 and r21182 from trunk into ruby_1_9_1.

- ext/dl/test/test_base.rb: add x86_64-linux's case again. #932
--
- ext/dl/test/test_base.rb: add libc search logic.
this patch is written by Takehiro Kubo.
[ruby-core:20963] [Bug #932]
- ext/dl/dl.h: Add "... " as the last argument.
this patch is written by Takehiro Kubo.
Bug #633 [ruby-core:19289]
- ext/dl/lib/dl/stack.rb: add add_padding() to calculate
alignment. this patch is written by Takehiro Kubo.
Bug #633 [ruby-core:19289]
- ext/dl/test/test_func.rb: atof()'s return value is double.
this patch is written by Takehiro Kubo.
Bug #633 [ruby-core:19289]
- ext/dl/test/test_import.rb:
 - atof()'s return value is double.
 - The types of qsort's second and third argument are size_t.
 - fprintf()'s return value is int.
this patch is written by Takehiro Kubo.
Bug #633 [ruby-core:19289]

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/branches/ruby_1_9_1@21195 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

Revision e8f6d849 - 12/30/2008 10:32 AM - yugui (Yuki Sonoda)

merges r21177 and r21182 from trunk into ruby_1_9_1.

- ext/dl/test/test_base.rb: add x86_64-linux's case again. #932
--
- ext/dl/test/test_base.rb: add libc search logic.
this patch is written by Takehiro Kubo.
[ruby-core:20963] [Bug #932]
- ext/dl/dl.h: Add "... " as the last argument.
this patch is written by Takehiro Kubo.
Bug #633 [ruby-core:19289]
- ext/dl/lib/dl/stack.rb: add add_padding() to calculate

- alignment. this patch is written by Takehiro Kubo.
Bug #633 [ruby-core:19289]
- ext/dl/test/test_func.rb: atof()'s return value is double.
this patch is written by Takehiro Kubo.
Bug #633 [ruby-core:19289]
 - ext/dl/test/test_import.rb:
 - atof()'s return value is double.
 - The types of qsort's second and third argument are size_t.
 - fprintf()'s return value is int.
this patch is written by Takehiro Kubo.
Bug #633 [ruby-core:19289]

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/branches/ruby_1_9_1@21195 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

History

#1 - 10/15/2008 04:19 AM - radarek (Radosław Bulat)

=begin
I want to confirm this issue. I have exactly the same output (of course paths are different).

```
$ ruby1.9 --version
ruby 1.9.0 (2008-10-14 revision 19786) [x86_64-linux]
```

=end

#2 - 10/29/2008 01:38 PM - rogerdpack (Roger Pack)

=begin
Here's my results from 32-bit OS X.
ruby19 test_all.rb
test_all.rb
Loaded suite test_all
Started

Finished in 0.000820 seconds.

0 tests, 0 assertions, 0 failures, 0 errors, 0 skips

=end

#3 - 11/29/2008 04:20 PM - ko1 (Koichi Sasada)

- Assignee set to nobu (Nobuyoshi Nakada)

=begin

=end

#4 - 12/11/2008 12:35 PM - yugui (Yuki Sonoda)

- Assignee changed from nobu (Nobuyoshi Nakada) to takano32 (Mitsuhiro TAKANO)

- Target version set to 1.9.1 Release Candidate

=begin

=end

#5 - 12/21/2008 12:10 AM - yugui (Yuki Sonoda)

- Due date set to 12/24/2008

- Assignee deleted (takano32 (Mitsuhiro TAKANO))

=begin

=end

#6 - 12/26/2008 06:06 PM - znmeb (Ed Borasky)

- File ruby-configure.log added

- File R-make.log added

- File ruby-install.log added

- File ruby-test.log added

=begin
I'm trying to reproduce this on my system. This machine is an Athlon64 X2 (dual-core x86_64). OS is openSUSE 11.1, 2.6.27 kernel, and gcc is "gcc (SUSE Linux) 4.3.2 [gcc-4_3-branch revision 141291]". I downloaded the Ruby source via subversion from trunk. The "autoconf", "configure", "make" and "make install" all ran fine, as did "make test". So I tried the test above. No segfaults, but I did get an interesting error message:

```
znmeb@DreamScape:~/Packages> export PATH=~/.test/bin:$PATH
znmeb@DreamScape:~/Packages> cd ruby/ext/dl/test/
znmeb@DreamScape:~/Packages/ruby/ext/dl/test> which ruby
/home/znmeb/test/bin/ruby
znmeb@DreamScape:~/Packages/ruby/ext/dl/test> ruby --version
ruby 1.9.1 (2008-12-26 patchlevel-5000 trunk 21067) [x86_64-linux]
znmeb@DreamScape:~/Packages/ruby/ext/dl/test> ruby test_all.rb
nil
Loaded suite test_all
Started
EEEEEEEEEEEEEEEEEEEE
Finished in 0.002599 seconds.
```

1. Error:
test_empty(DL::TestBase):
DL::DLLError: /lib/libc.so.6: wrong ELF class: ELFCLASS32
/home/znmeb/Packages/ruby/ext/dl/test/test_base.rb:29:in initialize' /home/znmeb/Packages/ruby/ext/dl/test/test_base.rb:29:in dlopen'
/home/znmeb/Packages/ruby/ext/dl/test/test_base.rb:29:in `setup'
2. Error:
test_call_double(DL::TestDL):
DL::DLLError: /lib/libc.so.6: wrong ELF class: ELFCLASS32
/home/znmeb/Packages/ruby/ext/dl/test/test_base.rb:29:in initialize' /home/znmeb/Packages/ruby/ext/dl/test/test_base.rb:29:in dlopen'
/home/znmeb/Packages/ruby/ext/dl/test/test_base.rb:29:in `setup'
3. Error:
test_call_int(DL::TestDL):
DL::DLLError: /lib/libc.so.6: wrong ELF class: ELFCLASS32
/home/znmeb/Packages/ruby/ext/dl/test/test_base.rb:29:in initialize' /home/znmeb/Packages/ruby/ext/dl/test/test_base.rb:29:in dlopen'
/home/znmeb/Packages/ruby/ext/dl/test/test_base.rb:29:in `setup'
4. Error:
test_call_long(DL::TestDL):
DL::DLLError: /lib/libc.so.6: wrong ELF class: ELFCLASS32
/home/znmeb/Packages/ruby/ext/dl/test/test_base.rb:29:in initialize' /home/znmeb/Packages/ruby/ext/dl/test/test_base.rb:29:in dlopen'
/home/znmeb/Packages/ruby/ext/dl/test/test_base.rb:29:in `setup'
5. Error:
test_callback(DL::TestDL):
DL::DLLError: /lib/libc.so.6: wrong ELF class: ELFCLASS32
/home/znmeb/Packages/ruby/ext/dl/test/test_base.rb:29:in initialize' /home/znmeb/Packages/ruby/ext/dl/test/test_base.rb:29:in dlopen'
/home/znmeb/Packages/ruby/ext/dl/test/test_base.rb:29:in `setup'
6. Error:
test_cptr(DL::TestDL):
DL::DLLError: /lib/libc.so.6: wrong ELF class: ELFCLASS32
/home/znmeb/Packages/ruby/ext/dl/test/test_base.rb:29:in initialize' /home/znmeb/Packages/ruby/ext/dl/test/test_base.rb:29:in dlopen'
/home/znmeb/Packages/ruby/ext/dl/test/test_base.rb:29:in `setup'
7. Error:
test_dlwrap(DL::TestDL):
DL::DLLError: /lib/libc.so.6: wrong ELF class: ELFCLASS32
/home/znmeb/Packages/ruby/ext/dl/test/test_base.rb:29:in initialize' /home/znmeb/Packages/ruby/ext/dl/test/test_base.rb:29:in dlopen'
/home/znmeb/Packages/ruby/ext/dl/test/test_base.rb:29:in `setup'
8. Error:
test_empty(DL::TestDL):
DL::DLLError: /lib/libc.so.6: wrong ELF class: ELFCLASS32
/home/znmeb/Packages/ruby/ext/dl/test/test_base.rb:29:in initialize' /home/znmeb/Packages/ruby/ext/dl/test/test_base.rb:29:in dlopen'
/home/znmeb/Packages/ruby/ext/dl/test/test_base.rb:29:in `setup'
9. Error:
test_sin(DL::TestDL):
DL::DLLError: /lib/libc.so.6: wrong ELF class: ELFCLASS32
/home/znmeb/Packages/ruby/ext/dl/test/test_base.rb:29:in initialize' /home/znmeb/Packages/ruby/ext/dl/test/test_base.rb:29:in dlopen'
/home/znmeb/Packages/ruby/ext/dl/test/test_base.rb:29:in `setup'
10. Error:

```

test_strcpy(DL::TestDL):
DL::DLError: /lib/libc.so.6: wrong ELF class: ELFCLASS32
/home/znmeb/Packages/ruby/ext/dl/test/test_base.rb:29:in initialize' /home/znmeb/Packages/ruby/ext/dl/test/test_base.rb:29:in dlopen'
/home/znmeb/Packages/ruby/ext/dl/test/test_base.rb:29:in `setup'

11. Error:
test_strlen(DL::TestDL):
DL::DLError: /lib/libc.so.6: wrong ELF class: ELFCLASS32
/home/znmeb/Packages/ruby/ext/dl/test/test_base.rb:29:in initialize' /home/znmeb/Packages/ruby/ext/dl/test/test_base.rb:29:in dlopen'
/home/znmeb/Packages/ruby/ext/dl/test/test_base.rb:29:in `setup'

12. Error:
test_atof(DL::TestFunc):
DL::DLError: /lib/libc.so.6: wrong ELF class: ELFCLASS32
/home/znmeb/Packages/ruby/ext/dl/test/test_base.rb:29:in initialize' /home/znmeb/Packages/ruby/ext/dl/test/test_base.rb:29:in dlopen'
/home/znmeb/Packages/ruby/ext/dl/test/test_base.rb:29:in `setup'

13. Error:
test_empty(DL::TestFunc):
DL::DLError: /lib/libc.so.6: wrong ELF class: ELFCLASS32
/home/znmeb/Packages/ruby/ext/dl/test/test_base.rb:29:in initialize' /home/znmeb/Packages/ruby/ext/dl/test/test_base.rb:29:in dlopen'
/home/znmeb/Packages/ruby/ext/dl/test/test_base.rb:29:in `setup'

14. Error:
test_isdigit(DL::TestFunc):
DL::DLError: /lib/libc.so.6: wrong ELF class: ELFCLASS32
/home/znmeb/Packages/ruby/ext/dl/test/test_base.rb:29:in initialize' /home/znmeb/Packages/ruby/ext/dl/test/test_base.rb:29:in dlopen'
/home/znmeb/Packages/ruby/ext/dl/test/test_base.rb:29:in `setup'

15. Error:
test_qsort1(DL::TestFunc):
DL::DLError: /lib/libc.so.6: wrong ELF class: ELFCLASS32
/home/znmeb/Packages/ruby/ext/dl/test/test_base.rb:29:in initialize' /home/znmeb/Packages/ruby/ext/dl/test/test_base.rb:29:in dlopen'
/home/znmeb/Packages/ruby/ext/dl/test/test_base.rb:29:in `setup'

16. Error:
test_qsort2(DL::TestFunc):
DL::DLError: /lib/libc.so.6: wrong ELF class: ELFCLASS32
/home/znmeb/Packages/ruby/ext/dl/test/test_base.rb:29:in initialize' /home/znmeb/Packages/ruby/ext/dl/test/test_base.rb:29:in dlopen'
/home/znmeb/Packages/ruby/ext/dl/test/test_base.rb:29:in `setup'

17. Error:
test_strcpy(DL::TestFunc):
DL::DLError: /lib/libc.so.6: wrong ELF class: ELFCLASS32
/home/znmeb/Packages/ruby/ext/dl/test/test_base.rb:29:in initialize' /home/znmeb/Packages/ruby/ext/dl/test/test_base.rb:29:in dlopen'
/home/znmeb/Packages/ruby/ext/dl/test/test_base.rb:29:in `setup'

18. Error:
test_strtod(DL::TestFunc):
DL::DLError: /lib/libc.so.6: wrong ELF class: ELFCLASS32
/home/znmeb/Packages/ruby/ext/dl/test/test_base.rb:29:in initialize' /home/znmeb/Packages/ruby/ext/dl/test/test_base.rb:29:in dlopen'
/home/znmeb/Packages/ruby/ext/dl/test/test_base.rb:29:in `setup'

18 tests, 0 assertions, 0 failures, 18 errors, 0 skips
/home/znmeb/test/lib/ruby/1.9.1/dl/import.rb:52:in rescue in block in dlopen': can't load /lib/libc.so.6 (DL::DLError) from
/home/znmeb/test/lib/ruby/1.9.1/dl/import.rb:49:in block in dlopen'
from /home/znmeb/test/lib/ruby/1.9.1/dl/import.rb:40:in collect' from /home/znmeb/test/lib/ruby/1.9.1/dl/import.rb:40:in dlopen'
from /home/znmeb/Packages/ruby/ext/dl/test/test_import.rb:7:in <module:LIBC>' from /home/znmeb/Packages/ruby/ext/dl/test/test_import.rb:5:in
module:DL'
from /home/znmeb/Packages/ruby/ext/dl/test/test_import.rb:4:in <top (required)>' from test_all.rb:6:in require'
from test_all.rb:6:in ``
znmeb@DreamScape:~/Packages/ruby/ext/dl/test>

```

In other words, it looks like I have linked against the wrong "libc" -- a 32-bit one! Could that be what's happening on the 64-bit Red Hat systems too? I think the "libc" should be "/lib64/libc.so.6":

```

znmeb@DreamScape:~/Packages> locate libc.so
/lib/libc.so.6
/lib64/libc.so.6
/usr/lib64/libc.so
znmeb@DreamScape:~/Packages> file /lib/libc.so.6
/lib/libc.so.6: symbolic link to libc-2.9.so' znmeb@DreamScape:~/Packages> file /lib64/libc.so.6 /lib64/libc.so.6: symbolic link to libc-2.9.so'
znmeb@DreamScape:~/Packages> file /usr/lib64/libc.so
/usr/lib64/libc.so: ASCII C program text

```

```
znmeb@DreamScape:~/Packages> file /lib/libc-2.9.so
/lib/libc-2.9.so: ELF 32-bit LSB shared object, Intel 80386, version 1 (SYSV), for GNU/Linux 2.6.4, dynamically linked (uses shared libs), stripped
znmeb@DreamScape:~/Packages> file /lib64/libc-2.9.so
/lib64/libc-2.9.so: ELF 64-bit LSB shared object, x86-64, version 1 (SYSV), for GNU/Linux 2.6.4, dynamically linked (uses shared libs), stripped
znmeb@DreamScape:~/Packages>
```

I'm attaching the output of the "make" step if that's any help. Incidentally, the default installed Ruby on openSUSE 11.1 is 1.8.7:

```
znmeb@DreamScape:~/Packages> which ruby
/usr/bin/ruby
znmeb@DreamScape:~/Packages> ruby --version
ruby 1.8.7 (2008-08-11 patchlevel 72) [x86_64-linux]
znmeb@DreamScape:~/Packages>
```

=end

#7 - 12/26/2008 06:08 PM - znmeb (Ed Borasky)

- File *ruby-make.log* added

```
=begin
Oops ... attached the wrong log file -- here's the right one!
=end
```

#8 - 12/26/2008 11:51 PM - febuiles (Federico Builes)

```
=begin
Ed: This segfaults in Ubuntu 8.10 x86_x64 too so I think the libc issue might be related to OpenSuse.
=end
```

#9 - 12/27/2008 03:11 AM - znmeb (Ed Borasky)

```
=begin
A little good news:
```

1. I can get rid of the library issue on my system.
2. I found the error in `"/ext/dl/test/test_base.rb"` that's causing the library issue. I don't know about how to port this to other distros, though.

```
1 require 'test/unit'
2 require 'dl'
3
4 case RUBY_PLATFORM
5 when /cygwin/
6   LIBC_SO = "cygwin1.dll"
7   LIBM_SO = "cygwin1.dll"
8 when /linux/
9   LIBC_SO = "/lib/libc.so.6"
10  LIBM_SO = "/lib/libm.so.6"
```

Other distros must symlink `"/lib"` to `"/lib64"`. In any event when I changed the constants to point to `"/lib64"` the library errors went away. So there probably needs to be two branches in the "case" -- one for 32-bit Linux and one for 64-bit Linux. I'll go ahead and file another bug to that effect specific to openSUSE 11.1 / x64

The bad news is that if I fix the library issue, I get segfaults now. But that's really good news; "gdb" should be able to help narrow this down. I'll see if I can get a C-level traceback next.

=end

#10 - 12/27/2008 04:25 AM - znmeb (Ed Borasky)

- File *ruby-segfault.log* added
- File *ruby-c-backtrace.txt* added

```
=begin
OK ... I have a core dump file and a C level traceback with "gdb". I've attached the files, rather than putting the details in line. Enough stuff was "optimized out" that I think I'm going to recompile with "-O0" (no optimization) and see if that helps / makes it go away / makes it easier to find.
=end
```

#11 - 12/27/2008 05:34 AM - znmeb (Ed Borasky)

- File *ruby-c-backtrace-noopt.txt* added

```
=begin
```

Here's a C-level backtrace with no optimization. It looks a lot better -- I can see the call from Ruby out to the system library now, and the whole path to the segfault. It's around line [#11](#):

```
#10 0x00007f8bd53d584c in qsort_r () from /lib64/libc.so.6
#11 0x00007f8bd4ce23c0 in rb_dlcfunc_call (self=11574080, ary=11573400) at cfunc.c:276
#12 0x0000000000508cbc in call_cfunc (func=0x7f8bd4ce200b <rb_dlcfunc_call>, recv=11574080, len=1, argc=1, argv=0x7f8bd62631b0) at
vm_insnhelper.c:290
```

I'm out of ideas at this point. Does the C-level backtrace mean anything to anyone else??

=end

#12 - 12/27/2008 05:36 AM - znmeb (Ed Borasky)

- File *ruby-c-backtrace-noopt.txt* added

```
=begin
Here's a C-level backtrace with no optimization. It looks a lot better -- I can see the call from Ruby out to the system library now, and the whole path to
the segfault. It's around line #11:
```

```
#10 0x00007f8bd53d584c in qsort_r () from /lib64/libc.so.6
#11 0x00007f8bd4ce23c0 in rb_dlcfunc_call (self=11574080, ary=11573400) at cfunc.c:276
#12 0x0000000000508cbc in call_cfunc (func=0x7f8bd4ce200b <rb_dlcfunc_call>, recv=11574080, len=1, argc=1, argv=0x7f8bd62631b0) at
vm_insnhelper.c:290
```

I'm out of ideas at this point. Does the C-level backtrace mean anything to anyone else??

=end

#13 - 12/27/2008 05:37 AM - znmeb (Ed Borasky)

- File *ruby-c-backtrace-noopt.txt* added

```
=begin
Here's a C-level backtrace with no optimization. It looks a lot better -- I can see the call from Ruby out to the system library now, and the whole path to
the segfault. It's around line #11:
```

```
#10 0x00007f8bd53d584c in qsort_r () from /lib64/libc.so.6
#11 0x00007f8bd4ce23c0 in rb_dlcfunc_call (self=11574080, ary=11573400) at cfunc.c:276
#12 0x0000000000508cbc in call_cfunc (func=0x7f8bd4ce200b <rb_dlcfunc_call>, recv=11574080, len=1, argc=1, argv=0x7f8bd62631b0) at
vm_insnhelper.c:290
```

I'm out of ideas at this point. Does the C-level backtrace mean anything to anyone else??

=end

#14 - 12/27/2008 05:40 AM - znmeb (Ed Borasky)

- File *ruby-c-backtrace-noopt.txt* added

```
=begin
Here's a C-level backtrace with no optimization. It looks a lot better -- I can see the call from Ruby out to the system library now, and the whole path to
the segfault. It's around line #11:
```

```
#10 0x00007f8bd53d584c in qsort_r () from /lib64/libc.so.6
#11 0x00007f8bd4ce23c0 in rb_dlcfunc_call (self=11574080, ary=11573400) at cfunc.c:276
#12 0x0000000000508cbc in call_cfunc (func=0x7f8bd4ce200b <rb_dlcfunc_call>, recv=11574080, len=1, argc=1, argv=0x7f8bd62631b0) at
vm_insnhelper.c:290
```

I'm out of ideas at this point. Does the C-level backtrace mean anything to anyone else??

=end

#15 - 12/28/2008 09:27 AM - kubo (Takehiro Kubo)

```
=begin
Here is a patch to fix the problem at line 78 of ext/dl/test/test_dl2.rb.
```

```
--- test_dl2.rb (revision 21104)
+++ test_dl2.rb (working copy)
@@ -75,7 +75,7 @@
buff = "foobarbaz"
cb = set_callback(TYPE_INT,2){|x,y| CPtr.new(x)[0] <=> CPtr.new(y)[0]}
cfunc = CFunc.new(@libc['qsort'], TYPE_VOID, 'qsort')
```

- cfunc.call([buff, buff.size, 1, cb].pack("pL!!L!").unpack("!I**"))
- cfunc.call([buff, buff.size, 1, cb].pack("pL!L!L!").unpack("!I**"))
 assert_equal('aabbfoorz', buff)
 end

The type of qsort's second and third arguments is size_t.

Note that this fixes only one problem. The test fails as before.

=end

#16 - 12/28/2008 12:16 PM - kubo (Takehiro Kubo)

- File dl-test.dif added

=begin

Here is a patch to fix all segv faults.

=end

#17 - 12/28/2008 05:17 PM - takano32 (Mitsuhiro TAKANO)

- Status changed from Open to Closed

- % Done changed from 0 to 100

=begin

Applied in changeset r21110.

=end

#18 - 12/29/2008 03:03 AM - znmeb (Ed Borasky)

=begin

I'm still seeing a segfault in r21112:

```
which ruby
/home/znmeb/test/bin/ruby
ruby --version
ruby 1.9.1 (2008-12-28 patchlevel-5000 trunk 21112) [x86_64-linux]
cd ruby/ext/dl/test/
ruby test_all.rb 2>&1 | tee ~/Packages/ruby-segfault.log
Loaded suite test_all
Started
.....F./home/znmeb/test/lib/ruby/1.9.1/dl/func.rb:31: [BUG] Segmentation fault
ruby 1.9.1 (2008-12-28 patchlevel-5000 trunk 21112) [x86_64-linux]
```

-- control frame -----

```
c:0015 p:---- s:0063 b:0063 l:000062 d:000062 CFUNC :call
c:0014 p:0053 s:0059 b:0059 l:000058 d:000058 METHOD
/home/znmeb/test/lib/ruby/1.9.1/dl/func.rb:31
c:0013 p:0073 s:0052 b:0052 l:000051 d:000051 METHOD
/home/znmeb/Packages/ruby/ext/dl/test/test_func.rb:18
c:0012 p:0041 s:0045 b:0045 l:000044 d:000044 METHOD
/home/znmeb/test/lib/ruby/1.9.1/minitest/unit.rb:436
c:0011 p:0096 s:0039 b:0039 l:000019 d:000038 BLOCK
/home/znmeb/test/lib/ruby/1.9.1/minitest/unit.rb:415
c:0010 p:---- s:0033 b:0033 l:000032 d:000032 FINISH
c:0009 p:---- s:0031 b:0031 l:000030 d:000030 CFUNC :each
c:0008 p:0026 s:0028 b:0028 l:000019 d:000027 BLOCK
/home/znmeb/test/lib/ruby/1.9.1/minitest/unit.rb:409
c:0007 p:---- s:0025 b:0025 l:000024 d:000024 FINISH
c:0006 p:---- s:0023 b:0023 l:000022 d:000022 CFUNC :each
c:0005 p:0080 s:0020 b:0020 l:000019 d:000019 METHOD
/home/znmeb/test/lib/ruby/1.9.1/minitest/unit.rb:408
```

c:0004 p:0153 s:0015 b:0015 l:000014 d:000014 METHOD
/home/znmeb/test/lib/ruby/1.9.1/minitest/unit.rb:388
c:0003 p:0040 s:0007 b:0007 l:000dd8 d:000006 BLOCK
/home/znmeb/test/lib/ruby/1.9.1/minitest/unit.rb:329
c:0002 p:---- s:0004 b:0004 l:000003 d:000003 FINISH
c:0001 p:0000 s:0002 b:0002 l:000bc8 d:000bc8 TOP

-- Ruby level backtrace information-----

/home/znmeb/test/lib/ruby/1.9.1/dl/func.rb:31:in call' /home/znmeb/test/lib/ruby/1.9.1/dl/func.rb:31:in call'
/home/znmeb/Packages/ruby/ext/dl/test/test_func.rb:18:in test_isdigit' /home/znmeb/test/lib/ruby/1.9.1/minitest/unit.rb:436:in run'
/home/znmeb/test/lib/ruby/1.9.1/minitest/unit.rb:415:in block (2 levels) in run_test_suites' /home/znmeb/test/lib/ruby/1.9.1/minitest/unit.rb:409:in each'
/home/znmeb/test/lib/ruby/1.9.1/minitest/unit.rb:409:in block in run_test_suites' /home/znmeb/test/lib/ruby/1.9.1/minitest/unit.rb:408:in each'
/home/znmeb/test/lib/ruby/1.9.1/minitest/unit.rb:408:in run_test_suites' /home/znmeb/test/lib/ruby/1.9.1/minitest/unit.rb:388:in run'
/home/znmeb/test/lib/ruby/1.9.1/minitest/unit.rb:329:in `block in autorun'

-- C level backtrace information -----

0x51ba89 ruby(rb_vm_bugreport+0x179) [0x51ba89]
0x54fb3a ruby [0x54fb3a]
0x54fc47 ruby(rb_bug+0xf1) [0x54fc47]
0x4af46b ruby [0x4af46b]
0x7f9499593a90 /lib64/libpthread.so.0 [0x7f9499593a90]
0x7f94989b75fe /lib64/libc.so.6(isdigit+0x1e) [0x7f94989b75fe]
0x7f94982d0fc3 /home/znmeb/test/lib/ruby/1.9.1/x86_64-linux/dl.so(rb_dlfunc_call+0x3fb8) [0x7f94982d0fc3]
0x5104a5 ruby [0x5104a5]
0x5102cc ruby [0x5102cc]
0x50fa9e ruby [0x50fa9e]
0x50b382 ruby [0x50b382]
0x5186b9 ruby [0x5186b9]
0x5173f7 ruby [0x5173f7]
0x51747e ruby [0x51747e]
0x51452c ruby [0x51452c]
0x5144fd ruby(rb_yield+0x39) [0x5144fd]
0x52c46b ruby(rb_ary_each+0x8a) [0x52c46b]
0x510486 ruby [0x510486]
0x5102cc ruby [0x5102cc]
0x50fa9e ruby [0x50fa9e]
0x50b382 ruby [0x50b382]
0x5186b9 ruby [0x5186b9]
0x5173f7 ruby [0x5173f7]
0x51747e ruby [0x51747e]
0x51452c ruby [0x51452c]
0x5144fd ruby(rb_yield+0x39) [0x5144fd]
0x52c46b ruby(rb_ary_each+0x8a) [0x52c46b]
0x510486 ruby [0x510486]
0x5102cc ruby [0x5102cc]
0x50fa9e ruby [0x50fa9e]
0x50b382 ruby [0x50b382]
0x5186b9 ruby [0x5186b9]
0x5173f7 ruby [0x5173f7]
0x51758c ruby(vm_invoke_proc+0x10c) [0x51758c]
0x41de07 ruby(rb_proc_call+0x9f) [0x41de07]
0x41ac69 ruby(rb_call_end_proc+0x1d) [0x41ac69]
0x41af8c ruby(rb_exec_end_proc+0x1b3) [0x41af8c]
0x41b24f ruby [0x41b24f]
0x41b33a ruby(ruby_cleanup+0xaf) [0x41b33a]
0x41b670 ruby(ruby_run_node+0x73) [0x41b670]
0x419e7b ruby(main+0x4f) [0x419e7b]
0x7f94989aa586 /lib64/libc.so.6(__libc_start_main+0xe6) [0x7f94989aa586]
0x419d69 ruby [0x419d69]

[NOTE]

You may encounter a bug of Ruby interpreter. Bug reports are welcome.

For details: <http://www.ruby-lang.org/bugreport.html>

cd ~/Packages

znmeb@DreamScape:~/Packages>

I'll do a C-level backtrace and see if it's in the same place.

=end

#19 - 12/29/2008 03:14 AM - znmeb (Ed Borasky)

- File isdigit-trace.txt added

```
=begin
Different place ... it's calling "isdigit" now. C-level backtrace is attached
=end
```

#20 - 12/29/2008 02:08 PM - yugui (Yuki Sonoda)

- Status changed from Closed to Open

- Assignee set to takano32 (Mitsuhiro TAKANO)

```
=begin

=end
```

#21 - 12/29/2008 09:47 PM - kubo (Takehiro Kubo)

```
=begin
A patch again which I previously attached excluding changeset r21110
and including a few new issues.
```

Index: ext/dl/test/test_base.rb

```
--- ext/dl/test/test_base.rb (revision 21112)
+++ ext/dl/test/test_base.rb (working copy)
@@ -6,8 +6,17 @@
LIBC_SO = "cygwin1.dll"
LIBM_SO = "cygwin1.dll"
when /linux/
```

- LIBC_SO = "/lib/libc.so.6"
- LIBM_SO = "/lib/libm.so.6"
- libdir = '/lib'
- case [0].pack('L!').size
- when 4

• 32-bit ruby

- libdir = '/lib32' if File.directory? '/lib32'
- when 8

• 64-bit ruby

- libdir = '/lib64' if File.directory? '/lib64'
- end
- LIBC_SO = File.join(libdir, "libc.so.6")

- LIBM_SO = File.join(libdir, "libm.so.6")
when /mingw/, /mswin32/
LIBC_SO = "msvcrt.dll"
LIBM_SO = "msvcrt.dll"

Index: ext/dl/test/test_import.rb

=====

```
--- ext/dl/test/test_import.rb (revision 21112)
+++ ext/dl/test/test_import.rb (working copy)
@@ -11,10 +11,10 @@
```

```
extern "void strcpy(char, char*)"
extern "int isdigit(int)"
```

- extern "float atof(string)"
- extern "double atof(string)"
extern "unsigned long strtoul(char*, char**, int)"

- extern "int qsort(void*, int, int, void*)"
- extern "void fprintf(FILE*, char*)"
- extern "int qsort(void*, unsigned long, unsigned long, void*)"
- extern "int fprintf(FILE*, char*)"
extern "int gettimeofday(timeval*, timezone*)" rescue nil

QsortCallback = bind("void *qsort_callback*(void, void*)", :temp)
Index: ext/dl/test/test_func.rb

```
=====
--- ext/dl/test/test_func.rb (revision 21112)
+++ ext/dl/test/test_func.rb (working copy)
@@ -24,7 +24,7 @@
end

def test_atof()
```

- [REDACTED]

- [REDACTED]

```
[TYPE_VOIDP])
r = f.call("12.34")
assert_match(12.00..13.00, r)
```

Index: ext/dl/dl.h

```
--- ext/dl/dl.h (revision 21112)
+++ ext/dl/dl.h (working copy)
@@ -50,29 +50,65 @@
stack[15],stack[16],stack[17],stack[18],stack[19]
```

```
#define DLSTACK_PROTO0
#define DLSTACK_PROTO1 DLSTACK_TYPE
#define DLSTACK_PROTO2 DLSTACK_PROTO1, DLSTACK_TYPE
#define DLSTACK_PROTO3 DLSTACK_PROTO2, DLSTACK_TYPE
#define DLSTACK_PROTO4 DLSTACK_PROTO3, DLSTACK_TYPE
#define DLSTACK_PROTO4 DLSTACK_PROTO3, DLSTACK_TYPE
#define DLSTACK_PROTO5 DLSTACK_PROTO4, DLSTACK_TYPE
#define DLSTACK_PROTO6 DLSTACK_PROTO5, DLSTACK_TYPE
#define DLSTACK_PROTO7 DLSTACK_PROTO6, DLSTACK_TYPE
#define DLSTACK_PROTO8 DLSTACK_PROTO7, DLSTACK_TYPE
#define DLSTACK_PROTO9 DLSTACK_PROTO8, DLSTACK_TYPE
#define DLSTACK_PROTO10 DLSTACK_PROTO9, DLSTACK_TYPE
#define DLSTACK_PROTO11 DLSTACK_PROTO10, DLSTACK_TYPE
#define DLSTACK_PROTO12 DLSTACK_PROTO11, DLSTACK_TYPE
#define DLSTACK_PROTO13 DLSTACK_PROTO12, DLSTACK_TYPE
#define DLSTACK_PROTO14 DLSTACK_PROTO13, DLSTACK_TYPE
#define DLSTACK_PROTO14 DLSTACK_PROTO13, DLSTACK_TYPE
#define DLSTACK_PROTO15 DLSTACK_PROTO14, DLSTACK_TYPE
#define DLSTACK_PROTO16 DLSTACK_PROTO15, DLSTACK_TYPE
#define DLSTACK_PROTO17 DLSTACK_PROTO16, DLSTACK_TYPE
#define DLSTACK_PROTO18 DLSTACK_PROTO17, DLSTACK_TYPE
#define DLSTACK_PROTO19 DLSTACK_PROTO18, DLSTACK_TYPE
#define DLSTACK_PROTO20 DLSTACK_PROTO19, DLSTACK_TYPE
#define DLSTACK_PROTO1_ DLSTACK_TYPE
#define DLSTACK_PROTO2_ DLSTACK_PROTO1_, DLSTACK_TYPE
#define DLSTACK_PROTO3_ DLSTACK_PROTO2_, DLSTACK_TYPE
#define DLSTACK_PROTO4_ DLSTACK_PROTO3_, DLSTACK_TYPE
#define DLSTACK_PROTO4_ DLSTACK_PROTO3_, DLSTACK_TYPE
#define DLSTACK_PROTO5_ DLSTACK_PROTO4_, DLSTACK_TYPE
#define DLSTACK_PROTO6_ DLSTACK_PROTO5_, DLSTACK_TYPE
#define DLSTACK_PROTO7_ DLSTACK_PROTO6_, DLSTACK_TYPE
#define DLSTACK_PROTO8_ DLSTACK_PROTO7_, DLSTACK_TYPE
#define DLSTACK_PROTO9_ DLSTACK_PROTO8_, DLSTACK_TYPE
#define DLSTACK_PROTO10_ DLSTACK_PROTO9_, DLSTACK_TYPE
#define DLSTACK_PROTO11_ DLSTACK_PROTO10_, DLSTACK_TYPE
#define DLSTACK_PROTO12_ DLSTACK_PROTO11_, DLSTACK_TYPE
#define DLSTACK_PROTO13_ DLSTACK_PROTO12_, DLSTACK_TYPE
#define DLSTACK_PROTO14_ DLSTACK_PROTO13_, DLSTACK_TYPE
#define DLSTACK_PROTO14_ DLSTACK_PROTO13_, DLSTACK_TYPE
```

```

+#define DLSTACK_PROTO15_ DLSTACK_PROTO14_, DLSTACK_TYPE
+#define DLSTACK_PROTO16_ DLSTACK_PROTO15_, DLSTACK_TYPE
+#define DLSTACK_PROTO17_ DLSTACK_PROTO16_, DLSTACK_TYPE
+#define DLSTACK_PROTO18_ DLSTACK_PROTO17_, DLSTACK_TYPE
+#define DLSTACK_PROTO19_ DLSTACK_PROTO18_, DLSTACK_TYPE
+#define DLSTACK_PROTO20_ DLSTACK_PROTO19_, DLSTACK_TYPE

```

```

+/*

```

- Add "...", as the last argument.
- This is required for variable argument functions such
- as fprintf() on x86_64-linux.

◦ http://refspecs.linuxfoundation.org/elf/x86_64-abi-0.95.pdf

◦ page 19:

- For calls that may call functions that use varargs or stdargs
- (prototype-less calls or calls to functions containing ellipsis
- (...) in the declaration) %a is used as hidden argument to
- specify the number of SSE registers used.

```

• */

```

```

+#define DLSTACK_PROTO1 DLSTACK_PROTO1_, ...
+#define DLSTACK_PROTO2 DLSTACK_PROTO2_, ...
+#define DLSTACK_PROTO3 DLSTACK_PROTO3_, ...
+#define DLSTACK_PROTO4 DLSTACK_PROTO4_, ...
+#define DLSTACK_PROTO4 DLSTACK_PROTO4_, ...
+#define DLSTACK_PROTO5 DLSTACK_PROTO5_, ...
+#define DLSTACK_PROTO6 DLSTACK_PROTO6_, ...
+#define DLSTACK_PROTO7 DLSTACK_PROTO7_, ...
+#define DLSTACK_PROTO8 DLSTACK_PROTO8_, ...
+#define DLSTACK_PROTO9 DLSTACK_PROTO9_, ...
+#define DLSTACK_PROTO10 DLSTACK_PROTO10_, ...
+#define DLSTACK_PROTO11 DLSTACK_PROTO11_, ...
+#define DLSTACK_PROTO12 DLSTACK_PROTO12_, ...
+#define DLSTACK_PROTO13 DLSTACK_PROTO13_, ...
+#define DLSTACK_PROTO14 DLSTACK_PROTO14_, ...
+#define DLSTACK_PROTO14 DLSTACK_PROTO14_, ...
+#define DLSTACK_PROTO15 DLSTACK_PROTO15_, ...
+#define DLSTACK_PROTO16 DLSTACK_PROTO16_, ...
+#define DLSTACK_PROTO17 DLSTACK_PROTO17_, ...
+#define DLSTACK_PROTO18 DLSTACK_PROTO18_, ...
+#define DLSTACK_PROTO19 DLSTACK_PROTO19_, ...
+#define DLSTACK_PROTO20 DLSTACK_PROTO20_, ...

```

#define DLSTACK_ARGS0(stack)

#define DLSTACK_ARGS1(stack) stack[0]

#define DLSTACK_ARGS2(stack) DLSTACK_ARGS1(stack), stack[1]

Index: ext/dl/lib/dl/stack.rb

```

--- ext/dl/lib/dl/stack.rb (revision 21112)

```

```

+++ ext/dl/lib/dl/stack.rb (working copy)

```

```

@@ -121,20 +121,26 @@

```

```

@template = ""

```

```

addr = 0

```

```

types.each{|t|

```

- [REDACTED]
- [REDACTED]
- [REDACTED]

- [REDACTED]

- [REDACTED]

- [REDACTED]

- [REDACTED]

```
@template << PACK_MAP[t]
  addr += SIZE_MAP[t]
}
```

- [REDACTED]

```
if( addr % SIZEOF_VOIDP == 0 )
  @size = addr / SIZEOF_VOIDP
else
  @size = (addr / SIZEOF_VOIDP) + 1
end
```

end

- def add_padding(addr, align)

- [REDACTED]

- [REDACTED]

- [REDACTED]

- [REDACTED]

- [REDACTED]

- [REDACTED]

- [REDACTED]

- end
end
end

- ext/dl/test/test_base.rb

/lib/libc.so is i386 binary on x86_64 redhat.

redhat-based x86_64 linux distributions:

/lib - 32-bit libraries

/lib64 - 64-bit libraries

debian-based x86_64 linux distributions:

/lib - 64-bit libraries

/lib32 - 32-bit libraries

/lib64 - symbolic link to /lib

This will work on the following combinations.

- i386 ruby on i386 linux
- i386 ruby on redhat-based x86_64 linux
- i386 ruby on debian-based x86_64 linux
- x86_64 ruby on redhat-based x86_64 linux
- x86_64 ruby on debian-based x86_64 linux

- ext/dl/test/test_import.rb

atof()'s return value is double.

The test at test_import.rb:133 fails on x86_64 linux without this fix.

The types of qsort's second and third argument are size_t. But DL::Importer cannot handle size_t. So I replaced them to unsigned long. It happens to work on 64-bit little-endian binary, but not on 64-bit big-endian binary without this fix.

fprintf()'s return value is int.
I don't know what difference is made by this change, but
it will be safe.

- ext/dl/test/test_func.rb

atof()'s return value is double.
The test at test_func.rb:30 fails on x86_64 linux without this fix.

- ext/dl/dl.h

The process may be dumped by segv at test_import.rb:67 without this
fix. It depends on the value of %al register at cfunc.c:276.
The reason is described in a comment of the patch.

- ext/dl/lib/dl/stack.rb

The process may be dumped by segv at test_func.rb:18 without this
fix. If the last argument's size is less than SIZEOF_VOIDP, the
value is deleted by .unpack('l!') at stack.rb:24.

=end

#22 - 12/29/2008 11:57 PM - ko1 (Koichi Sasada)

- Status changed from Open to Closed

=begin
Applied in changeset r21182.
=end

Files

ruby-configure.log	12.4 KB	12/26/2008	znmeb (Ed Borasky)
R-make.log	274 KB	12/26/2008	znmeb (Ed Borasky)
ruby-install.log	24.3 KB	12/26/2008	znmeb (Ed Borasky)
ruby-test.log	3.14 KB	12/26/2008	znmeb (Ed Borasky)
ruby-make.log	115 KB	12/26/2008	znmeb (Ed Borasky)
ruby-segfault.log	2.11 KB	12/27/2008	znmeb (Ed Borasky)
ruby-c-backtrace.txt	2.65 KB	12/27/2008	znmeb (Ed Borasky)
ruby-c-backtrace-noopt.txt	5.07 KB	12/27/2008	znmeb (Ed Borasky)
ruby-c-backtrace-noopt.txt	5.07 KB	12/27/2008	znmeb (Ed Borasky)
ruby-c-backtrace-noopt.txt	5.07 KB	12/27/2008	znmeb (Ed Borasky)
ruby-c-backtrace-noopt.txt	5.07 KB	12/27/2008	znmeb (Ed Borasky)
dl-test.dif	7.43 KB	12/28/2008	kubo (Takehiro Kubo)
isdigit-trace.txt	4.69 KB	12/29/2008	znmeb (Ed Borasky)