CrystaX NDK - Bug #1440

SIGSEGV at libCoreFoundation.so

07/13/2016 07:35 PM - Andrew Druk

Status:	Open	**Start date:**	07/13/2016
Priority:	High	**Due date:**	
Assignee:	Dmitry Moskalchuk	**% Done:**	0%
Category:	libobjc2	**Estimated time:**	0.00 hour
Target version:	11.0.0		
CPU Architecture:	x86, x86_64	**Android version:**	5.0 (android-21), 6.0 (android-23)
Host OS:	OS X	**CrystaX Version:**	10.3.1
Toolchain:	clang-3.7		

Description

I got crash when I'm trying to use blocks in objc:

```
#import <stdio.h>
#import <Foundation/Foundation.h>

int main()
{
    void (^testBlock)(void) = ^{
        NSLog(@"Hello world!");
    };
    testBlock();
    return 0;
}
```

```
*** *** *** *** *** *** *** *** *** *** *** *** *** *** *** ***
Build fingerprint: 'Android/sdk_google_phone_x86_64/generic_x86_64:N/NPD56O/2964822:userdebug/test
-keys'
Revision: '0'
ABI: 'x86_64'
pid: 4109, tid: 4109, name: ystax_bugreport  >>> com.readdle.crystax_bugreport <<<
signal 11 (SIGSEGV), code 1 (SEGV_MAPERR), fault addr 0x7ffeeca00a38
    rax 00007ffeeca00000  rbx 00007ffef6db7d08  rcx 000000000000013a  rdx 00007ffef6db7d20
    rsi 00007ffeecb46c10  rdi 00007ffef3626208
    r8  000000000000100d  r9  00007ffef7ff9b40  r10 0000000000000000  r11 0000000000000000
    r12 7fffffffffffff000  r13 00007ffeecb46c10  r14 00007ffef360c000  r15 00007ffef3626208
    cs  0000000000000033  ss  000000000000002b
    rip 00007ffef6d728cd  rbp 0000000000000000  rsp 00007ffff65e9890  eflags 0000000000000216
backtrace:
    #00 pc 00000000000b78cd  /system/lib64/libc.so (ifree+77)
    #01 pc 00000000000b7de3  /system/lib64/libc.so (je_free+115)
    #02 pc 00000000002926ef  /data/app/com.readdle.crystax_bugreport-2/lib/x86_64/libCoreFoundatio
n.so (NSZoneFree+15)
    #03 pc 0000000000271d2a  /data/app/com.readdle.crystax_bugreport-2/lib/x86_64/libCoreFoundatio
n.so (NSDeallocateObject+58)
    #04 pc 000000000022ce4c  /data/app/com.readdle.crystax_bugreport-2/lib/x86_64/libCoreFoundatio
n.so
    #05 pc 000000000029d183  /data/app/com.readdle.crystax_bugreport-2/lib/x86_64/libCoreFoundatio
n.so (objc_release+83)
    #06 pc 0000000000002789  /data/app/com.readdle.crystax_bugreport-2/lib/x86_64/libnative-lib.so
 (main+41)
    #07 pc 00000000000026a5  /data/app/com.readdle.crystax_bugreport-2/lib/x86_64/libnative-lib.so
 (Java_com_readdle_crystax_1bugreport_MainActivity_stringFromJNI+37)
    #08 pc 00000000003aaf71  /data/app/com.readdle.crystax_bugreport-2/oat/x86_64/base.odex (offse
t 0x36d000)
    #09 pc 00000000007fae3f  <anonymous:00007ffff5def000>
    #10 pc 00000000002e7399  /system/lib64/libart.so (_ZN3art11interpreter30EnterInterpreterFromEn
tryPointEPNS_6ThreadEPKNS_7DexFile8CodeItemEPNS_11ShadowFrameE+105)
```

I assume that it's issue with blocks without capturing because next version of main method works for me

```
int main()
{
    int anInteger = 42;
    void (^testBlock)(void) = ^{
        NSLog(@"Integer is: %i", anInteger);
    };
    testBlock();
    return 0;
}
```

History

#1 - 07/14/2016 06:38 PM - Dmitry Moskalchuk

- Priority changed from Normal to High

#2 - 07/14/2016 06:39 PM - Dmitry Moskalchuk

- Description updated