



Debugging.TV

Frame 0x34

Presenter: Dmitry Vostokov

SOFTWARE DIAGNOSTICS SERVICES

www.PatternDiagnostics.com

Including Memory Dump and Software Trace Analysis Audit, Seminars,
Certification and Training

Sponsors

OPENTASK
Iterative and Incremental Publishing

A world map in shades of blue and black, serving as a background for the Opentask logo.

Topics

- GDB debugging for Android
- Android processes and threads
- Memory analysis patterns
- Android core dumps

Setting Environment

- Remote: GDB Server debugging
- Local: GDB inside Android device
 - Rooted device (Samsung Galaxy Tab 2 7.0, Android 4.2.2)
 - (Eclipse +) Android SDK
 - ADB
 - Dan Drown <http://dan.drown.org/android/howto/gdb.html>

ADB session..

Spiking Thread

```
root@android:/data/local/tmp/bin # ps -t
ps -t
USER      PID     PPID  VSIZE  RSS      WCHAN    PC         NAME
[...]
u0_a33    30703  445   522908 44880    ffffffff 401c6044 S  com.example.spikingthread

u0_a33    30707  30703 522908 44880    c00fdc38 401c62a0 S  GC
u0_a33    30708  30703 522908 44880    c00ddbc8 401c5b28 S  Signal Catcher
u0_a33    30709  30703 522908 44880    c01969c0 401c526c S  JDWP
u0_a33    30710  30703 522908 44880    c00fdc38 401c62a0 S  Compiler
u0_a33    30711  30703 522908 44880    c00fdc38 401c62a0 S  ReferenceQueueD
u0_a33    30712  30703 522908 44880    c00fdc38 401c62a0 S  FinalizerDaemon
u0_a33    30713  30703 522908 44880    c00fdc38 401c62a0 S  FinalizerWatchd
u0_a33    30714  30703 522908 44880    c0465b2c 401c5148 S  Binder_1
u0_a33    30715  30703 522908 44880    c0465b2c 401c5148 S  Binder_2
u0_a33    30727  30703 522908 44880    c00fdc38 401c62a0 S  Thread-758
u0_a33    30774  30703 522908 44880    00000000 5f54ec08 R  Thread-759
```

```
root@android:/data/local/tmp/bin # ./gdb --pid=30727
(gdb) bt
bt
#0  0x401c62a0 in __futex_syscall3 () from /system/lib/libc.so
#1  0x401bc580 in __pthread_cond_timedwait_relative ()
    from /system/lib/libc.so
```

```
root@android:/data/local/tmp/bin # ./gdb --pid=30774
(gdb) bt
bt
#0  0x5f54e64c in ?? ()
#1  0x5f54e976 in ?? ()
Backtrace stopped: previous frame identical to this frame
```

```
(gdb) x/i $pc
x/i $pc
=> 0x5f54e64c:  cbz    r2, 0x5f54e660
```


Invalid Pointer

Program terminated with signal 11, Segmentation fault.

#0 0x40128be2 in ?? () from /system/lib/libc.so

(gdb) bt

bt

#0 **0x40128be2** in ?? () from /system/lib/libc.so

#1 0x4012c54c in _fwalk () from /system/lib/libc.so

#2 0x4012c54c in _fwalk () from /system/lib/libc.so

Backtrace stopped: previous frame identical to this frame

(gdb) info r

info r

| | | |
|-----------|-------------------|------------|
| r0 | 0x27 | 39 |
| r1 | 0xdeadbaad | 3735927469 |
| r2 | 0x40159258 | 1075155544 |
| r3 | 0x0 | 0 |
| r4 | 0x0 | 0 |
| r5 | 0xbe9ff564 | 3198154084 |
| r6 | 0x32542c | 3298348 |
| r7 | 0x648 | 1608 |
| r8 | 0x8682f0 | 8815344 |
| r9 | 0x1 | 1 |
| r10 | 0x93b2d8 | 9679576 |
| r11 | 0xbe9ff6c4 | 3198154436 |
| r12 | 0x323010 | 3289104 |
| sp | 0xbe9ff560 | 0xbe9ff560 |
| lr | 0x4012c54d | 1074971981 |
| pc | 0x40128be2 | 0x40128be2 |
| fps | 0x0 | 0 |
| cpsr | 0x60000030 | 1610612784 |

(gdb) x/i \$pc

x/i \$pc

=> **0x40128be2:** strb r0, [r1, #0]

!Ad Hardcore Software Diagnostics Training

| | |
|----------------------|---|
| Nov - December, 2013 | <u>Psychology of Software Diagnostics</u> (FREE) <u>Semiotics of Debugging</u> (FREE) <u>Generative Software Narratology</u> (FREE) <u>Software Diagnostics: Requirements, Architecture, Design, Implementation and Improvement</u> (FREE) |
| October 25-28, 2013 | <u>Accelerated Disassembly, Reconstruction and Reversing</u> |
| November 15-25, 2013 | <u>Accelerated Windows Memory Dump Analysis</u> |
| December | Accelerated Linux Core Dump Analysis |

Debugging.TV

Now on YouTube!

<http://www.youtube.com/DebuggingTV>