Mac OS X Core Dump Analysis Accelerated

Version 2.0

Dmitry Vostokov
Software Diagnostics Services

Published by OpenTask, Republic of Ireland

OpenTask books and magazines are available through booksellers and distributors worldwide. For further information or comments send requests to press@opentask.com.

A CIP catalogue record for this book is available from the British Library.

ISBN-l3: 978-1-908043-71-9 (Paperback)

1st printing, 2014

Contents

Exercise A1 (GDB)

Goal: Learn how to list stack traces, disassemble functions, check their correctness, dump data, compare core dumps with diagnostic reports, get environment

Patterns: Manual Dump, Stack Trace, Stack Trace Collection, Annotated Disassembly, Paratext, Not My Version, Environment Hint

1. Load a core dump core.1394 and App1 executable:

```
$ gdb -c ~/Documents/AMCDA-Dumps/core.1394 -e ~/Documents/AMCDA-
Dumps/Apps/App1/Build/Products/Release/App1
GNU gdb 6.3.50-20050815 (Apple version gdb-1820) (Sat Jun 16 02:40:11 UTC 2012)
Copyright 2004 Free Software Foundation, Inc.
GDB is free software, covered by the GNU General Public License, and you are
welcome to change it and/or distribute copies of it under certain conditions.
Type "show copying" to see the conditions.
There is absolutely no warranty for GDB.  Type "show warranty" for details.
This GDB was configured as "x86_64-apple-darwin".
Reading symbols for shared libraries . done
Reading symbols for shared libraries ..... done
#0  0x00007fff8a10ce42 in __semwait_signal ()
```

2. List all threads:

```
(gdb) info threads
  6 0x00007fff8a10ce42 in __semwait_signal ()
  5 0x00007fff8a10ce42 in __semwait_signal ()
  4 0x00007fff8a10ce42 in __semwait_signal ()
  3 0x00007fff8a10ce42 in __semwait_signal ()
  2 0x00007fff8a10ce42 in __semwait_signal ()
* 1 0x00007fff8a10ce42 in __semwait_signal ()
```

3. Get all thread stack traces:

```
(gdb) thread apply all bt

Thread 6 (core thread 5):
#0  0x00007fff8a10ce42 in __semwait_signal ()
#1  0x00007fff84d6edea in nanosleep ()
#2  0x00007fff84d6ec2c in sleep ()
#3  0x00007fff84d6ec08 in sleep ()
#4  0x0000000010390bbb2 in bar_five ()
#5  0x0000000010390bbc9 in foo_five ()
#6  0x0000000010390bbe1 in thread_five ()
#7  0x00007fff84db88bf in _pthread_start ()
#8  0x00007fff84dbbb75 in thread_start ()
```

```
Thread 5 (core thread 4):
#0  0x00007fff8a10ce42 in __semwait_signal ()
#1  0x00007fff84d6edea in nanosleep ()
#2  0x00007fff84d6ec2c in sleep ()
#3  0x00007fff84d6ec08 in sleep ()
#4  0x0000000010390bb52 in bar_four ()
#5  0x0000000010390bb69 in foo_four ()
#6  0x0000000010390bb81 in thread_four ()
#7  0x00007fff84db88bf in _pthread_start ()
#8  0x00007fff84dbbb75 in thread_start ()

Thread 4 (core thread 3):
#0  0x00007fff8a10ce42 in __semwait_signal ()
#1  0x00007fff84d6edea in nanosleep ()
#2  0x00007fff84d6ec2c in sleep ()
#3  0x00007fff84d6ec08 in sleep ()
#4  0x0000000010390baf2 in bar_three ()
#5  0x0000000010390bb09 in foo_three ()
#6  0x0000000010390bb21 in thread_three ()
#7  0x00007fff84db88bf in _pthread_start ()
#8  0x00007fff84dbbb75 in thread_start ()

Thread 3 (core thread 2):
#0  0x00007fff8a10ce42 in __semwait_signal ()
#1  0x00007fff84d6edea in nanosleep ()
#2  0x00007fff84d6ec2c in sleep ()
#3  0x00007fff84d6ec08 in sleep ()
#4  0x0000000010390ba92 in bar_two ()
#5  0x0000000010390baa9 in foo_two ()
#6  0x0000000010390bac1 in thread_two ()
---Type <return> to continue, or q <return> to quit---
#7  0x00007fff84db88bf in _pthread_start ()
#8  0x00007fff84dbbb75 in thread_start ()

Thread 2 (core thread 1):
#0  0x00007fff8a10ce42 in __semwait_signal ()
#1  0x00007fff84d6edea in nanosleep ()
#2  0x00007fff84d6ec2c in sleep ()
#3  0x00007fff84d6ec08 in sleep ()
#4  0x0000000010390ba32 in bar_one ()
#5  0x0000000010390ba49 in foo_one ()
#6  0x0000000010390ba61 in thread_one ()
#7  0x00007fff84db88bf in _pthread_start ()
#8  0x00007fff84dbbb75 in thread_start ()

Thread 1 (core thread 0):
#0  0x00007fff8a10ce42 in __semwait_signal ()
#1  0x00007fff84d6edea in nanosleep ()
#2  0x00007fff84d6ec2c in sleep ()
#3  0x00007fff84d6ec08 in sleep ()
#4  0x0000000010390bcc3 in main ()
```

4. Switch to the thread #3 and get its stack trace:

```
(gdb) thread 3
[Switching to thread 3 (core thread 2)]
0x00007fff8a10ce42 in __semwait_signal ()
```

```
(gdb) bt
#0  0x00007fff8a10ce42 in __semwait_signal ()
#1  0x00007fff84d6edea in nanosleep ()
#2  0x00007fff84d6ec2c in sleep ()
#3  0x00007fff84d6ec08 in sleep ()
#4  0x0000000010390ba92 in bar_two ()
#5  0x0000000010390baa9 in foo_two ()
#6  0x0000000010390bac1 in thread_two ()
#7  0x00007fff84db88bf in _pthread_start ()
#8  0x00007fff84dbbb75 in thread_start ()
```

5. Check that bar_two called sleep function:

```
(gdb) disassemble bar_two
Dump of assembler code for function bar_two:
0x0000000010390ba80 <bar_two+0>:  push   %rbp
0x0000000010390ba81 <bar_two+1>:  mov    %rsp,%rbp
0x0000000010390ba84 <bar_two+4>:  sub    $0x10,%rsp
0x0000000010390ba88 <bar_two+8>:  mov    $0xffffffff,%edi
0x0000000010390ba8d <bar_two+13>: callq  0x10390bce0 <dyld_stub_sleep>
0x0000000010390ba92 <bar_two+18>: mov    %eax,-0x4(%rbp)
0x0000000010390ba95 <bar_two+21>: add    $0x10,%rsp
0x0000000010390ba99 <bar_two+25>: pop    %rbp
0x0000000010390ba9a <bar_two+26>: retq
0x0000000010390ba9b <bar_two+27>: nopl   0x0(%rax,%rax,1)
End of assembler dump.
```

6. Compare with intel disassembly flavor:

```
(gdb) set disassembly-flavor intel

(gdb) disassemble bar_two
Dump of assembler code for function bar_two:
0x0000000010390ba80 <bar_two+0>:  push   rbp
0x0000000010390ba81 <bar_two+1>:  mov    rbp,rsp
0x0000000010390ba84 <bar_two+4>:  sub    rsp,0x10
0x0000000010390ba88 <bar_two+8>:  mov    edi,0xffffffff
0x0000000010390ba8d <bar_two+13>: call   0x10390bce0 <dyld_stub_sleep>
0x0000000010390ba92 <bar_two+18>: mov    DWORD PTR [rbp-0x4],eax
0x0000000010390ba95 <bar_two+21>: add    rsp,0x10
0x0000000010390ba99 <bar_two+25>: pop    rbp
0x0000000010390ba9a <bar_two+26>: ret
0x0000000010390ba9b <bar_two+27>: nop    DWORD PTR [rax+rax+0x0]
End of assembler dump.

(gdb) set disassembly-flavor att
```

7. Follow bar_two to sleep function code:

```
(gdb) disassemble bar_two
Dump of assembler code for function bar_two:
0x000000010390ba80 <bar_two+0>:  push   %rbp
0x000000010390ba81 <bar_two+1>:  mov    %rsp,%rbp
0x000000010390ba84 <bar_two+4>:  sub    $0x10,%rsp
0x000000010390ba88 <bar_two+8>:  mov    $0xffffffff,%edi
0x000000010390ba8d <bar_two+13>: callq  0x10390bce0 <dyld_stub_sleep>
0x000000010390ba92 <bar_two+18>: mov    %eax,-0x4(%rbp)
0x000000010390ba95 <bar_two+21>: add    $0x10,%rsp
0x000000010390ba99 <bar_two+25>: pop    %rbp
0x000000010390ba9a <bar_two+26>: retq
0x000000010390ba9b <bar_two+27>: nopl   0x0(%rax,%rax,1)
End of assembler dump.

(gdb) disassemble dyld_stub_sleep
Dump of assembler code for function dyld_stub_sleep:
0x000000010390bce0 <dyld_stub_sleep+0>: jmpq   *0x362(%rip)        # 0x10390c048
End of assembler dump.
```

8. Dump the annotated value as a memory address interpreting its contents as a symbol and then disassemble it:

```
(gdb) x/a 0x10390c048
0x10390c048: 0x7fff84d6ebef <sleep>


(gdb) disassemble 0x7fff84d6ebef
Dump of assembler code for function sleep:
0x00007fff84d6ebef <sleep+0>:    push   %rbp
0x00007fff84d6ebf0 <sleep+1>:    mov    %rsp,%rbp
0x00007fff84d6ebf3 <sleep+4>:    push   %rbx
0x00007fff84d6ebf4 <sleep+5>:    sub    $0x28,%rsp
0x00007fff84d6ebf8 <sleep+9>:    test   %edi,%edi
0x00007fff84d6ebfa <sleep+11>:   mov    %edi,%ebx
0x00007fff84d6ebfc <sleep+13>:   jns    0x7fff84d6ec11 <sleep+34>
0x00007fff84d6ebfe <sleep+15>:   mov    $0x7fffffff,%edi
0x00007fff84d6ec03 <sleep+20>:   callq  0x7fff84d6ebef <sleep>
0x00007fff84d6ec08 <sleep+25>:   lea    -0x7fffffff(%rbx,%rax,1),%eax
0x00007fff84d6ec0f <sleep+32>:   jmp    0x7fff84d6ec4f <sleep+96>
0x00007fff84d6ec11 <sleep+34>:   mov    %ebx,%eax
0x00007fff84d6ec13 <sleep+36>:   mov    %rax,-0x18(%rbp)
0x00007fff84d6ec17 <sleep+40>:   movq   $0x0,-0x10(%rbp)
0x00007fff84d6ec1f <sleep+48>:   lea    -0x18(%rbp),%rdi
0x00007fff84d6ec23 <sleep+52>:   lea    -0x28(%rbp),%rsi
0x00007fff84d6ec27 <sleep+56>:   callq  0x7fff84d6ed46 <nanosleep>
0x00007fff84d6ec2c <sleep+61>:   cmp    $0xffffffffffffffff,%eax
0x00007fff84d6ec2f <sleep+64>:   je     0x7fff84d6ec37 <sleep+72>
0x00007fff84d6ec31 <sleep+66>:   xor    %ebx,%ebx
0x00007fff84d6ec33 <sleep+68>:   mov    %ebx,%eax
0x00007fff84d6ec35 <sleep+70>:   jmp    0x7fff84d6ec4f <sleep+96>
0x00007fff84d6ec37 <sleep+72>:   callq  0x7fff84e0cc88 <__error>
0x00007fff84d6ec3c <sleep+77>:   cmpl   $0x4,(%rax)
0x00007fff84d6ec3f <sleep+80>:   jne    0x7fff84d6ec33 <sleep+68>
0x00007fff84d6ec41 <sleep+82>:   cmpq   $0x0,-0x20(%rbp)
0x00007fff84d6ec46 <sleep+87>:   setne  %al
0x00007fff84d6ec49 <sleep+90>:   movzbl %al,%eax
0x00007fff84d6ec4c <sleep+93>:   add    -0x28(%rbp),%eax
0x00007fff84d6ec4f <sleep+96>:   add    $0x28,%rsp
```

```
0x00007fff84d6ec53 <sleep+100>:  pop    %rbx
0x00007fff84d6ec54 <sleep+101>:  pop    %rbp
0x00007fff84d6ec55 <sleep+102>:  retq
End of assembler dump.
```

9. Repeat the same with resolving DYLD trampoline stub command:

```
(gdb) disassemble bar_two
Dump of assembler code for function bar_two:
0x0000000010390ba80 <bar_two+0>:  push   %rbp
0x0000000010390ba81 <bar_two+1>:  mov    %rsp,%rbp
0x0000000010390ba84 <bar_two+4>:  sub    $0x10,%rsp
0x0000000010390ba88 <bar_two+8>:  mov    $0xffffffff,%edi
0x0000000010390ba8d <bar_two+13>: callq  0x10390bce0 <dyld_stub_sleep>
0x0000000010390ba92 <bar_two+18>: mov    %eax,-0x4(%rbp)
0x0000000010390ba95 <bar_two+21>: add    $0x10,%rsp
0x0000000010390ba99 <bar_two+25>: pop    %rbp
0x0000000010390ba9a <bar_two+26>: retq
0x0000000010390ba9b <bar_two+27>: nopl   0x0(%rax,%rax,1)
End of assembler dump.

(gdb) info trampoline 0x10390bce0
Function at 0x10390bce0 becomes 0x7fff84d6ebef becomes 0x0
```

10. Compare stack trace for thread #3 (core thread 2) and its module info with the diagnostic report App1_1394.crash:

```
Process:         App1 [1394]
Path:            /Users/USER/Documents/*/App1
Identifier:      App1
Version:         ??? (???)
Code Type:       X86-64 (Native)
Parent Process:  bash [661]

Date/Time:       2012-07-24 00:20:26.078 +0100
OS Version:      Mac OS X 10.7.4 (11E53)
Report Version:  9

Crashed Thread:  0  Dispatch queue: com.apple.main-thread

Exception Type:  EXC_CRASH (SIGABRT)
Exception Codes: 0x0000000000000000, 0x0000000000000000

Thread 0 Crashed:: Dispatch queue: com.apple.main-thread
0   libsystem_kernel.dylib              0x00007fff8a10ce42 __semwait_signal + 10
1   libsystem_c.dylib                   0x00007fff84d6edea nanosleep + 164
2   libsystem_c.dylib                   0x00007fff84d6ec2c sleep + 61
3   libsystem_c.dylib                   0x00007fff84d6ec08 sleep + 25
4   App1                                0x0000000010390bcc3 main + 195
5   App1                                0x0000000010390ba14 start + 52

Thread 1:
0   libsystem_kernel.dylib              0x00007fff8a10ce42 __semwait_signal + 10
1   libsystem_c.dylib                   0x00007fff84d6edea nanosleep + 164
2   libsystem_c.dylib                   0x00007fff84d6ec2c sleep + 61
3   libsystem_c.dylib                   0x00007fff84d6ec08 sleep + 25
4   App1                                0x0000000010390ba32 bar_one + 18
5   App1                                0x0000000010390ba49 foo_one + 9
6   App1                                0x0000000010390ba61 thread_one + 17
7   libsystem_c.dylib                   0x00007fff84db88bf _pthread_start + 335
8   libsystem_c.dylib                   0x00007fff84dbbb75 thread_start + 13
```

```
Thread 2:
0   libsystem_kernel.dylib              0x00007fff8a10ce42 __semwait_signal + 10
1   libsystem_c.dylib                   0x00007fff84d6edea nanosleep + 164
2   libsystem_c.dylib                   0x00007fff84d6ec2c sleep + 61
3   libsystem_c.dylib                   0x00007fff84d6ec08 sleep + 25
4   App1                                0x0000000010390ba92 bar_two + 18
5   App1                                0x0000000010390baa9 foo_two + 9
6   App1                                0x0000000010390bac1 thread_two + 17
7   libsystem_c.dylib                   0x00007fff84db88bf _pthread_start + 335
8   libsystem_c.dylib                   0x00007fff84dbbb75 thread_start + 13

Thread 3:
0   libsystem_kernel.dylib              0x00007fff8a10ce42 __semwait_signal + 10
1   libsystem_c.dylib                   0x00007fff84d6edea nanosleep + 164
2   libsystem_c.dylib                   0x00007fff84d6ec2c sleep + 61
3   libsystem_c.dylib                   0x00007fff84d6ec08 sleep + 25
4   App1                                0x0000000010390baf2 bar_three + 18
5   App1                                0x0000000010390bb09 foo_three + 9
6   App1                                0x0000000010390bb21 thread_three + 17
7   libsystem_c.dylib                   0x00007fff84db88bf _pthread_start + 335
8   libsystem_c.dylib                   0x00007fff84dbbb75 thread_start + 13

Thread 4:
0   libsystem_kernel.dylib              0x00007fff8a10ce42 __semwait_signal + 10
1   libsystem_c.dylib                   0x00007fff84d6edea nanosleep + 164
2   libsystem_c.dylib                   0x00007fff84d6ec2c sleep + 61
3   libsystem_c.dylib                   0x00007fff84d6ec08 sleep + 25
4   App1                                0x0000000010390bb52 bar_four + 18
5   App1                                0x0000000010390bb69 foo_four + 9
6   App1                                0x0000000010390bb81 thread_four + 17
7   libsystem_c.dylib                   0x00007fff84db88bf _pthread_start + 335
8   libsystem_c.dylib                   0x00007fff84dbbb75 thread_start + 13

Thread 5:
0   libsystem_kernel.dylib              0x00007fff8a10ce42 __semwait_signal + 10
1   libsystem_c.dylib                   0x00007fff84d6edea nanosleep + 164
2   libsystem_c.dylib                   0x00007fff84d6ec2c sleep + 61
3   libsystem_c.dylib                   0x00007fff84d6ec08 sleep + 25
4   App1                                0x0000000010390bbb2 bar_five + 18
5   App1                                0x0000000010390bbc9 foo_five + 9
6   App1                                0x0000000010390bbe1 thread_five + 17
7   libsystem_c.dylib                   0x00007fff84db88bf _pthread_start + 335
8   libsystem_c.dylib                   0x00007fff84dbbb75 thread_start + 13

Thread 0 crashed with X86 Thread State (64-bit):
  rax: 0x0000000000000004  rbx: 0x00007fff6350aa08  rcx: 0x00007fff6350a9c8  rdx: 0x0000000000000001
  rdi: 0x0000000000000c03  rsi: 0x0000000000000000  rbp: 0x00007fff6350a9f0  rsp: 0x00007fff6350a9c8
   r8: 0x000000007fffffff   r9: 0x0000000000000000  r10: 0x0000000000000001  r11: 0xffffff80002da8d0
  r12: 0x0000000000000000  r13: 0x0000000000000000  r14: 0x00007fff6350aa18  r15: 0x0000000000000000
  rip: 0x00007fff8a10ce42  rfl: 0x0000000000000247  cr2: 0x0000000103d0b880
Logical CPU: 0

Binary Images:
       0x10390b000 -        0x10390bfff +App1 (??? - ???) <5BC0342F-7E97-3A7D-8EA6-75A0468021EA>
/Users/USER/Documents/*/App1
    0x7fff6350b000 -     0x7fff6353fbaf  dyld (195.6 - ???) <0CD1B35B-A28F-32DA-B72E-452EAD609613> /usr/lib/dyld
    0x7fff849f2000 -     0x7fff84a0ffff  libxpc.dylib (77.19.0 - compatibility 1.0.0) <9F57891B-D7EF-3050-BEDD-
21E7C6668248> /usr/lib/system/libxpc.dylib
    0x7fff84d68000 -     0x7fff84d69ff7  libsystem_blocks.dylib (53.0.0 - compatibility 1.0.0) <8BCA214A-8992-34B2-
A8B9-B74DEACA1869> /usr/lib/system/libsystem_blocks.dylib
    0x7fff84d6a000 -     0x7fff84e47fef  libsystem_c.dylib (763.13.0 - compatibility 1.0.0) <41B43515-2806-3FBC-ACF1-
A16F35B7E290> /usr/lib/system/libsystem_c.dylib
    0x7fff85022000 -     0x7fff85030fff  libdispatch.dylib (187.9.0 - compatibility 1.0.0) <1D5BE322-A9B9-3BCE-8FAC-
076FB07CF54A> /usr/lib/system/libdispatch.dylib
    0x7fff855f0000 -     0x7fff855f1fff  libunc.dylib (24.0.0 - compatibility 1.0.0) <337960EE-0A85-3DD0-A760-
7134CF4C0AFF> /usr/lib/system/libunc.dylib
    0x7fff85ae3000 -     0x7fff85ae4ff7  libremovefile.dylib (21.1.0 - compatibility 1.0.0) <739E6C83-AA52-3C6C-A680-
B37FE2888A04> /usr/lib/system/libremovefile.dylib
    0x7fff89114000 -     0x7fff89118fff  libmathCommon.A.dylib (2026.0.0 - compatibility 1.0.0) <FF83AFF7-42B2-306E-
90AF-D539C51A4542> /usr/lib/system/libmathCommon.A.dylib
    0x7fff89119000 -     0x7fff8911dfff  libdyld.dylib (195.5.0 - compatibility 1.0.0) <380C3F44-0CA7-3514-8080-
46D1C9DF4FCD> /usr/lib/system/libdyld.dylib
    0x7fff89740000 -     0x7fff89741ff7  libsystem_sandbox.dylib (??? - ???) <96D38E74-F18F-3CCB-A20B-E8E3ADC4E166>
/usr/lib/system/libsystem_sandbox.dylib
    0x7fff8a0ef000 -     0x7fff8a0f5fff  libmacho.dylib (800.0.0 - compatibility 1.0.0) <165514D7-1BFA-38EF-A151-
676DCD21FB64> /usr/lib/system/libmacho.dylib
```

```
    0x7fff8a0f6000 -     0x7fff8a116fff  libsystem_kernel.dylib (1699.26.8 - compatibility 1.0.0) <1DDC0B0F-DB2A-34D6-
895D-E5B2B5618946> /usr/lib/system/libsystem_kernel.dylib
    0x7fff8a2ac000 -     0x7fff8a2b4fff  libsystem_dnssd.dylib (??? - ???) <D9BB1F87-A42B-3CBC-9DC2-FC07FCEF0016>
/usr/lib/system/libsystem_dnssd.dylib
    0x7fff8ae26000 -     0x7fff8ae61fff  libsystem_info.dylib (??? - ???) <35F90252-2AE1-32C5-8D34-782C614D9639>
/usr/lib/system/libsystem_info.dylib
    0x7fff8b248000 -     0x7fff8b24afff  libquarantine.dylib (36.6.0 - compatibility 1.0.0) <0EBF714B-4B69-3E1F-9A7D-
6BBC2AACB310> /usr/lib/system/libquarantine.dylib
    0x7fff8b3b4000 -     0x7fff8b3b4fff  libkeymgr.dylib (23.0.0 - compatibility 1.0.0) <61EFED6A-A407-301E-B454-
CD18314F0075> /usr/lib/system/libkeymgr.dylib
    0x7fff8b3dd000 -     0x7fff8b3e2fff  libcompiler_rt.dylib (6.0.0 - compatibility 1.0.0) <98ECD5F6-E85C-32A5-98CD-
8911230CB66A> /usr/lib/system/libcompiler_rt.dylib
    0x7fff8bd1a000 -     0x7fff8bd1bfff  libdnsinfo.dylib (395.11.0 - compatibility 1.0.0) <853BAAA5-270F-3FDC-B025-
D448DB72E1C3> /usr/lib/system/libdnsinfo.dylib
    0x7fff8c528000 -     0x7fff8c52dff7  libsystem_network.dylib (??? - ???) <5DE7024E-1D2D-34A2-80F4-08326331A75B>
/usr/lib/system/libsystem_network.dylib
    0x7fff8cfa3000 -     0x7fff8cfadff7  liblaunch.dylib (392.38.0 - compatibility 1.0.0) <6ECB7F19-B384-32C1-8652-
2463C1CF4815> /usr/lib/system/liblaunch.dylib
    0x7fff8fe02000 -     0x7fff8fe09fff  libcopyfile.dylib (85.1.0 - compatibility 1.0.0) <0AB51EE2-E914-358C-AC19-
47BC024BDAE7> /usr/lib/system/libcopyfile.dylib
    0x7fff8fe4b000 -     0x7fff8fe8dff7  libcommonCrypto.dylib (55010.0.0 - compatibility 1.0.0) <BB770C22-8C57-365A-
8716-4A3C36AE7BFB> /usr/lib/system/libcommonCrypto.dylib
    0x7fff90c0f000 -     0x7fff90c18ff7  libsystem_notify.dylib (80.1.0 - compatibility 1.0.0) <A4D651E3-D1C6-3934-
AD49-7A104FD14596> /usr/lib/system/libsystem_notify.dylib
    0x7fff91376000 -     0x7fff913a3fe7  libSystem.B.dylib (159.1.0 - compatibility 1.0.0) <7BEBB139-50BB-3112-947A-
F4AA168F991C> /usr/lib/libSystem.B.dylib
    0x7fff91489000 -     0x7fff9148fff7  libunwind.dylib (30.0.0 - compatibility 1.0.0) <1E9C6C8C-CBE8-3F4B-A5B5-
E03E3AB53231> /usr/lib/system/libunwind.dylib
    0x7fff91a22000 -     0x7fff91a27fff  libcache.dylib (47.0.0 - compatibility 1.0.0) <1571C3AB-BCB2-38CD-B3B2-
C5FC3F927C6A> /usr/lib/system/libcache.dylib

External Modification Summary:
  Calls made by other processes targeting this process:
    task_for_pid: 2
    thread_create: 0
    thread_set_state: 0
  Calls made by this process:
    task_for_pid: 0
    thread_create: 0
    thread_set_state: 0
  Calls made by all processes on this machine:
    task_for_pid: 2696
    thread_create: 0
    thread_set_state: 0

VM Region Summary:
ReadOnly portion of Libraries: Total=50.2M resident=50.2M(100%) swapped_out_or_unallocated=0K(0%)
Writable regions: Total=38.9M written=10.8M(28%) resident=42.6M(110%) swapped_out=0K(0%)
unallocated=16777216.0T(45221404475392%)

REGION TYPE                      VIRTUAL
===========                      =======
MALLOC                             1220K
Stack                              66.6M
__DATA                              464K
__LINKEDIT                         47.7M
__TEXT                             2484K
shared memory                        12K
===========                      =======
TOTAL                             118.4M
```

11. Get App1 data section from the output of vmmap_1394.log:

```
Virtual Memory Map of process 1394 (App1)
Output report format:  2.2  -- 64-bit process

==== Non-writable regions for process 1394
__TEXT                 000000010390b000-000000010390c000 [    4K] r-x/rwx SM=COW  /Users/DumpAnalysis/Documents/AMCDA-
Dumps/Apps/App1/Build/Products/Release/App1

[...]

==== Writable regions for process 1394
__DATA                 000000010390c000-000000010390d000 [    4K] rw-/rwx SM=PRV  /Users/DumpAnalysis/Documents/AMCDA-
Dumps/Apps/App1/Build/Products/Release/App1

[...]
```

12. Compare with the section information in the core dump:

```
(gdb) maintenance info sections
Exec file:
    `/Users/DumpAnalysis/Documents/AMCDA-Dumps/Apps/App1/Build/Products/Release/App1', file type mach-o-le.
    0x0000000000000000->0x0000000000000000 at 0x00000000: LC_SEGMENT.__PAGEZERO ALLOC LOAD CODE HAS_CONTENTS
    0x0000000100000000->0x0000000100001000 at 0x00000000: LC_SEGMENT.__TEXT ALLOC LOAD CODE HAS_CONTENTS
    0x00000001000009e0->0x0000000100000cd3 at 0x000009e0: LC_SEGMENT.__TEXT.__text ALLOC LOAD READONLY CODE
HAS_CONTENTS
    0x0000000100000cd4->0x0000000100000ce6 at 0x00000cd4: LC_SEGMENT.__TEXT.__stubs ALLOC LOAD CODE HAS_CONTENTS
    0x0000000100000ce8->0x0000000100000d16 at 0x00000ce8: LC_SEGMENT.__TEXT.__stub_helper ALLOC LOAD CODE HAS_CONTENTS
    0x0000000100000d16->0x0000000100000d66 at 0x00000d16: LC_SEGMENT.__TEXT.__unwind_info ALLOC LOAD CODE HAS_CONTENTS
    0x0000000100000d68->0x0000000100001000 at 0x00000d68: LC_SEGMENT.__TEXT.__eh_frame ALLOC LOAD CODE HAS_CONTENTS
    0x0000000100001000->0x0000000100002000 at 0x00001000: LC_SEGMENT.__DATA ALLOC LOAD CODE HAS_CONTENTS
    0x0000000100001000->0x0000000100001028 at 0x00001000: LC_SEGMENT.__DATA.__program_vars ALLOC LOAD CODE
HAS_CONTENTS
    0x0000000100001028->0x0000000100001038 at 0x00001028: LC_SEGMENT.__DATA.__nl_symbol_ptr ALLOC LOAD CODE
HAS_CONTENTS
    0x0000000100001038->0x0000000100001050 at 0x00001038: LC_SEGMENT.__DATA.__la_symbol_ptr ALLOC LOAD CODE
HAS_CONTENTS
    0x0000000100001050->0x0000000100001070 at 0x00000000: LC_SEGMENT.__DATA.__common ALLOC
    0x0000000100002000->0x00000001000023b0 at 0x00002000: LC_SEGMENT.__LINKEDIT ALLOC LOAD CODE HAS_CONTENTS
    0x0000000000000000->0x00000000000001a0 at 0x000020d0: LC_SYMTAB.stabs HAS_CONTENTS
    0x0000000000000000->0x0000000000000120 at 0x00002290: LC_SYMTAB.stabstr HAS_CONTENTS
    0x0000000000000000->0x0000000000000100 at 0x000020d0: LC_DYSYMTAB.localstabs HAS_CONTENTS
    0x0000000000000000->0x00000000000000a0 at 0x000021d0: LC_DYSYMTAB.nonlocalstabs HAS_CONTENTS
    0x0000000000000000->0x0000000000000018 at 0x000004b0: LC_LOAD_DYLINKER HAS_CONTENTS
    0x0000000000000000->0x00000000000000a8 at 0x00000500: LC_THREAD.x86_THREAD_STATE64.0 HAS_CONTENTS
    0x0000000000000000->0x0000000000000030 at 0x000005b0: LC_LOAD_DYLIB HAS_CONTENTS
Core file:
    `/Users/DumpAnalysis/Documents/AMCDA-Dumps/core.1394', file type mach-o-le.
    0x000000010390b000->0x000000010390c000 at 0x00002000: LC_SEGMENT. ALLOC LOAD CODE HAS_CONTENTS
    0x000000010390c000->0x000000010390d000 at 0x00003000: LC_SEGMENT. ALLOC LOAD CODE HAS_CONTENTS
    0x000000010390d000->0x000000010390e000 at 0x00004000: LC_SEGMENT. ALLOC LOAD CODE HAS_CONTENTS
    0x000000010390e000->0x000000010390f000 at 0x00005000: LC_SEGMENT. ALLOC LOAD CODE HAS_CONTENTS
    0x000000010390f000->0x0000000103910000 at 0x00006000: LC_SEGMENT. ALLOC LOAD CODE HAS_CONTENTS
    0x0000000103910000->0x0000000103911000 at 0x00007000: LC_SEGMENT. ALLOC LOAD CODE HAS_CONTENTS
    0x0000000103911000->0x0000000103926000 at 0x00008000: LC_SEGMENT. ALLOC LOAD CODE HAS_CONTENTS
    0x0000000103926000->0x0000000103927000 at 0x0001d000: LC_SEGMENT. ALLOC LOAD CODE HAS_CONTENTS
    0x0000000103927000->0x0000000103928000 at 0x0001e000: LC_SEGMENT. ALLOC LOAD CODE HAS_CONTENTS
    0x0000000103928000->0x000000010393d000 at 0x0001f000: LC_SEGMENT. ALLOC LOAD CODE HAS_CONTENTS
    0x000000010393d000->0x000000010393e000 at 0x00034000: LC_SEGMENT. ALLOC LOAD CODE HAS_CONTENTS
    0x000000010393e000->0x000000010393f000 at 0x00035000: LC_SEGMENT. ALLOC LOAD CODE HAS_CONTENTS
    0x000000010393f000->0x0000000103940000 at 0x00036000: LC_SEGMENT. ALLOC LOAD CODE HAS_CONTENTS
    0x0000000103940000->0x00000001039c2000 at 0x00037000: LC_SEGMENT. ALLOC LOAD CODE HAS_CONTENTS
    0x0000000103a00000->0x0000000103b00000 at 0x000b9000: LC_SEGMENT. ALLOC LOAD CODE HAS_CONTENTS
    0x0000000103b00000->0x0000000103b01000 at 0x001b9000: LC_SEGMENT. ALLOC LOAD CODE HAS_CONTENTS
    0x0000000103b01000->0x0000000103b83000 at 0x001ba000: LC_SEGMENT. ALLOC LOAD CODE HAS_CONTENTS
    0x0000000103b83000->0x0000000103b84000 at 0x0023c000: LC_SEGMENT. ALLOC LOAD CODE HAS_CONTENTS
    0x0000000103b84000->0x0000000103c06000 at 0x0023d000: LC_SEGMENT. ALLOC LOAD CODE HAS_CONTENTS
    0x0000000103c06000->0x0000000103c07000 at 0x002bf000: LC_SEGMENT. ALLOC LOAD CODE HAS_CONTENTS
    0x0000000103c07000->0x0000000103c89000 at 0x002c0000: LC_SEGMENT. ALLOC LOAD CODE HAS_CONTENTS
    0x0000000103c89000->0x0000000103c8a000 at 0x00342000: LC_SEGMENT. ALLOC LOAD CODE HAS_CONTENTS
    0x0000000103c8a000->0x0000000103d0c000 at 0x00343000: LC_SEGMENT. ALLOC LOAD CODE HAS_CONTENTS
```

```
0x00007fff5f50b000->0x00007fff62d0b000 at 0x003c5000: LC_SEGMENT. ALLOC LOAD CODE HAS_CONTENTS
0x00007fff62d0b000->0x00007fff6350a000 at 0x03bc5000: LC_SEGMENT. ALLOC LOAD CODE HAS_CONTENTS
0x00007fff6350a000->0x00007fff6350b000 at 0x043c4000: LC_SEGMENT. ALLOC LOAD CODE HAS_CONTENTS
0x00007fff6350b000->0x00007fff63540000 at 0x043c5000: LC_SEGMENT. ALLOC LOAD CODE HAS_CONTENTS
0x00007fff63540000->0x00007fff63542000 at 0x043fa000: LC_SEGMENT. ALLOC LOAD CODE HAS_CONTENTS
0x00007fff63542000->0x00007fff6357c000 at 0x043fc000: LC_SEGMENT. ALLOC LOAD CODE HAS_CONTENTS
0x00007fff6357c000->0x00007fff6358f000 at 0x04436000: LC_SEGMENT. ALLOC LOAD CODE HAS_CONTENTS
0x00007fff749b8000->0x00007fff74a00000 at 0x04449000: LC_SEGMENT. ALLOC LOAD CODE HAS_CONTENTS
0x00007fff74a00000->0x00007fff74c00000 at 0x04491000: LC_SEGMENT. ALLOC LOAD CODE HAS_CONTENTS
0x00007fff74c00000->0x00007fff74e00000 at 0x04691000: LC_SEGMENT. ALLOC LOAD CODE HAS_CONTENTS
0x00007fff74e00000->0x00007fff75000000 at 0x04891000: LC_SEGMENT. ALLOC LOAD CODE HAS_CONTENTS
0x00007fff75000000->0x00007fff75200000 at 0x04a91000: LC_SEGMENT. ALLOC LOAD CODE HAS_CONTENTS
0x00007fff75200000->0x00007fff75400000 at 0x04c91000: LC_SEGMENT. ALLOC LOAD CODE HAS_CONTENTS
0x00007fff75400000->0x00007fff75600000 at 0x04e91000: LC_SEGMENT. ALLOC LOAD CODE HAS_CONTENTS
0x00007fff75600000->0x00007fff75800000 at 0x05091000: LC_SEGMENT. ALLOC LOAD CODE HAS_CONTENTS
0x00007fff75800000->0x00007fff75a00000 at 0x05291000: LC_SEGMENT. ALLOC LOAD CODE HAS_CONTENTS
0x00007fff75a00000->0x00007fff75c00000 at 0x05491000: LC_SEGMENT. ALLOC LOAD CODE HAS_CONTENTS
0x00007fff75c00000->0x00007fff75e00000 at 0x05691000: LC_SEGMENT. ALLOC LOAD CODE HAS_CONTENTS
0x00007fff75e00000->0x00007fff76200000 at 0x05891000: LC_SEGMENT. ALLOC LOAD CODE HAS_CONTENTS
0x00007fff76200000->0x00007fff76400000 at 0x05c91000: LC_SEGMENT. ALLOC LOAD CODE HAS_CONTENTS
0x00007fff76400000->0x00007fff764ac000 at 0x05e91000: LC_SEGMENT. ALLOC LOAD CODE HAS_CONTENTS
0x00007fff849b8000->0x00007fff91a28000 at 0x05f3d000: LC_SEGMENT. ALLOC LOAD CODE HAS_CONTENTS
0x00007fff91a28000->0x00007fff94b30000 at 0x12fad000: LC_SEGMENT. ALLOC LOAD CODE HAS_CONTENTS
0x00007fffffe00000->0x00007fffffe02000 at 0x160b5000: LC_SEGMENT. ALLOC LOAD CODE HAS_CONTENTS
0x0000000000000000->0x00000000000000b0 at 0x00000d68: LC_THREAD.x86_THREAD_STATE.0 HAS_CONTENTS
0x0000000000000000->0x0000000000000214 at 0x00000e20: LC_THREAD.x86_FLOAT_STATE.0 HAS_CONTENTS
0x0000000000000000->0x0000000000000018 at 0x0000103c: LC_THREAD.x86_EXCEPTION_STATE.0 HAS_CONTENTS
0x0000000000000000->0x00000000000000b0 at 0x00001064: LC_THREAD.x86_THREAD_STATE.1 HAS_CONTENTS
0x0000000000000000->0x0000000000000214 at 0x0000111c: LC_THREAD.x86_FLOAT_STATE.1 HAS_CONTENTS
0x0000000000000000->0x0000000000000018 at 0x00001338: LC_THREAD.x86_EXCEPTION_STATE.1 HAS_CONTENTS
0x0000000000000000->0x00000000000000b0 at 0x00001360: LC_THREAD.x86_THREAD_STATE.2 HAS_CONTENTS
0x0000000000000000->0x0000000000000214 at 0x00001418: LC_THREAD.x86_FLOAT_STATE.2 HAS_CONTENTS
0x0000000000000000->0x0000000000000018 at 0x00001634: LC_THREAD.x86_EXCEPTION_STATE.2 HAS_CONTENTS
0x0000000000000000->0x00000000000000b0 at 0x0000165c: LC_THREAD.x86_THREAD_STATE.3 HAS_CONTENTS
0x0000000000000000->0x0000000000000214 at 0x00001714: LC_THREAD.x86_FLOAT_STATE.3 HAS_CONTENTS
0x0000000000000000->0x0000000000000018 at 0x00001930: LC_THREAD.x86_EXCEPTION_STATE.3 HAS_CONTENTS
0x0000000000000000->0x00000000000000b0 at 0x00001958: LC_THREAD.x86_THREAD_STATE.4 HAS_CONTENTS
0x0000000000000000->0x0000000000000214 at 0x00001a10: LC_THREAD.x86_FLOAT_STATE.4 HAS_CONTENTS
0x0000000000000000->0x0000000000000018 at 0x00001c2c: LC_THREAD.x86_EXCEPTION_STATE.4 HAS_CONTENTS
0x0000000000000000->0x00000000000000b0 at 0x00001c54: LC_THREAD.x86_THREAD_STATE.5 HAS_CONTENTS
0x0000000000000000->0x0000000000000214 at 0x00001d0c: LC_THREAD.x86_FLOAT_STATE.5 HAS_CONTENTS
0x0000000000000000->0x0000000000000018 at 0x00001f28: LC_THREAD.x86_EXCEPTION_STATE.5 HAS_CONTENTS
```

13. Dump data with possible symbolic information:

```
 (gdb) x/512a 0x000000010390c000
0x10390c000: 0x10390b000  0x10390c050 <NXArgc>
0x10390c010: 0x10390c058 <NXArgv>      0x10390c060 <environ>
0x10390c020: 0x10390c068 <__progname>  0x7fff8911a6a0 <dyld_stub_binder>
0x10390c030: 0x7fff63546d80      0x10390bcf8
0x10390c040: 0x7fff84dbab01 <pthread_create>  0x7fff84d6ebef <sleep>
0x10390c050 <NXArgc>:     0x1    0x7fff6350aaf0
0x10390c060 <environ>:    0x7fff6350ab00      0x7fff6350ac73
0x10390c070: 0x0    0x0
0x10390c080: 0x0    0x0
0x10390c090: 0x0    0x0
0x10390c0a0: 0x0    0x0
0x10390c0b0: 0x0    0x0
0x10390c0c0: 0x0    0x0
0x10390c0d0: 0x0    0x0
0x10390c0e0: 0x0    0x0
0x10390c0f0: 0x0    0x0
0x10390c100: 0x0    0x0
0x10390c110: 0x0    0x0
0x10390c120: 0x0    0x0
0x10390c130: 0x0    0x0
0x10390c140: 0x0    0x0
```

```
0x10390c150: 0x0    0x0
0x10390c160: 0x0    0x0
0x10390c170: 0x0    0x0
0x10390c180: 0x0    0x0
0x10390c190: 0x0    0x0
0x10390c1a0: 0x0    0x0
0x10390c1b0: 0x0    0x0
0x10390c1c0: 0x0    0x0
0x10390c1d0: 0x0    0x0
0x10390c1e0: 0x0    0x0
0x10390c1f0: 0x0    0x0
0x10390c200: 0x0    0x0
0x10390c210: 0x0    0x0
0x10390c220: 0x0    0x0
0x10390c230: 0x0    0x0
0x10390c240: 0x0    0x0
0x10390c250: 0x0    0x0
0x10390c260: 0x0    0x0
0x10390c270: 0x0    0x0
0x10390c280: 0x0    0x0
0x10390c290: 0x0    0x0
---Type <return> to continue, or q <return> to quit---q
Quit
```

14. Dump the contents of memory pointed to by environ variable in null-terminated string format:

```
(gdb) x/100s 0x7fff6350ab00
[...]
0x7fff6350abd5:      ""
0x7fff6350abd6:      ""
0x7fff6350abd7:      ""
0x7fff6350abd8:      "/Users/DumpAnalysis/Documents/AMCDA-
Dumps/Apps/App1/Build/Products/Release/App1"
0x7fff6350ac28:      "/Users/DumpAnalysis/Documents/AMCDA-
Dumps/Apps/App1/Build/Products/Release/App1"
0x7fff6350ac78:      "TERM_PROGRAM=Apple_Terminal"
0x7fff6350ac94:      "TERM=xterm-256color"
0x7fff6350aca8:      "SHELL=/bin/bash"
0x7fff6350acb8:      "TMPDIR=/var/folders/ww/rmtqfhl93yj4213dnl2rqy6w0000gn/T/"
0x7fff6350acf1:      "Apple_PubSub_Socket_Render=/tmp/launch-mYEvtN/Render"
0x7fff6350ad26:      "TERM_PROGRAM_VERSION=303.2"
0x7fff6350ad41:      "TERM_SESSION_ID=2B039506-8384-4620-B354-120BE31AEA84"
0x7fff6350ad76:      "USER=DumpAnalysis"
0x7fff6350ad88:      "COMMAND_MODE=unix2003"
0x7fff6350ad9e:      "SSH_AUTH_SOCK=/tmp/launch-9sm7dH/Listeners"
0x7fff6350adc9:      "__CF_USER_TEXT_ENCODING=0x1F5:0:0"
0x7fff6350adeb:      "Apple_Ubiquity_Message=/tmp/launch-tWsFs8/Apple_Ubiquity_Message"
0x7fff6350ae2c:
"PATH=/Applications/Xcode.app/Contents/Developer/usr/bin/:/usr/bin:/bin:/usr/sbin:/sbin:/usr/lo
cal/bin:/usr/X11/bin"
0x7fff6350ae9f:      "PWD=/Users/DumpAnalysis"
0x7fff6350aeb7:      "LANG=en_IE.UTF-8"
---Type <return> to continue, or q <return> to quit---
0x7fff6350aec8:      "SHLVL=1"
0x7fff6350aed0:      "HOME=/Users/DumpAnalysis"
0x7fff6350aee9:      "LOGNAME=DumpAnalysis"
0x7fff6350aefe:      "DISPLAY=/tmp/launch-M8cgb1/org.x:0"
0x7fff6350af21:      "SECURITYSESSIONID=186af"
```

```
0x7fff6350af39:      "_=/Users/DumpAnalysis/Documents/AMCDA-
Dumps/Apps/App1/Build/Products/Release/App1"
0x7fff6350af8b:      "OLDPWD=/usr/share/man/man1"
0x7fff6350afa6:      ""
0x7fff6350afa7:      ""
0x7fff6350afa8:      "stack_guard=0x74843dc6068699c3"
0x7fff6350afc7:      "malloc_entropy=0x7406669509034332,0x71e4e2253a6d22b0"
0x7fff6350affc:      ""
0x7fff6350affd:      ""
```

15. Get the list of loaded modules:

```
(gdb) info sharedlibrary
The DYLD shared library state has been initialized from the executable's shared library information.  All symbols should be present, but the addresses of some
symbols may move when the program is executed, as DYLD may relocate library load addresses if necessary.
                                  Requested State Current State
Num Basename             Type Address         Reason | | Source
  | |                       | |                   | | | |
  1 App1                   - 0x10390b000        exec Y Y /Users/DumpAnalysis/Documents/AMCDA-Dumps/Apps/App1/Build/Products/Release/App1 at 0x10390b000
(offset 0x390b000)
                                              (objfile is) [memory object "/Users/DumpAnalysis/Documents/AMCDA-Dumps/Apps/App1/Build/Products/Release/App1" at
0x10390b000]
  2 dyld                   - 0x7fff6350b000        dyld Y Y /usr/lib/dyld at 0x7fff6350b000 (offset 0x7fff6350b001) with prefix "__dyld_"
                                              (objfile is) [memory object "/usr/lib/dyld" at 0x7fff6350b000]
  3 libSystem.B.dylib      - 0x7fff91376000        dyld Y Y /usr/lib/libSystem.B.dylib at 0x7fff91376000 (offset 0x49b8000)
                                              (objfile is) [memory object "/usr/lib/libSystem.B.dylib" at 0x7fff91376000]
  4 libcache.dylib         - 0x7fff91a22000        dyld Y Y /usr/lib/system/libcache.dylib at 0x7fff91a22000 (offset 0x49b8000)
                                              (objfile is) [memory object "/usr/lib/system/libcache.dylib" at 0x7fff91a22000]
  5 libcommonCrypto.dylib  - 0x7fff8fe4b000        dyld Y Y /usr/lib/system/libcommonCrypto.dylib at 0x7fff8fe4b000 (offset 0x49b8000)
                                              (objfile is) [memory object "/usr/lib/system/libcommonCrypto.dylib" at 0x7fff8fe4b000]
  6 libcompiler_rt.dylib   - 0x7fff8b3dd000        dyld Y Y /usr/lib/system/libcompiler_rt.dylib at 0x7fff8b3dd000 (offset 0x49b8000)
                                              (objfile is) [memory object "/usr/lib/system/libcompiler_rt.dylib" at 0x7fff8b3dd000]
  7 libcopyfile.dylib      - 0x7fff8fe02000        dyld Y Y /usr/lib/system/libcopyfile.dylib at 0x7fff8fe02000 (offset 0x49b8000)
                                              (objfile is) [memory object "/usr/lib/system/libcopyfile.dylib" at 0x7fff8fe02000]
  8 libdispatch.dylib      - 0x7fff85022000        dyld Y Y /usr/lib/system/libdispatch.dylib at 0x7fff85022000 (offset 0x49b8000)
                                              (objfile is) [memory object "/usr/lib/system/libdispatch.dylib" at 0x7fff85022000]
  9 libdnsinfo.dylib       - 0x7fff8bd1a000        dyld Y Y /usr/lib/system/libdnsinfo.dylib at 0x7fff8bd1a000 (offset 0x49b8000)
                                              (objfile is) [memory object "/usr/lib/system/libdnsinfo.dylib" at 0x7fff8bd1a000]
 10 libdyld.dylib          - 0x7fff89119000        dyld Y Y /usr/lib/system/libdyld.dylib at 0x7fff89119000 (offset 0x49b8000)
                                              (objfile is) [memory object "/usr/lib/system/libdyld.dylib" at 0x7fff89119000]
 11 libkeymgr.dylib        - 0x7fff8b3b4000        dyld Y Y /usr/lib/system/libkeymgr.dylib at 0x7fff8b3b4000 (offset 0x49b8000)
                                              (objfile is) [memory object "/usr/lib/system/libkeymgr.dylib" at 0x7fff8b3b4000]
 12 liblaunch.dylib        - 0x7fff8cfa3000        dyld Y Y /usr/lib/system/liblaunch.dylib at 0x7fff8cfa3000 (offset 0x49b800---Type <return> to continue,
or q <return> to quit---
0)
                                              (objfile is) [memory object "/usr/lib/system/liblaunch.dylib" at 0x7fff8cfa3000]
 13 libmacho.dylib         - 0x7fff8a0ef000        dyld Y Y /usr/lib/system/libmacho.dylib at 0x7fff8a0ef000 (offset 0x49b8000)
                                              (objfile is) [memory object "/usr/lib/system/libmacho.dylib" at 0x7fff8a0ef000]
 14 libmathCommon.A.dylib  - 0x7fff89114000        dyld Y Y /usr/lib/system/libmathCommon.A.dylib at 0x7fff89114000 (offset 0x49b8000)
                                              (objfile is) [memory object "/usr/lib/system/libmathCommon.A.dylib" at 0x7fff89114000]
 15 libquarantine.dylib    - 0x7fff8b248000        dyld Y Y /usr/lib/system/libquarantine.dylib at 0x7fff8b248000 (offset 0x49b8000)
                                              (objfile is) [memory object "/usr/lib/system/libquarantine.dylib" at 0x7fff8b248000]
 16 libremovefile.dylib    - 0x7fff85ae3000        dyld Y Y /usr/lib/system/libremovefile.dylib at 0x7fff85ae3000 (offset 0x49b8000)
                                              (objfile is) [memory object "/usr/lib/system/libremovefile.dylib" at 0x7fff85ae3000]
 17 libsystem_blocks.dylib - 0x7fff84d68000        dyld Y Y /usr/lib/system/libsystem_blocks.dylib at 0x7fff84d68000 (offset 0x49b8000)
                                              (objfile is) [memory object "/usr/lib/system/libsystem_blocks.dylib" at 0x7fff84d68000]
 18 libsystem_c.dylib      - 0x7fff84d6a000        dyld Y Y /usr/lib/system/libsystem_c.dylib at 0x7fff84d6a000 (offset 0x49b8000)
                                              (objfile is) [memory object "/usr/lib/system/libsystem_c.dylib" at 0x7fff84d6a000]
 19 libsystem_dnssd.dylib  - 0x7fff8a2ac000        dyld Y Y /usr/lib/system/libsystem_dnssd.dylib at 0x7fff8a2ac000 (offset 0x49b8000)
                                              (objfile is) [memory object "/usr/lib/system/libsystem_dnssd.dylib" at 0x7fff8a2ac000]
 20 libsystem_info.dylib   - 0x7fff8ae26000        dyld Y Y /usr/lib/system/libsystem_info.dylib at 0x7fff8ae26000 (offset 0x49b8000)
                                              (objfile is) [memory object "/usr/lib/system/libsystem_info.dylib" at 0x7fff8ae26000]
 21 libsystem_kernel.dylib - 0x7fff8a0f6000        dyld Y Y /usr/lib/system/libsystem_kernel.dylib at 0x7fff8a0f6000 (offset 0x49b8000)
                                              (objfile is) [memory object "/usr/lib/system/libsystem_kernel.dylib" at 0x7fff8a0f6000]
 22 libsystem_network.dylib - 0x7fff8c528000       dyld Y Y /usr/lib/system/libsystem_network.dylib at 0x7fff8c528000 (offset 0x49b8000)
                                              (objfile is) [memory object "/usr/lib/system/libsystem_network.dylib" at 0x7fff8c528000]
 23 libsystem_notify.dylib - 0x7fff90c0f000        dyld Y Y /usr/lib/system/libsystem_notify.dylib at 0x7fff90c0f000 (offset 0x49b8000)
---Type <return> to continue, or q <return> to quit---
                                              (objfile is) [memory object "/usr/lib/system/libsystem_notify.dylib" at 0x7fff90c0f000]
 24 libsystem_sandbox.dylib - 0x7fff89740000       dyld Y Y /usr/lib/system/libsystem_sandbox.dylib at 0x7fff89740000 (offset 0x49b8000)
                                              (objfile is) [memory object "/usr/lib/system/libsystem_sandbox.dylib" at 0x7fff89740000]
 25 libunc.dylib           - 0x7fff855f0000        dyld Y Y /usr/lib/system/libunc.dylib at 0x7fff855f0000 (offset 0x49b8000)
                                              (objfile is) [memory object "/usr/lib/system/libunc.dylib" at 0x7fff855f0000]
 26 libunwind.dylib        - 0x7fff91489000        dyld Y Y /usr/lib/system/libunwind.dylib at 0x7fff91489000 (offset 0x49b8000)
                                              (objfile is) [memory object "/usr/lib/system/libunwind.dylib" at 0x7fff91489000]
 27 libxpc.dylib           - 0x7fff849f2000        dyld Y Y /usr/lib/system/libxpc.dylib at 0x7fff849f2000 (offset 0x49b8000)
                                              (objfile is) [memory object "/usr/lib/system/libxpc.dylib" at 0x7fff849f2000]
```

Exercise A1 (LLDB)

Goal: Learn how to list stack traces, disassemble functions, check their correctness, dump data, compare core dumps with diagnostic reports, get environment

Patterns: Manual Dump, Stack Trace, Stack Trace Collection, Annotated Disassembly, Paratext, Not My Version, Environment Hint

1. Load a core dump core.1394 and App1 executable:

```
$ lldb -c ~/Documents/AMCDA-Dumps/core.1394 -f ~/Documents/AMCDA-
Dumps/Apps/App1/Build/Products/Release/App1
error: core.1394 is a corrupt mach-o file: load command 46 LC_SEGMENT_64 has a fileoff +
filesize (0x160b7000) that extends beyond the end of the file (0x160b5000), the segment will
be truncated
Core file '/Users/DumpAnalysis/Documents/AMCDA-Dumps/core.1394' (x86_64) was loaded.
Process 0 stopped
* thread #1: tid = 0x0000, 0x00007fff8a10ce42 libsystem_kernel.dylib`__semwait_signal + 10,
stop reason = signal SIGSTOP
    frame #0: 0x00007fff8a10ce42 libsystem_kernel.dylib`__semwait_signal + 10
libsystem_kernel.dylib`__semwait_signal + 10:
-> 0x7fff8a10ce42:  jae    0x7fff8a10ce49            ; __semwait_signal + 17
   0x7fff8a10ce44:  jmpq   0x7fff8a10dffc            ; cerror
   0x7fff8a10ce49:  ret
   0x7fff8a10ce4a:  nop
  thread #2: tid = 0x0001, 0x00007fff8a10ce42 libsystem_kernel.dylib`__semwait_signal + 10,
stop reason = signal SIGSTOP
    frame #0: 0x00007fff8a10ce42 libsystem_kernel.dylib`__semwait_signal + 10
libsystem_kernel.dylib`__semwait_signal + 10:
-> 0x7fff8a10ce42:  jae    0x7fff8a10ce49            ; __semwait_signal + 17
   0x7fff8a10ce44:  jmpq   0x7fff8a10dffc            ; cerror
   0x7fff8a10ce49:  ret
   0x7fff8a10ce4a:  nop
  thread #3: tid = 0x0002, 0x00007fff8a10ce42 libsystem_kernel.dylib`__semwait_signal + 10,
stop reason = signal SIGSTOP
    frame #0: 0x00007fff8a10ce42 libsystem_kernel.dylib`__semwait_signal + 10
libsystem_kernel.dylib`__semwait_signal + 10:
-> 0x7fff8a10ce42:  jae    0x7fff8a10ce49            ; __semwait_signal + 17
   0x7fff8a10ce44:  jmpq   0x7fff8a10dffc            ; cerror
   0x7fff8a10ce49:  ret
   0x7fff8a10ce4a:  nop
  thread #4: tid = 0x0003, 0x00007fff8a10ce42 libsystem_kernel.dylib`__semwait_signal + 10,
stop reason = signal SIGSTOP
    frame #0: 0x00007fff8a10ce42 libsystem_kernel.dylib`__semwait_signal + 10
libsystem_kernel.dylib`__semwait_signal + 10:
-> 0x7fff8a10ce42:  jae    0x7fff8a10ce49            ; __semwait_signal + 17
   0x7fff8a10ce44:  jmpq   0x7fff8a10dffc            ; cerror
   0x7fff8a10ce49:  ret
   0x7fff8a10ce4a:  nop
```

```
  thread #5: tid = 0x0004, 0x00007fff8a10ce42 libsystem_kernel.dylib`__semwait_signal + 10,
stop reason = signal SIGSTOP
    frame #0: 0x00007fff8a10ce42 libsystem_kernel.dylib`__semwait_signal + 10
libsystem_kernel.dylib`__semwait_signal + 10:
-> 0x7fff8a10ce42:  jae    0x7fff8a10ce49            ; __semwait_signal + 17
   0x7fff8a10ce44:  jmpq   0x7fff8a10dffc            ; cerror
   0x7fff8a10ce49:  ret
   0x7fff8a10ce4a:  nop
  thread #6: tid = 0x0005, 0x00007fff8a10ce42 libsystem_kernel.dylib`__semwait_signal + 10,
stop reason = signal SIGSTOP
    frame #0: 0x00007fff8a10ce42 libsystem_kernel.dylib`__semwait_signal + 10
libsystem_kernel.dylib`__semwait_signal + 10:
-> 0x7fff8a10ce42:  jae    0x7fff8a10ce49            ; __semwait_signal + 17
   0x7fff8a10ce44:  jmpq   0x7fff8a10dffc            ; cerror
   0x7fff8a10ce49:  ret
   0x7fff8a10ce4a:  nop
(lldb)
```

Note: We see LLDB listed 6 threads with their TIDs numbered from 0. Also we have code disassembly starting from the next instruction that was to be executed if dump wasn't saved. The nice feature is annotated disassembly that shows symbolic names for jump and call destinations.

2. List all threads:

```
(lldb) thread list
Process 0 stopped
* thread #1: tid = 0x0000, 0x00007fff8a10ce42 libsystem_kernel.dylib`__semwait_signal + 10,
stop reason = signal SIGSTOP
  thread #2: tid = 0x0001, 0x00007fff8a10ce42 libsystem_kernel.dylib`__semwait_signal + 10,
stop reason = signal SIGSTOP
  thread #3: tid = 0x0002, 0x00007fff8a10ce42 libsystem_kernel.dylib`__semwait_signal + 10,
stop reason = signal SIGSTOP
  thread #4: tid = 0x0003, 0x00007fff8a10ce42 libsystem_kernel.dylib`__semwait_signal + 10,
stop reason = signal SIGSTOP
  thread #5: tid = 0x0004, 0x00007fff8a10ce42 libsystem_kernel.dylib`__semwait_signal + 10,
stop reason = signal SIGSTOP
  thread #6: tid = 0x0005, 0x00007fff8a10ce42 libsystem_kernel.dylib`__semwait_signal + 10,
stop reason = signal SIGSTOP
```

Note: Compared to GDB here threads are listed according to increasing thread number order.

3. Get all thread stack traces:

```
(lldb) thread backtrace all

* thread #1: tid = 0x0000, 0x00007fff8a10ce42 libsystem_kernel.dylib`__semwait_signal + 10,
stop reason = signal SIGSTOP
    frame #0: 0x00007fff8a10ce42 libsystem_kernel.dylib`__semwait_signal + 10
    frame #1: 0x00007fff84d6edea libsystem_c.dylib`nanosleep + 164
    frame #2: 0x00007fff84d6ec2c libsystem_c.dylib`sleep + 61
    frame #3: 0x00007fff84d6ec08 libsystem_c.dylib`sleep + 25
    frame #4: 0x000000010390bcc3 App1`main + 195
    frame #5: 0x000000010390ba14 App1`start + 52
```

```
  thread #2: tid = 0x0001, 0x00007fff8a10ce42 libsystem_kernel.dylib`__semwait_signal + 10,
stop reason = signal SIGSTOP
    frame #0: 0x00007fff8a10ce42 libsystem_kernel.dylib`__semwait_signal + 10
    frame #1: 0x00007fff84d6edea libsystem_c.dylib`nanosleep + 164
    frame #2: 0x00007fff84d6ec2c libsystem_c.dylib`sleep + 61
    frame #3: 0x00007fff84d6ec08 libsystem_c.dylib`sleep + 25
    frame #4: 0x000000010390ba32 App1`bar_one + 18
    frame #5: 0x000000010390ba49 App1`foo_one + 9
    frame #6: 0x000000010390ba61 App1`thread_one + 17
    frame #7: 0x00007fff84db88bf libsystem_c.dylib`_pthread_start + 335
    frame #8: 0x00007fff84dbbb75 libsystem_c.dylib`thread_start + 13

  thread #3: tid = 0x0002, 0x00007fff8a10ce42 libsystem_kernel.dylib`__semwait_signal + 10,
stop reason = signal SIGSTOP
    frame #0: 0x00007fff8a10ce42 libsystem_kernel.dylib`__semwait_signal + 10
    frame #1: 0x00007fff84d6edea libsystem_c.dylib`nanosleep + 164
    frame #2: 0x00007fff84d6ec2c libsystem_c.dylib`sleep + 61
    frame #3: 0x00007fff84d6ec08 libsystem_c.dylib`sleep + 25
    frame #4: 0x000000010390ba92 App1`bar_two + 18
    frame #5: 0x000000010390baa9 App1`foo_two + 9
    frame #6: 0x000000010390bac1 App1`thread_two + 17
    frame #7: 0x00007fff84db88bf libsystem_c.dylib`_pthread_start + 335
    frame #8: 0x00007fff84dbbb75 libsystem_c.dylib`thread_start + 13

  thread #4: tid = 0x0003, 0x00007fff8a10ce42 libsystem_kernel.dylib`__semwait_signal + 10,
stop reason = signal SIGSTOP
    frame #0: 0x00007fff8a10ce42 libsystem_kernel.dylib`__semwait_signal + 10
    frame #1: 0x00007fff84d6edea libsystem_c.dylib`nanosleep + 164
    frame #2: 0x00007fff84d6ec2c libsystem_c.dylib`sleep + 61
    frame #3: 0x00007fff84d6ec08 libsystem_c.dylib`sleep + 25
    frame #4: 0x000000010390baf2 App1`bar_three + 18
    frame #5: 0x000000010390bb09 App1`foo_three + 9
    frame #6: 0x000000010390bb21 App1`thread_three + 17
    frame #7: 0x00007fff84db88bf libsystem_c.dylib`_pthread_start + 335
    frame #8: 0x00007fff84dbbb75 libsystem_c.dylib`thread_start + 13

  thread #5: tid = 0x0004, 0x00007fff8a10ce42 libsystem_kernel.dylib`__semwait_signal + 10,
stop reason = signal SIGSTOP
    frame #0: 0x00007fff8a10ce42 libsystem_kernel.dylib`__semwait_signal + 10
    frame #1: 0x00007fff84d6edea libsystem_c.dylib`nanosleep + 164
    frame #2: 0x00007fff84d6ec2c libsystem_c.dylib`sleep + 61
    frame #3: 0x00007fff84d6ec08 libsystem_c.dylib`sleep + 25
    frame #4: 0x000000010390bb52 App1`bar_four + 18
    frame #5: 0x000000010390bb69 App1`foo_four + 9
    frame #6: 0x000000010390bb81 App1`thread_four + 17
    frame #7: 0x00007fff84db88bf libsystem_c.dylib`_pthread_start + 335
    frame #8: 0x00007fff84dbbb75 libsystem_c.dylib`thread_start + 13

  thread #6: tid = 0x0005, 0x00007fff8a10ce42 libsystem_kernel.dylib`__semwait_signal + 10,
stop reason = signal SIGSTOP
    frame #0: 0x00007fff8a10ce42 libsystem_kernel.dylib`__semwait_signal + 10
    frame #1: 0x00007fff84d6edea libsystem_c.dylib`nanosleep + 164
    frame #2: 0x00007fff84d6ec2c libsystem_c.dylib`sleep + 61
    frame #3: 0x00007fff84d6ec08 libsystem_c.dylib`sleep + 25
    frame #4: 0x000000010390bbb2 App1`bar_five + 18
    frame #5: 0x000000010390bbc9 App1`foo_five + 9
    frame #6: 0x000000010390bbe1 App1`thread_five + 17
    frame #7: 0x00007fff84db88bf libsystem_c.dylib`_pthread_start + 335
    frame #8: 0x00007fff84dbbb75 libsystem_c.dylib`thread_start + 13
```

4. Switch to the thread #3 and get its stack trace:

```
(lldb) thread select 3
* thread #3: tid = 0x0002, 0x00007fff8a10ce42 libsystem_kernel.dylib`__semwait_signal + 10,
stop reason = signal SIGSTOP
    frame #0: 0x00007fff8a10ce42 libsystem_kernel.dylib`__semwait_signal + 10
libsystem_kernel.dylib`__semwait_signal + 10:
-> 0x7fff8a10ce42:  jae    0x7fff8a10ce49            ; __semwait_signal + 17
   0x7fff8a10ce44:  jmpq   0x7fff8a10dffc            ; cerror
   0x7fff8a10ce49:  ret
   0x7fff8a10ce4a:  nop

(lldb) bt
* thread #3: tid = 0x0002, 0x00007fff8a10ce42 libsystem_kernel.dylib`__semwait_signal + 10,
stop reason = signal SIGSTOP
    frame #0: 0x00007fff8a10ce42 libsystem_kernel.dylib`__semwait_signal + 10
    frame #1: 0x00007fff84d6edea libsystem_c.dylib`nanosleep + 164
    frame #2: 0x00007fff84d6ec2c libsystem_c.dylib`sleep + 61
    frame #3: 0x00007fff84d6ec08 libsystem_c.dylib`sleep + 25
    frame #4: 0x000000010390ba92 App1`bar_two + 18
    frame #5: 0x000000010390baa9 App1`foo_two + 9
    frame #6: 0x000000010390bac1 App1`thread_two + 17
    frame #7: 0x00007fff84db88bf libsystem_c.dylib`_pthread_start + 335
    frame #8: 0x00007fff84dbbb75 libsystem_c.dylib`thread_start + 13
```

Note: We can also list any thread stack trace without switching to it:

```
(lldb) thread backtrace 4
  thread #4: tid = 0x0003, 0x00007fff8a10ce42 libsystem_kernel.dylib`__semwait_signal + 10,
stop reason = signal SIGSTOP
    frame #0: 0x00007fff8a10ce42 libsystem_kernel.dylib`__semwait_signal + 10
    frame #1: 0x00007fff84d6edea libsystem_c.dylib`nanosleep + 164
    frame #2: 0x00007fff84d6ec2c libsystem_c.dylib`sleep + 61
    frame #3: 0x00007fff84d6ec08 libsystem_c.dylib`sleep + 25
    frame #4: 0x000000010390baf2 App1`bar_three + 18
    frame #5: 0x000000010390bb09 App1`foo_three + 9
    frame #6: 0x000000010390bb21 App1`thread_three + 17
    frame #7: 0x00007fff84db88bf libsystem_c.dylib`_pthread_start + 335
    frame #8: 0x00007fff84dbbb75 libsystem_c.dylib`thread_start + 13
```

5. Check that *bar_two* called *sleep* function:

```
(lldb) di -n bar_two
App1`bar_two:
   0x10390ba80:  pushq  %rbp
   0x10390ba81:  movq   %rsp, %rbp
   0x10390ba84:  subq   $16, %rsp
   0x10390ba88:  movl   $4294967295, %edi
   0x10390ba8d:  callq  0x10390bce0               ; symbol stub for: sleep
   0x10390ba92:  movl   %eax, -4(%rbp)
   0x10390ba95:  addq   $16, %rsp
   0x10390ba99:  popq   %rbp
   0x10390ba9a:  ret
   0x10390ba9b:  nopl   (%rax,%rax)
```

```
(lldb) bt
* thread #3: tid = 0x0002, 0x00007fff8a10ce42 libsystem_kernel.dylib`__semwait_signal + 10,
stop reason = signal SIGSTOP
    frame #0: 0x00007fff8a10ce42 libsystem_kernel.dylib`__semwait_signal + 10
    frame #1: 0x00007fff84d6edea libsystem_c.dylib`nanosleep + 164
    frame #2: 0x00007fff84d6ec2c libsystem_c.dylib`sleep + 61
    frame #3: 0x00007fff84d6ec08 libsystem_c.dylib`sleep + 25
    frame #4: 0x000000010390ba92 App1`bar_two + 18
    frame #5: 0x000000010390baa9 App1`foo_two + 9
    frame #6: 0x000000010390bac1 App1`thread_two + 17
    frame #7: 0x00007fff84db88bf libsystem_c.dylib`_pthread_start + 335
    frame #8: 0x00007fff84dbbb75 libsystem_c.dylib`thread_start + 13
```

6. Compare with Intel disassembly flavor:

```
(lldb) settings set target.x86-disassembly-flavor intel

(lldb) di -n bar_two
App1`bar_two:
   0x10390ba80:  push   RBP
   0x10390ba81:  mov    RBP, RSP
   0x10390ba84:  sub    RSP, 16
   0x10390ba88:  mov    EDI, 4294967295
   0x10390ba8d:  call   0x10390bce0               ; symbol stub for: sleep
   0x10390ba92:  mov    DWORD PTR [RBP - 4], EAX
   0x10390ba95:  add    RSP, 16
   0x10390ba99:  pop    RBP
   0x10390ba9a:  ret
   0x10390ba9b:  nop    DWORD PTR [RAX + RAX]

(lldb) set disassembly-flavor att
(lldb)
```

7. Follow *bar_two* function to *sleep* function code:

```
(lldb) di -n bar_two
App1`bar_two:
   0x10390ba80:  pushq  %rbp
   0x10390ba81:  movq   %rsp, %rbp
   0x10390ba84:  subq   $16, %rsp
   0x10390ba88:  movl   $4294967295, %edi
   0x10390ba8d:  callq  0x10390bce0               ; symbol stub for: sleep
   0x10390ba92:  movl   %eax, -4(%rbp)
   0x10390ba95:  addq   $16, %rsp
   0x10390ba99:  popq   %rbp
   0x10390ba9a:  ret
   0x10390ba9b:  nopl   (%rax,%rax)

(lldb) di -a 0x10390bce0
App1`symbol stub for: sleep:
   0x10390bce0:  jmpq   *866(%rip)               ; (void *)0x00007fff84d6ebef: sleep
```

8. Disassemble the annotated value:

```
(lldb) di -a 0x00007fff84d6ebef
libsystem_c.dylib`sleep:
   0x7fff84d6ebef:  pushq  %rbp
   0x7fff84d6ebf0:  movq   %rsp, %rbp
   0x7fff84d6ebf3:  pushq  %rbx
   0x7fff84d6ebf4:  subq   $40, %rsp
   0x7fff84d6ebf8:  testl  %edi, %edi
   0x7fff84d6ebfa:  movl   %edi, %ebx
   0x7fff84d6ebfc:  jns    0x7fff84d6ec11            ; sleep + 34
   0x7fff84d6ebfe:  movl   $2147483647, %edi
   0x7fff84d6ec03:  callq  0x7fff84d6ebef            ; sleep
   0x7fff84d6ec08:  leal   -2147483647(%rbx,%rax), %eax
   0x7fff84d6ec0f:  jmp    0x7fff84d6ec4f            ; sleep + 96
   0x7fff84d6ec11:  movl   %ebx, %eax
   0x7fff84d6ec13:  movq   %rax, -24(%rbp)
   0x7fff84d6ec17:  movq   $0, -16(%rbp)
   0x7fff84d6ec1f:  leaq   -24(%rbp), %rdi
   0x7fff84d6ec23:  leaq   -40(%rbp), %rsi
   0x7fff84d6ec27:  callq  0x7fff84d6ed46            ; nanosleep
   0x7fff84d6ec2c:  cmpl   $-1, %eax
   0x7fff84d6ec2f:  je     0x7fff84d6ec37            ; sleep + 72
   0x7fff84d6ec31:  xorl   %ebx, %ebx
   0x7fff84d6ec33:  movl   %ebx, %eax
   0x7fff84d6ec35:  jmp    0x7fff84d6ec4f            ; sleep + 96
   0x7fff84d6ec37:  callq  0x7fff84e0cc88            ; __error
   0x7fff84d6ec3c:  cmpl   $4, (%rax)
   0x7fff84d6ec3f:  jne    0x7fff84d6ec33            ; sleep + 68
   0x7fff84d6ec41:  cmpq   $0, -32(%rbp)
   0x7fff84d6ec46:  setne  %al
   0x7fff84d6ec49:  movzbl %al, %eax
   0x7fff84d6ec4c:  addl   -40(%rbp), %eax
   0x7fff84d6ec4f:  addq   $40, %rsp
   0x7fff84d6ec53:  popq   %rbx
   0x7fff84d6ec54:  popq   %rbp
```

9. Compare stack trace for thread #3 (core thread 2) and its module info with the diagnostic report App1_1394.crash:

```
Process:         App1 [1394]
Path:            /Users/USER/Documents/*/App1
Identifier:      App1
Version:         ??? (???)
Code Type:       X86-64 (Native)
Parent Process:  bash [661]

Date/Time:       2012-07-24 00:20:26.078 +0100
OS Version:      Mac OS X 10.7.4 (11E53)
Report Version:  9

Crashed Thread:  0  Dispatch queue: com.apple.main-thread

Exception Type:  EXC_CRASH (SIGABRT)
Exception Codes: 0x0000000000000000, 0x0000000000000000

Thread 0 Crashed:: Dispatch queue: com.apple.main-thread
0   libsystem_kernel.dylib              0x00007fff8a10ce42 __semwait_signal + 10
1   libsystem_c.dylib                   0x00007fff84d6edea nanosleep + 164
2   libsystem_c.dylib                   0x00007fff84d6ec2c sleep + 61
3   libsystem_c.dylib                   0x00007fff84d6ec08 sleep + 25
4   App1                                0x000000010390bcc3 main + 195
5   App1                                0x000000010390ba14 start + 52
```

```
Thread 1:
0   libsystem_kernel.dylib              0x00007fff8a10ce42 __semwait_signal + 10
1   libsystem_c.dylib                   0x00007fff84d6edea nanosleep + 164
2   libsystem_c.dylib                   0x00007fff84d6ec2c sleep + 61
3   libsystem_c.dylib                   0x00007fff84d6ec08 sleep + 25
4   App1                                0x0000000010390ba32 bar_one + 18
5   App1                                0x0000000010390ba49 foo_one + 9
6   App1                                0x0000000010390ba61 thread_one + 17
7   libsystem_c.dylib                   0x00007fff84db88bf _pthread_start + 335
8   libsystem_c.dylib                   0x00007fff84dbbb75 thread_start + 13

Thread 2:
0   libsystem_kernel.dylib              0x00007fff8a10ce42 __semwait_signal + 10
1   libsystem_c.dylib                   0x00007fff84d6edea nanosleep + 164
2   libsystem_c.dylib                   0x00007fff84d6ec2c sleep + 61
3   libsystem_c.dylib                   0x00007fff84d6ec08 sleep + 25
4   App1                                0x0000000010390ba92 bar_two + 18
5   App1                                0x0000000010390baa9 foo_two + 9
6   App1                                0x0000000010390bac1 thread_two + 17
7   libsystem_c.dylib                   0x00007fff84db88bf _pthread_start + 335
8   libsystem_c.dylib                   0x00007fff84dbbb75 thread_start + 13

Thread 3:
0   libsystem_kernel.dylib              0x00007fff8a10ce42 __semwait_signal + 10
1   libsystem_c.dylib                   0x00007fff84d6edea nanosleep + 164
2   libsystem_c.dylib                   0x00007fff84d6ec2c sleep + 61
3   libsystem_c.dylib                   0x00007fff84d6ec08 sleep + 25
4   App1                                0x0000000010390baf2 bar_three + 18
5   App1                                0x0000000010390bb09 foo_three + 9
6   App1                                0x0000000010390bb21 thread_three + 17
7   libsystem_c.dylib                   0x00007fff84db88bf _pthread_start + 335
8   libsystem_c.dylib                   0x00007fff84dbbb75 thread_start + 13

Thread 4:
0   libsystem_kernel.dylib              0x00007fff8a10ce42 __semwait_signal + 10
1   libsystem_c.dylib                   0x00007fff84d6edea nanosleep + 164
2   libsystem_c.dylib                   0x00007fff84d6ec2c sleep + 61
3   libsystem_c.dylib                   0x00007fff84d6ec08 sleep + 25
4   App1                                0x0000000010390bb52 bar_four + 18
5   App1                                0x0000000010390bb69 foo_four + 9
6   App1                                0x0000000010390bb81 thread_four + 17
7   libsystem_c.dylib                   0x00007fff84db88bf _pthread_start + 335
8   libsystem_c.dylib                   0x00007fff84dbbb75 thread_start + 13

Thread 5:
0   libsystem_kernel.dylib              0x00007fff8a10ce42 __semwait_signal + 10
1   libsystem_c.dylib                   0x00007fff84d6edea nanosleep + 164
2   libsystem_c.dylib                   0x00007fff84d6ec2c sleep + 61
3   libsystem_c.dylib                   0x00007fff84d6ec08 sleep + 25
4   App1                                0x0000000010390bbb2 bar_five + 18
5   App1                                0x0000000010390bbc9 foo_five + 9
6   App1                                0x0000000010390bbe1 thread_five + 17
7   libsystem_c.dylib                   0x00007fff84db88bf _pthread_start + 335
8   libsystem_c.dylib                   0x00007fff84dbbb75 thread_start + 13

Thread 0 crashed with X86 Thread State (64-bit):
  rax: 0x0000000000000004  rbx: 0x00007fff6350aa08  rcx: 0x00007fff6350a9c8  rdx: 0x0000000000000001
  rdi: 0x0000000000000c03  rsi: 0x0000000000000000  rbp: 0x00007fff6350a9f0  rsp: 0x00007fff6350a9c8
   r8: 0x000000007fffffff   r9: 0x0000000000000000  r10: 0x0000000000000001  r11: 0xffffff80002da8d0
  r12: 0x0000000000000000  r13: 0x0000000000000000  r14: 0x00007fff6350aa18  r15: 0x0000000000000000
  rip: 0x00007fff8a10ce42  rfl: 0x0000000000000247  cr2: 0x0000000103d0b880
Logical CPU: 0
```

```
Binary Images:
       0x10390b000 -        0x10390bfff +App1 (??? - ???) <5BC0342F-7E97-3A7D-8EA6-75A0468021EA>
/Users/USER/Documents/*/App1
    0x7fff6350b000 -     0x7fff6353fbaf  dyld (195.6 - ???) <0CD1B35B-A28F-32DA-B72E-452EAD609613> /usr/lib/dyld
    0x7fff849f2000 -     0x7fff84a0ffff  libxpc.dylib (77.19.0 - compatibility 1.0.0) <9F57891B-D7EF-3050-BEDD-
21E7C6668248> /usr/lib/system/libxpc.dylib
    0x7fff84d68000 -     0x7fff84d69ff7  libsystem_blocks.dylib (53.0.0 - compatibility 1.0.0) <8BCA214A-8992-34B2-
A8B9-B74DEACA1869> /usr/lib/system/libsystem_blocks.dylib
    0x7fff84d6a000 -     0x7fff84e47fef  libsystem_c.dylib (763.13.0 - compatibility 1.0.0) <41B43515-2806-3FBC-ACF1-
A16F35B7E290> /usr/lib/system/libsystem_c.dylib
    0x7fff85022000 -     0x7fff85030fff  libdispatch.dylib (187.9.0 - compatibility 1.0.0) <1D5BE322-A9B9-3BCE-8FAC-
076FB07CF54A> /usr/lib/system/libdispatch.dylib
    0x7fff855f0000 -     0x7fff855f1fff  libunc.dylib (24.0.0 - compatibility 1.0.0) <337960EE-0A85-3DD0-A760-
7134CF4C0AFF> /usr/lib/system/libunc.dylib
    0x7fff85ae3000 -     0x7fff85ae4ff7  libremovefile.dylib (21.1.0 - compatibility 1.0.0) <739E6C83-AA52-3C6C-A680-
B37FE2888A04> /usr/lib/system/libremovefile.dylib
    0x7fff89114000 -     0x7fff89118fff  libmathCommon.A.dylib (2026.0.0 - compatibility 1.0.0) <FF83AFF7-42B2-306E-
90AF-D539C51A4542> /usr/lib/system/libmathCommon.A.dylib
    0x7fff89119000 -     0x7fff8911dfff  libdyld.dylib (195.5.0 - compatibility 1.0.0) <380C3F44-0CA7-3514-8080-
46D1C9DF4FCD> /usr/lib/system/libdyld.dylib
    0x7fff89740000 -     0x7fff89741ff7  libsystem_sandbox.dylib (??? - ???) <96D38E74-F18F-3CCB-A20B-E8E3ADC4E166>
/usr/lib/system/libsystem_sandbox.dylib
    0x7fff8a0ef000 -     0x7fff8a0f5fff  libmacho.dylib (800.0.0 - compatibility 1.0.0) <165514D7-1BFA-38EF-A151-
676DCD21FB64> /usr/lib/system/libmacho.dylib
    0x7fff8a0f6000 -     0x7fff8a116fff  libsystem_kernel.dylib (1699.26.8 - compatibility 1.0.0) <1DDC0B0F-DB2A-34D6-
895D-E5B2B5618946> /usr/lib/system/libsystem_kernel.dylib
    0x7fff8a2ac000 -     0x7fff8a2b4fff  libsystem_dnssd.dylib (??? - ???) <D9BB1F87-A42B-3CBC-9DC2-FC07FCEF0016>
/usr/lib/system/libsystem_dnssd.dylib
    0x7fff8ae26000 -     0x7fff8ae61fff  libsystem_info.dylib (??? - ???) <35F90252-2AE1-32C5-8D34-782C614D9639>
/usr/lib/system/libsystem_info.dylib
    0x7fff8b248000 -     0x7fff8b24afff  libquarantine.dylib (36.6.0 - compatibility 1.0.0) <0EBF714B-4B69-3E1F-9A7D-
6BBC2AACB310> /usr/lib/system/libquarantine.dylib
    0x7fff8b3b4000 -     0x7fff8b3b4fff  libkeymgr.dylib (23.0.0 - compatibility 1.0.0) <61EFED6A-A407-301E-B454-
CD18314F0075> /usr/lib/system/libkeymgr.dylib
    0x7fff8b3dd000 -     0x7fff8b3e2fff  libcompiler_rt.dylib (6.0.0 - compatibility 1.0.0) <98ECD5F6-E85C-32A5-98CD-
8911230CB66A> /usr/lib/system/libcompiler_rt.dylib
    0x7fff8bd1a000 -     0x7fff8bd1bfff  libdnsinfo.dylib (395.11.0 - compatibility 1.0.0) <853BAAA5-270F-3FDC-B025-
D448DB72E1C3> /usr/lib/system/libdnsinfo.dylib
    0x7fff8c528000 -     0x7fff8c52dff7  libsystem_network.dylib (??? - ???) <5DE7024E-1D2D-34A2-80F4-08326331A75B>
/usr/lib/system/libsystem_network.dylib
    0x7fff8cfa3000 -     0x7fff8cfadff7  liblaunch.dylib (392.38.0 - compatibility 1.0.0) <6ECB7F19-B384-32C1-8652-
2463C1CF4815> /usr/lib/system/liblaunch.dylib
    0x7fff8fe02000 -     0x7fff8fe09fff  libcopyfile.dylib (85.1.0 - compatibility 1.0.0) <0AB51EE2-E914-358C-AC19-
47BC024BDAE7> /usr/lib/system/libcopyfile.dylib
    0x7fff8fe4b000 -     0x7fff8fe8dff7  libcommonCrypto.dylib (55010.0.0 - compatibility 1.0.0) <BB770C22-8C57-365A-
8716-4A3C36AE7BFB> /usr/lib/system/libcommonCrypto.dylib
    0x7fff90c0f000 -     0x7fff90c18ff7  libsystem_notify.dylib (80.1.0 - compatibility 1.0.0) <A4D651E3-D1C6-3934-
AD49-7A104FD14596> /usr/lib/system/libsystem_notify.dylib
    0x7fff91376000 -     0x7fff913a3fe7  libSystem.B.dylib (159.1.0 - compatibility 1.0.0) <7BEBB139-50BB-3112-947A-
F4AA168F991C> /usr/lib/libSystem.B.dylib
    0x7fff91489000 -     0x7fff9148fff7  libunwind.dylib (30.0.0 - compatibility 1.0.0) <1E9C6C8C-CBE8-3F4B-A5B5-
E03E3AB53231> /usr/lib/system/libunwind.dylib
    0x7fff91a22000 -     0x7fff91a27fff  libcache.dylib (47.0.0 - compatibility 1.0.0) <1571C3AB-BCB2-38CD-B3B2-
C5FC3F927C6A> /usr/lib/system/libcache.dylib

External Modification Summary:
  Calls made by other processes targeting this process:
    task_for_pid: 2
    thread_create: 0
    thread_set_state: 0
  Calls made by this process:
    task_for_pid: 0
    thread_create: 0
    thread_set_state: 0
  Calls made by all processes on this machine:
    task_for_pid: 2696
    thread_create: 0
    thread_set_state: 0
```

```
VM Region Summary:
ReadOnly portion of Libraries: Total=50.2M resident=50.2M(100%) swapped_out_or_unallocated=0K(0%)
Writable regions: Total=38.9M written=10.8M(28%) resident=42.6M(110%) swapped_out=0K(0%)
unallocated=16777216.0T(45221404475392%)

REGION TYPE                      VIRTUAL
===========                      =======
MALLOC                             1220K
Stack                              66.6M
__DATA                              464K
__LINKEDIT                         47.7M
__TEXT                             2484K
shared memory                        12K
===========                      =======
TOTAL                             118.4M
```

10. Get App1 data section from the output of vmmap_1394.log:

```
Virtual Memory Map of process 1394 (App1)
Output report format:  2.2  -- 64-bit process

==== Non-writable regions for process 1394
__TEXT                 000000010390b000-000000010390c000 [    4K] r-x/rwx SM=COW  /Users/DumpAnalysis/Documents/AMCDA-
Dumps/Apps/App1/Build/Products/Release/App1

[...]

==== Writable regions for process 1394
__DATA                 000000010390c000-000000010390d000 [    4K] rw-/rwx SM=PRV  /Users/DumpAnalysis/Documents/AMCDA-
Dumps/Apps/App1/Build/Products/Release/App1

[...]
```

11. Compare with the section information in the core dump:

```
(lldb) image dump sections App1
Sections for '/Users/DumpAnalysis/Documents/AMCDA-Dumps/Apps/App1/Build/Products/Release/App1' (x86_64):
  SectID     Type             Load Address                                  File Off.  File Size  Flags      Section Name
  ---------- ---------------- --------------------------------------------  ---------- ---------- ---------- ----------------------------
  0x00000100 container        [0x0000000000000000-0x0000000100000000)* 0x00000000 0x00000000 0x00000000 App1.__PAGEZERO
  0x00000200 container        [0x000000010390b000-0x000000010390c000)  0x00000000 0x00001000 0x00000000 App1.__TEXT
  0x00000001 code             [0x000000010390b9e0-0x000000010390bcd3)  0x000009e0 0x000002f3 0x80000400 App1.__TEXT.__text
  0x00000002 code             [0x000000010390bcd4-0x000000010390bce6)  0x00000cd4 0x00000012 0x80000408 App1.__TEXT.__stubs
  0x00000003 code             [0x000000010390bce8-0x000000010390bd16)  0x00000ce8 0x0000002e 0x80000400 App1.__TEXT.__stub_helper
  0x00000004 code             [0x000000010390bd16-0x000000010390bd66)  0x00000d16 0x00000050 0x00000000 App1.__TEXT.__unwind_info
  0x00000005 eh-frame         [0x000000010390bd68-0x000000010390c000)  0x00000d68 0x00000298 0x00000000 App1.__TEXT.__eh_frame
  0x00000300 container        [0x000000010390c000-0x000000010390d000)  0x00001000 0x00001000 0x00000000 App1.__DATA
  0x00000006 data             [0x000000010390c000-0x000000010390c028)  0x00001000 0x00000028 0x00000000 App1.__DATA.__program_vars
  0x00000007 data-ptrs        [0x000000010390c028-0x000000010390c038)  0x00001028 0x00000010 0x00000006 App1.__DATA.__nl_symbol_ptr
  0x00000008 data-ptrs        [0x000000010390c038-0x000000010390c050)  0x00001038 0x00000018 0x00000007 App1.__DATA.__la_symbol_ptr
  0x00000009 zero-fill        [0x000000010390c050-0x000000010390c070)  0x00000000 0x00000000 0x00000001 App1.__DATA.__common
  0x00000400 container        [0x000000010390d000-0x000000010390d3b0)  0x00002000 0x000003b0 0x00000000 App1.__LINKEDIT
```

12. Dump data with possible symbolic information:

```
(lldb) x/512a 0x000000010390c000
error: Normally, 'memory read' will not read over 1024 bytes of data.
error: Please use --force to override this restriction just once.
error: or set target.max-memory-read-size if you will often need a larger limit.
```

```
(lldb) x/512a 0x000000010390c000 --force
0x10390c000: 0x000000010390b000
0x10390c008: 0x000000010390c050 App1`NXArgc
0x10390c010: 0x000000010390c058 App1`NXArgv
0x10390c018: 0x000000010390c060 App1`environ
0x10390c020: 0x000000010390c068
0x10390c028: 0x00007fff8911a6a0 libdyld.dylib`dyld_stub_binder
0x10390c030: 0x00007fff63546d80 dyld`initialPoolContent + 2128
0x10390c038: 0x000000010390bcf8
0x10390c040: 0x00007fff84dbab01 libsystem_c.dylib`pthread_create
0x10390c048: 0x00007fff84d6ebef libsystem_c.dylib`sleep
0x10390c050: 0x0000000000000001
0x10390c058: 0x00007fff6350aaf0
0x10390c060: 0x00007fff6350ab00
0x10390c068: 0x00007fff6350ac73
0x10390c070: 0x0000000000000000
0x10390c078: 0x0000000000000000
0x10390c080: 0x0000000000000000
0x10390c088: 0x0000000000000000
0x10390c090: 0x0000000000000000
[...]
```

13. Dump the contents of memory pointed to by *environ* variable in null-terminated string format:

```
(lldb) x/100s 0x00007fff6350ab00
[...]
0x7fff6350abd5:  ""
0x7fff6350abd6:  ""
0x7fff6350abd7:  ""
0x7fff6350abd8:  "/Users/DumpAnalysis/Documents/AMCDA-Dumps/Apps/App1/Build/Products/Release/App1"
0x7fff6350ac28:  "/Users/DumpAnalysis/Documents/AMCDA-Dumps/Apps/App1/Build/Products/Release/App1"
0x7fff6350ac78:  "TERM_PROGRAM=Apple_Terminal"
0x7fff6350ac94:  "TERM=xterm-256color"
0x7fff6350aca8:  "SHELL=/bin/bash"
0x7fff6350acb8:  "TMPDIR=/var/folders/ww/rmtqfhl93yj4213dnl2rqy6w0000gn/T/"
0x7fff6350acf1:  "Apple_PubSub_Socket_Render=/tmp/launch-mYEvtN/Render"
0x7fff6350ad26:  "TERM_PROGRAM_VERSION=303.2"
0x7fff6350ad41:  "TERM_SESSION_ID=2B039506-8384-4620-B354-120BE31AEA84"
0x7fff6350ad76:  "USER=DumpAnalysis"
0x7fff6350ad88:  "COMMAND_MODE=unix2003"
0x7fff6350ad9e:  "SSH_AUTH_SOCK=/tmp/launch-9sm7dH/Listeners"
0x7fff6350adc9:  "__CF_USER_TEXT_ENCODING=0x1F5:0:0"
0x7fff6350adeb:  "Apple_Ubiquity_Message=/tmp/launch-tWsFs8/Apple_Ubiquity_Message"
0x7fff6350ae2c:
"PATH=/Applications/Xcode.app/Contents/Developer/usr/bin/:/usr/bin:/bin:/usr/sbin:/sbin:/usr/local/bin:/usr/X11/bin"
0x7fff6350ae9f:  "PWD=/Users/DumpAnalysis"
0x7fff6350aeb7:  "LANG=en_IE.UTF-8"
---Type <return> to continue, or q <return> to quit---
0x7fff6350aec8:  "SHLVL=1"
0x7fff6350aed0:  "HOME=/Users/DumpAnalysis"
0x7fff6350aee9:  "LOGNAME=DumpAnalysis"
0x7fff6350aefe:  "DISPLAY=/tmp/launch-M8cgb1/org.x:0"
0x7fff6350af21:  "SECURITYSESSIONID=186af"
0x7fff6350af39:  "_=/Users/DumpAnalysis/Documents/AMCDA-Dumps/Apps/App1/Build/Products/Release/App1"
0x7fff6350af8b:  "OLDPWD=/usr/share/man/man1"
0x7fff6350afa6:  ""
0x7fff6350afa7:  ""
0x7fff6350afa8:  "stack_guard=0x74843dc6068699c3"
0x7fff6350afc7:  "malloc_entropy=0x7406669509034332,0x71e4e2253a6d22b0"
0x7fff6350affc:  ""
0x7fff6350affd:  ""
```

14. Get the list of loaded modules:

```
(lldb) image list
[  0] 5BC0342F-7E97-3A7D-8EA6-75A0468021EA 0x000000010390b000 /Users/DumpAnalysis/Documents/AMCDA-
Dumps/Apps/App1/Build/Products/Release/App1
[  1] 7BEBB139-50BB-3112-947A-F4AA168F991C 0x00007fff91376000 /usr/lib/libSystem.B.dylib (0x00007fff91376000)
[  2] 1571C3AB-BCB2-38CD-B3B2-C5FC3F927C6A 0x00007fff91a22000 /usr/lib/system/libcache.dylib (0x00007fff91a22000)
[  3] BB770C22-8C57-365A-8716-4A3C36AE7BFB 0x00007fff8fe4b000 /usr/lib/system/libcommonCrypto.dylib (0x00007fff8fe4b000)
[  4] 98ECD5F6-E85C-32A5-98CD-8911230CB66A 0x00007fff8b3dd000 /usr/lib/system/libcompiler_rt.dylib (0x00007fff8b3dd000)
[  5] 0AB51EE2-E914-358C-AC19-47BC024BDAE7 0x00007fff8fe02000 /usr/lib/system/libcopyfile.dylib (0x00007fff8fe02000)
[  6] 1D5BE322-A9B9-3BCE-8FAC-076FB07CF54A 0x00007fff85022000 /usr/lib/system/libdispatch.dylib (0x00007fff85022000)
[  7] 853BAAA5-270F-3FDC-B025-D448DB72E1C3 0x00007fff8bd1a000 /usr/lib/system/libdnsinfo.dylib (0x00007fff8bd1a000)
[  8] 380C3F44-0CA7-3514-8080-46D1C9DF4FCD 0x00007fff89119000 /usr/lib/system/libdyld.dylib (0x00007fff89119000)
[  9] 61EFED6A-A407-301E-B454-CD18314F0075 0x00007fff8b3b4000 /usr/lib/system/libkeymgr.dylib (0x00007fff8b3b4000)
[ 10] 6ECB7F19-B384-32C1-8652-2463C1CF4815 0x00007fff8cfa3000 /usr/lib/system/liblaunch.dylib (0x00007fff8cfa3000)
[ 11] 165514D7-1BFA-38EF-A151-676DCD21FB64 0x00007fff8a0ef000 /usr/lib/system/libmacho.dylib (0x00007fff8a0ef000)
[ 12] FF83AFF7-42B2-306E-90AF-D539C51A4542 0x00007fff89114000 /usr/lib/system/libmathCommon.A.dylib (0x00007fff89114000)
[ 13] 0EBF714B-4B69-3E1F-9A7D-6BBC2AACB310 0x00007fff8b248000 /usr/lib/system/libquarantine.dylib (0x00007fff8b248000)
[ 14] 739E6C83-AA52-3C6C-A680-B37FE2888A04 0x00007fff85ae3000 /usr/lib/system/libremovefile.dylib (0x00007fff85ae3000)
[ 15] 8BCA214A-8992-34B2-A8B9-B74DEACA1869 0x00007fff84d68000 /usr/lib/system/libsystem_blocks.dylib (0x00007fff84d68000)
[ 16] 41B43515-2806-3FBC-ACF1-A16F35B7E290 0x00007fff84d6a000 /usr/lib/system/libsystem_c.dylib (0x00007fff84d6a000)
[ 17] D9BB1F87-A42B-3CBC-9DC2-FC07FCEF0016 0x00007fff8a2ac000 /usr/lib/system/libsystem_dnssd.dylib (0x00007fff8a2ac000)
[ 18] 35F90252-2AE1-32C5-8D34-782C614D9639 0x00007fff8ae26000 /usr/lib/system/libsystem_info.dylib (0x00007fff8ae26000)
[ 19] 1DDC0B0F-DB2A-34D6-895D-E5B2B5618946 0x00007fff8a0f6000 /usr/lib/system/libsystem_kernel.dylib (0x00007fff8a0f6000)
[ 20] 5DE7024E-1D2D-34A2-80F4-08326331A75B 0x00007fff8c528000 /usr/lib/system/libsystem_network.dylib (0x00007fff8c528000)
[ 21] A4D651E3-D1C6-3934-AD49-7A104FD14596 0x00007fff90c0f000 /usr/lib/system/libsystem_notify.dylib (0x00007fff90c0f000)
[ 22] 96D38E74-F18F-3CCB-A20B-E8E3ADC4E166 0x00007fff89740000 /usr/lib/system/libsystem_sandbox.dylib (0x00007fff89740000)
[ 23] 337960EE-0A85-3DD0-A760-7134CF4C0AFF 0x00007fff855f0000 /usr/lib/system/libunc.dylib (0x00007fff855f0000)
[ 24] 1E9C6C8C-CBE8-3F4B-A5B5-E03E3AB53231 0x00007fff91489000 /usr/lib/system/libunwind.dylib (0x00007fff91489000)
[ 25] 9F57891B-D7EF-3050-BEDD-21E7C6668248 0x00007fff849f2000 /usr/lib/system/libxpc.dylib (0x00007fff849f2000)
[ 26] 0CD1B35B-A28F-32DA-B72E-452EAD609613 0x00007fff6350b000 /usr/lib/dyld (0x00007fff6350b000)
(lldb)
```