Ruby master - Bug #12711

Darwin doesn't show C backtrace correctly if iSIGSEGV is received when IP is in userland

08/29/2016 06:38 PM - naruse (Yui NARUSE)

Status:	Closed		
Priority:	Normal		
Assignee:			
Target version:			
ruby -v:	ruby 2.4.0dev (2016-08-18 trunk 55955) [x86_64-darwin15]	**Backport:**	2.1: REQUIRED, 2.2: DONE, 2.3: DONE

Description

Current Ruby can show C backtrace on the following case

```
Process.kill :SEGV, $$
```

But can't on the following:

```
require"fiddle"
Fiddle.dlunwrap(100).class
```

Related issues:

Related to Ruby master - Bug #13566: A process freezes at the beginning of C ...	**Closed**

Associated revisions

Revision 1d3665fd - 08/29/2016 06:43 PM - naruse (Yui NARUSE)

- vm_dump.c (backtrace): use rip in the saved context for the case the SIGSEGV is received when the process is in userland. Note that ip in the stack should be used if the signal is received when it is in kernel (when it is calling syscall) [Bug #12711]

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/trunk@56030 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

Revision 56030 - 08/29/2016 06:43 PM - naruse (Yui NARUSE)

- vm_dump.c (backtrace): use rip in the saved context for the case the SIGSEGV is received when the process is in userland. Note that ip in the stack should be used if the signal is received when it is in kernel (when it is calling syscall) [Bug #12711]

Revision 56030 - 08/29/2016 06:43 PM - naruse (Yui NARUSE)

- vm_dump.c (backtrace): use rip in the saved context for the case the SIGSEGV is received when the process is in userland. Note that ip in the stack should be used if the signal is received when it is in kernel (when it is calling syscall) [Bug #12711]

Revision 56030 - 08/29/2016 06:43 PM - naruse (Yui NARUSE)

- vm_dump.c (backtrace): use rip in the saved context for the case the SIGSEGV is received when the process is in userland. Note that ip in the stack should be used if the signal is received when it is in kernel (when it is calling syscall) [Bug #12711]

Revision 56030 - 08/29/2016 06:43 PM - naruse (Yui NARUSE)

- vm_dump.c (backtrace): use rip in the saved context for the case the SIGSEGV is received when the process is in userland. Note that ip in the stack should be used if the signal is received when it is in kernel (when it is calling syscall) [Bug #12711]

Revision 8a1c7bab - 08/30/2016 04:49 AM - naruse (Yui NARUSE)

fix r56030 [Bug #12711]

check whether it was syscall or not by getting previous instruction.
syscall instruction is 0x0f 0x05.

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/trunk@56035 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

Revision 56035 - 08/30/2016 04:49 AM - naruse (Yui NARUSE)

fix r56030 [Bug #12711]

check whether it was syscall or not by getting previous instruction.
syscall instruction is 0x0f 0x05.

Revision 56035 - 08/30/2016 04:49 AM - naruse (Yui NARUSE)

fix r56030 [Bug #12711]

check whether it was syscall or not by getting previous instruction.
syscall instruction is 0x0f 0x05.

Revision 56035 - 08/30/2016 04:49 AM - naruse (Yui NARUSE)

fix r56030 [Bug #12711]

check whether it was syscall or not by getting previous instruction.
syscall instruction is 0x0f 0x05.

Revision 56035 - 08/30/2016 04:49 AM - naruse (Yui NARUSE)

fix r56030 [Bug #12711]

check whether it was syscall or not by getting previous instruction.
syscall instruction is 0x0f 0x05.

Revision 6ccadbaf - 09/26/2016 02:13 PM - nagachika (Tomoyuki Chikanaga)

merge revision(s) 56030,56035: [Backport #12711]

```
    * vm_dump.c (backtrace): use rip in the saved context for the case
      the SIGSEGV is received when the process is in userland.
      Note that ip in the stack should be used if the signal is received
      when it is in kernel (when it is calling syscall) [Bug #12711]
```

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/branches/ruby_2_3@56257 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

Revision 56257 - 09/26/2016 02:13 PM - nagachika (Tomoyuki Chikanaga)

merge revision(s) 56030,56035: [Backport #12711]

```
* vm_dump.c (backtrace): use rip in the saved context for the case
  the SIGSEGV is received when the process is in userland.
  Note that ip in the stack should be used if the signal is received
  when it is in kernel (when it is calling syscall) [Bug #12711]
```

Revision 768cdfb2 - 09/30/2016 03:58 PM - usa (Usaku NAKAMURA)

merge revision(s) 56030,56035: [Backport #12711]

```
    * vm_dump.c (backtrace): use rip in the saved context for the case
      the SIGSEGV is received when the process is in userland.
      Note that ip in the stack should be used if the signal is received
      when it is in kernel (when it is calling syscall) [Bug #12711]
```

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/branches/ruby_2_2@56308 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

Revision 56308 - 09/30/2016 03:58 PM - usa (Usaku NAKAMURA)

merge revision(s) 56030,56035: [Backport #12711]

```
* vm_dump.c (backtrace): use rip in the saved context for the case
  the SIGSEGV is received when the process is in userland.
  Note that ip in the stack should be used if the signal is received
  when it is in kernel (when it is calling syscall) [Bug #12711]
```

History

#1 - 08/29/2016 06:43 PM - naruse (Yui NARUSE)

- Status changed from Open to Closed

Applied in changeset r56030.

- vm_dump.c (backtrace): use rip in the saved context for the case the SIGSEGV is received when the process is in userland. Note that ip in the stack should be used if the signal is received when it is in kernel (when it is calling syscall) [Bug #12711]

#2 - 09/26/2016 02:13 PM - nagachika (Tomoyuki Chikanaga)

- Backport changed from 2.1: REQUIRED, 2.2: REQUIRED, 2.3: REQUIRED to 2.1: REQUIRED, 2.2: REQUIRED, 2.3: DONE

ruby_2_3 r56257 merged revision(s) 56030,56035.

#3 - 10/27/2016 07:20 AM - usa (Usaku NAKAMURA)

- Backport changed from 2.1: REQUIRED, 2.2: REQUIRED, 2.3: DONE to 2.1: REQUIRED, 2.2: DONE, 2.3: DONE

#4 - 05/17/2017 12:28 AM - wanabe (_ wanabe)

- Related to Bug #13566: A process freezes at the beginning of C level backtrace when a certain SEGV is occurred added