```
root@granite2v8:~# gdbserver localhost:2345 ./jbigtest
Process ./jbigtest created; pid = 351
gdbserver: Unable to determine the number of hardware watchpoints available.
gdbserver: Unable to determine the number of hardware breakpoints available.
Listening on port 2345
Remote debugging from host 10.38.52.106

jbig_platform_get_config codec 0
UIO_LIB: uio_lib_init
posix: posix_create_thread start=0x7fb7e96fdc stack=0x7fb7eae150 stack_size=131072
UIO_LIB: Waiting for UIO interrupt event
UIO_LIB: uio_locate_dev_by_number: found dev: jbig-codec-core-uio0, num = 0x4, ver=devicetree
UIO_LIB: uio_get_device_map: map for /sys/class/uio/uio4/maps/map0
UIO_LIB: num = 0
UIO_LIB: name = /jbig-codec-core-uio0
UIO_LIB: phy_addr = 0xf9000000
UIO_LIB: size = 4096
UIO_LIB: Opened device jbig-codec-core-uio0
dev_jbig 0x416160 map: 0x4161f0, map->virt_addr 0xb7ffa000
UIO_LIB: uio_locate_dev_by_number: found dev: jbig-codec-idma-uio0, num = 0x5, ver=devicetree
UIO_LIB: uio_get_device_map: map for /sys/class/uio/uio5/maps/map0
UIO_LIB: num = 0
UIO_LIB: name = /jbig-codec-idma-uio0
UIO_LIB: phy_addr = 0xf9001000
UIO_LIB: size = 4096
UIO_LIB: Opened device jbig-codec-idma-uio0
dev_idma 0x416280 map: 0x416310, map->virt_addr 0xb7ff9000
UIO_LIB: uio_locate_dev_by_number: found dev: jbig-codec-odma-uio0, num = 0x6, ver=devicetree
UIO_LIB: uio_get_device_map: map for /sys/class/uio/uio6/maps/map0
UIO_LIB: num = 0
UIO_LIB: name = /jbig-codec-odma-uio0
UIO_LIB: phy_addr = 0xf9002000
UIO_LIB: size = 4096
UIO_LIB: Opened device jbig-codec-odma-uio0
dev_odma 0x4163a0 map: 0x416430, map->virt_addr 0xb7ff8000
UIO_LIB: uio_locate_dev_by_number: found dev: jbig-codec-odma-core-uio0, num = 0x7, ver=devicetree
UIO_LIB: uio_get_device_map: map for /sys/class/uio/uio7/maps/map0
UIO_LIB: num = 0
UIO_LIB: name = /jbig-codec-odma-core-uio0
UIO_LIB: phy_addr = 0xf9002800
UIO_LIB: size = 4096
UIO_LIB: Opened device jbig-codec-odma-core-uio0
dev_odma_core 0x4164c0 map: 0x416540, map->virt_addr 0xb7ff7800

codec 1
UIO_LIB: uio_locate_dev_by_number: found dev: jbig-codec-core-uio1, num = 0x8, ver=devicetree
```

```
UIO_LIB: uio_get_device_map: map for /sys/class/uio/uio8/maps/map0
UIO_LIB: num = 0
UIO_LIB: name = /jbig-codec-core-uio1
UIO_LIB: phy_addr = 0xf9008000
UIO_LIB: size = 4096
UIO_LIB: Opened device jbig-codec-core-uio1
UIO_LIB: uio_locate_dev_by_number: found dev: jbig-codec-idma-uio1, num = 0x9, ver=devicetree
UIO_LIB: uio_get_device_map: map for /sys/class/uio/uio9/maps/map0
UIO_LIB: num = 0
UIO_LIB: name = /jbig-codec-idma-uio1
UIO_LIB: phy_addr = 0xf9009000
UIO_LIB: size = 4096
UIO_LIB: Opened device jbig-codec-idma-uio1
UIO_LIB: uio_locate_dev_by_number: found dev: jbig-codec-odma-uio1, num = 0xa, ver=devicetree
UIO_LIB: uio_get_device_map: map for /sys/class/uio/uio10/maps/map0
UIO_LIB: num = 0
UIO_LIB: name = /jbig-codec-odma-uio1
UIO_LIB: phy_addr = 0xf900a000
UIO_LIB: size = 4096
UIO_LIB: Opened device jbig-codec-odma-uio1
UIO_LIB: uio_locate_dev_by_number: found dev: jbig-codec-odma-core-uio1, num = 0xb, ver=devicetree
UIO_LIB: uio_get_device_map: map for /sys/class/uio/uio11/maps/map0
UIO_LIB: num = 0
UIO_LIB: name = /jbig-codec-odma-core-uio1
UIO_LIB: phy_addr = 0xf900a800
UIO_LIB: size = 4096
UIO_LIB: Opened device jbig-codec-odma-core-uio1
dev_odma_core 0x416dc0 map: 0x416e10, map->virt_addr 0xb7ff0800

codec 2
UIO_LIB: uio_locate_dev_by_number: found dev: jbig-codec-core-uio2, num = 0xc, ver=devicetree
UIO_LIB: uio_get_device_map: map for /sys/class/uio/uio12/maps/map0
UIO_LIB: num = 0
UIO_LIB: name = /jbig-codec-core-uio2
UIO_LIB: phy_addr = 0xf9010000
UIO_LIB: size = 4096
UIO_LIB: Opened device jbig-codec-core-uio2
UIO_LIB: uio_locate_dev_by_number: found dev: jbig-codec-idma-uio2, num = 0xd, ver=devicetree
UIO_LIB: uio_get_device_map: map for /sys/class/uio/uio13/maps/map0
UIO_LIB: num = 0
UIO_LIB: name = /jbig-codec-idma-uio2
UIO_LIB: phy_addr = 0xf9011000
UIO_LIB: size = 4096
UIO_LIB: Opened device jbig-codec-idma-uio2
UIO_LIB: uio_locate_dev_by_number: found dev: jbig-codec-odma-uio2, num = 0xe, ver=devicetree
UIO_LIB: uio_get_device_map: map for /sys/class/uio/uio14/maps/map0
UIO_LIB: num = 0
UIO_LIB: name = /jbig-codec-odma-uio2
```

```
UIO_LIB: phy_addr = 0xf9012000
UIO_LIB: size = 4096
UIO_LIB: Opened device jbig-codec-odma-uio2
UIO_LIB: uio_locate_dev_by_number: found dev: jbig-codec-odma-core-uio2, num = 0xf, ver=devicetree
UIO_LIB: uio_gBad mode in Error handler detected, code 0xbf000002 -- SError
CPU: 0 PID: 351 Comm: jbigtest Tainted: G           O    4.2.8-yocto-standard #1
Hardware name: mv6220 TurnOn Card (DT)
task: ffffffc039c13f00 ti: ffffffc039e24000 task.ti: ffffffc039e24000
PC is at 0x7fb7e578f4
LR is at 0x7fb7e57a30
pc : [<0000007fb7e578f4>] lr : [<0000007fb7e57a30>] pstate: 80000000
sp : ffffffc039e27ff0
x29: 0000007ffffffb10 x28: 0000000000000000
x27: 0000000000000000 x26: 0000000000000000
x25: 0000000000000000 x24: 0000000000000000
x23: 0000000000000000 x22: 0000000000000000
x21: 0000000000000000 x20: 0000000000000000
x19: 0000000000403ea8 x18: 0000000000000000
x17: 0000007fb7e6e460 x16: 0000007fb7e578d0
x15: 00000000000057d8 x14: 0000007fb7e552f0
x13: 0000007fb7ffecb8 x12: 000000000000002d
x11: 0101010101010101 x10: 0000000000000000
x9 : 0000000000000004 x8 : 0000007fb7e8e680
x7 : 0000000000000000 x6 : 000000000000003f
x5 : 0000000000000040 x4 : 0000000000000000
x3 : 0000007fb7e8e540 x2 : 0000007fb7e8e540
x1 : 000000000000003f x0 : 0000007fb7ff8000

et_device_map: map for /sys/class/uio/uio15/maps/map0
UIO_LIB: num = 0
UIO_LIB: name = /jbig-codec-odma-core-uio2
UIO_LIB: phy_addr = 0xf9012800
UIO_LIB: size = 4096
UIO_LIB: Opened device jbig-codec-odma-core-uio2
dev_odma_core 0x416820 map: 0x416870, map->virt_addr 0xb7cf9800

codec 3
UIO_LIB: uio_locate_dev_by_number: found dev: jbig-codec-core-uio3, num = 0x10, ver=devicetree
UIO_LIB: uio_get_device_map: map for /sys/class/uio/uio16/maps/map0
UIO_LIB: num = 0
UIO_LIB: name = /jbig-codec-core-uio3
UIO_LIB: phy_addr = 0xf9018000
UIO_LIB: size = 4096
UIO_LIB: Opened device jbig-codec-core-uio3
UIO_LIB: uio_locate_dev_by_number: found dev: jbig-codec-idma-uio3, num = 0x11, ver=devicetree
UIO_LIB: uio_get_device_map: map for /sys/class/uio/uio17/maps/map0
UIO_LIB: num = 0
UIO_LIB: name = /jbig-codec-idma-uio3
UIO_LIB: phy_addr = 0xf9019000
UIO_LIB: size = 4096
```

```
UIO_LIB: Opened device jbig-codec-idma-uio3
UIO_LIB: uio_locate_dev_by_number: found dev: jbig-codec-odma-uio3, num = 0x12, ver=devicetree
UIO_LIB: uio_get_device_map: map for /sys/class/uio/uio18/maps/map0
UIO_LIB: num = 0
UIO_LIB: name = /jbig-codec-odma-uio3
UIO_LIB: phy_addr = 0xf901a000
UIO_LIB: size = 4096
UIO_LIB: Opened device jbig-codec-odma-uio3
UIO_LIB: uio_locate_dev_by_number: found dev: jbig-codec-odma-core-uio3, num = 0x13, ver=devicetree
UIO_LIB: uio_get_device_map: map for /sys/class/uio/uio19/maps/map0
UIO_LIB: num = 0
UIO_LIB: name = /jbig-codec-odma-core-uio3
UIO_LIB: phy_addr = 0xf901a800
UIO_LIB: size = 4096
UIO_LIB: Opened device jbig-codec-odma-core-uio3
dev_odma_core 0x4174b0 map: 0x4173c0, map->virt_addr 0xb7cf5800
Killing all inferiors
```

出现了如下trap

```
UIO_LIB: uio_gBad mode in Error handler detected, code 0xbf000002 -- SError
CPU: 0 PID: 351 Comm: jbigtest Tainted: G           O    4.2.8-yocto-standard #1
Hardware name: mv6220 TurnOn Card (DT)
task: ffffffc039c13f00 ti: ffffffc039e24000 task.ti: ffffffc039e24000
PC is at 0x7fb7e578f4
LR is at 0x7fb7e57a30
pc : [<0000007fb7e578f4>] lr : [<0000007fb7e57a30>] pstate: 80000000
sp : ffffffc039e27ff0
x29: 0000007ffffffb10 x28: 0000000000000000
x27: 0000000000000000 x26: 0000000000000000
x25: 0000000000000000 x24: 0000000000000000
x23: 0000000000000000 x22: 0000000000000000
x21: 0000000000000000 x20: 0000000000000000
x19: 0000000000403ea8 x18: 0000000000000000
x17: 0000007fb7e6e460 x16: 0000007fb7e578d0
x15: 00000000000057d8 x14: 0000007fb7e552f0
x13: 0000007fb7ffecb8 x12: 000000000000002d
x11: 0101010101010101 x10: 0000000000000000
x9 : 0000000000000004 x8 : 0000007fb7e8e680
x7 : 0000000000000000 x6 : 000000000000003f
x5 : 0000000000000040 x4 : 0000000000000000
x3 : 0000007fb7e8e540 x2 : 0000007fb7e8e540
x1 : 000000000000003f x0 : 0000007fb7ff8000
```

出错时的PC为

> PC is at 0x7fb7e578f4

查看jbig在gdb server控制下的memory map如下

```
root@granite2v8:~# cat /proc/351/maps
00400000-00405000 r-xp 00000000 b3:22 6205                               /home/root/jbigtest
00414000-00415000 rw-p 00004000 b3:22 6205                               /home/root/jbigtest
00415000-00416000 rw-p 00000000 00:00 0                                  [heap]
7fb7d0c000-7fb7e3c000 r-xp 00000000 b3:22 23                             /lib64/libc-2.21.so
7fb7e3c000-7fb7e4b000 ---p 00130000 b3:22 23                             /lib64/libc-2.21.so
7fb7e4b000-7fb7e4f000 r--p 0012f000 b3:22 23                             /lib64/libc-2.21.so
7fb7e4f000-7fb7e51000 rw-p 00133000 b3:22 23                             /lib64/libc-2.21.so
7fb7e51000-7fb7e55000 rw-p 00000000 00:00 0
7fb7e55000-7fb7e5e000 r-xp 00000000 b3:22 8034                           /usr/lib64/libjbig.so.1.0
7fb7e5e000-7fb7e6e000 ---p 00009000 b3:22 8034                           /usr/lib64/libjbig.so.1.0
7fb7e6e000-7fb7e6f000 rw-p 00009000 b3:22 8034                           /usr/lib64/libjbig.so.1.0
7fb7e6f000-7fb7e8f000 rw-p 00000000 00:00 0
7fb7e8f000-7fb7e9e000 r-xp 00000000 b3:22 3424                           /usr/lib64/libdmaalloc.so.1.0
7fb7e9e000-7fb7ead000 ---p 0000f000 b3:22 3424                           /usr/lib64/libdmaalloc.so.1.0
7fb7ead000-7fb7eaf000 rw-p 0000e000 b3:22 3424                           /usr/lib64/libdmaalloc.so.1.0
7fb7eaf000-7fb7eee000 rw-p 00000000 00:00 0
7fb7eee000-7fb7f7f000 r-xp 00000000 b3:22 86                             /lib64/libm-2.21.so
7fb7f7f000-7fb7f8f000 ---p 00091000 b3:22 86                             /lib64/libm-2.21.so
7fb7f8f000-7fb7f90000 r--p 00091000 b3:22 86                             /lib64/libm-2.21.so
7fb7f90000-7fb7f91000 rw-p 00092000 b3:22 86                             /lib64/libm-2.21.so
7fb7f91000-7fb7f97000 r-xp 00000000 b3:22 67                             /lib64/librt-2.21.so
7fb7f97000-7fb7fa6000 ---p 00006000 b3:22 67                             /lib64/librt-2.21.so
7fb7fa6000-7fb7fa7000 r--p 00005000 b3:22 67                             /lib64/librt-2.21.so
7fb7fa7000-7fb7fa8000 rw-p 00006000 b3:22 67                             /lib64/librt-2.21.so
7fb7fa8000-7fb7fbe000 r-xp 00000000 b3:22 90                             /lib64/libpthread-2.21.so
7fb7fbe000-7fb7fcd000 ---p 00016000 b3:22 90                             /lib64/libpthread-2.21.so
7fb7fcd000-7fb7fce000 r--p 00015000 b3:22 90                             /lib64/libpthread-2.21.so
7fb7fce000-7fb7fcf000 rw-p 00016000 b3:22 90                             /li
```

```
b64/libpthread-2.21.so
7fb7fcf000-7fb7fd3000 rw-p 00000000 00:00 0
7fb7fd3000-7fb7fef000 r-xp 00000000 b3:22 108                            /lib64/ld-2.21.so
7fb7ff4000-7fb7ff7000 rw-p 00000000 00:00 0
7fb7ffb000-7fb7ffc000 rw-p 00000000 00:00 0
7fb7ffc000-7fb7ffd000 r--p 00000000 00:00 0                              [vvar]
7fb7ffd000-7fb7ffe000 r-xp 00000000 00:00 0                              [vdso]
7fb7ffe000-7fb7fff000 r--p 0001b000 b3:22 108                            /lib64/ld-2.21.so
7fb7fff000-7fb8001000 rw-p 0001c000 b3:22 108                            /lib64/ld-2.21.so
7ffffdf000-8000000000 rw-p 00000000 00:00 0                              [stack]
root@granite2v8:~#
```

0x7fb7e578f4落在libjbig.so.1.0 code中

> 7fb7e55000-7fb7e5e000 r-xp 00000000 b3:22 8034 /usr/lib64/libjbig.so.1.0

0x7fb7e578f4 - 0x7fb7e55000 = 0x28f4 (offset)

确定libjbig.so.1.0　code的大致偏移

```
walterzh@walterzh-Precision-T1650:~/work/current/ccsgit/driver/jbig-codec/jbig-codec-app$ /home/walterzh/work/2016-05-LSP/64-bit/tmp/sysroots/x86_64-linux/usr/bin/aarch64-poky-linux/aarch64-poky-linux-readelf -l libjbig.so.1.0

Elf file type is DYN (Shared object file)
Entry point 0x2770
There are 5 program headers, starting at offset 64

Program Headers:
  Type           Offset             VirtAddr           PhysAddr
                 FileSiz            MemSiz              Flags  Align
  LOAD           0x0000000000000000 0x0000000000000000 0x0000000000000000
                 0x00000000000086bc 0x00000000000086bc  R E    10000
  LOAD           0x0000000000009000 0x0000000000019000 0x0000000000019000
                 0x0000000000000508 0x0000000000020b60  RW     10000
  DYNAMIC        0x0000000000009018 0x0000000000019018 0x0000000000019018
                 0x00000000000001f0 0x00000000000001f0  RW     8
  NOTE           0x0000000000000158 0x0000000000000158 0x0000000000000158
                 0x0000000000000024 0x0000000000000024  R      4
  GNU_STACK      0x0000000000000000 0x0000000000000000 0x0000000000000000
                 0x0000000000000000 0x0000000000000000  RW     10

 Section to Segment mapping:
  Segment Sections...
   00     .note.gnu.build-id .gnu.hash .dynsym .dynstr .gnu.version .gnu.version_r .rela.dyn .rela.plt .init .plt .text .fini .rodata .eh_frame
   01     .init_array .fini_array .jcr .dynamic .got .got.plt .data .bss
   02     .dynamic
   03     .note.gnu.build-id
   04
```

```
  LOAD           0x0000000000000000 0x0000000000000000 0x0000000000000000
                 0x00000000000086bc 0x00000000000086bc  R E    10000
```

即libjbig.so.1.0 载入内存后的偏移为0 - 0x86bc
地址为零是因为是动态载入，静态期无法确定address.

反汇编libjbig.so.1.0 code to locate the bug code

> /home/walterzh/work/2016-05-LSP/64-bit/tmp/sysroots/x86_64-linux/usr/bin/aarch64-poky-linux/aarch64-poky-linux-objdump -dS libjbig.so.1.0

```
libjbig.so.1.0:     file format elf64-littleaarch64


Disassembly of section .init:

0000000000002200 <_init>:
    .section .init,"ax",%progbits
    .align  2
    .global _init
    .type   _init, %function
_init:
    stp x29, x30, [sp, -16]!
    2200:   a9bf7bfd    stp x29, x30, [sp,#-16]!
    mov x29, sp
    2204:   910003fd    mov x29, sp
#if PREINIT_FUNCTION_WEAK
    bl  call_weak_fn
    2208:   9400015a    bl  2770 <call_weak_fn>

/* crtn.S puts function epilogues in the .init and .fini sections
   corresponding to the prologues in crti.S. */

    .section .init,"ax",%progbits
    ldp x29, x30, [sp], 16
    220c:   a8c17bfd    ldp x29, x30, [sp],#16
    RET
    2210:   d65f03c0    ret

Disassembly of section .plt:

0000000000002220 <memcpy@plt-0x20>:
    2220:   a9bf7bf0    stp x16, x30, [sp,#-16]!
    2224:   f00000b0    adrp    x16, 19000 <__frame_dummy_init_array_entry>
    2228:   f9413211    ldr x17, [x16,#608]
    222c:   91098210    add x16, x16, #0x260
    2230:   d61f0220    br  x17
    2234:   d503201f    nop
    2238:   d503201f    nop
    223c:   d503201f    nop

......

00000000000028d0 <jbig_block_init>:
 * @author  (10/13/2011)
 *
 * @param jbig_block_interface
 */
void jbig_block_init(const jbig_block_config_t* jbig_block_interface)
{
    28d0:   d10043ff    sub sp, sp, #0x10
    28d4:   f90007e0    str x0, [sp,#8]
    DBG_MEMLOG(LOG_INFO,"JBIG BLOCK INIT FROM POWER MANAGER!!!\n");
    //jbig_block_interface->jbig_regs->JCTL = 0;
```

```
54.     jbig_block_interface->jbig_idma_regs->int_cl = 0x1FF;
55.     28d8:   f94007e0    ldr x0, [sp,#8]
56.     28dc:   f9400800    ldr x0, [x0,#16]
57.     28e0:   52803fe1    mov w1, #0x1ff                  // #511
58.     28e4:   b9001401    str w1, [x0,#20]
59.     jbig_block_interface->jbig_odma_regs->UICR = JBIG_ODMA_UDMA_INT_ENABLE_M
    ASK;
60.     28e8:   f94007e0    ldr x0, [sp,#8]
61.     28ec:   f9400c00    ldr x0, [x0,#24]
62.     28f0:   528007e1    mov w1, #0x3f                   // #63
63.     28f4:   b9001401    str w1, [x0,#20]
```

找到出错指令 `28f4: b9001401 str w1, [x0,#20]`
也就是

> jbig_block_interface->jbig_odma_regs->UICR =
> JBIG_ODMA_UDMA_INT_ENABLE_MASK;
> 引起trap.

出错的原因：
**jbig block依赖与pegmatite regulator supply power，但pegmatite-regulator.ko没有载入，所以jbig block没有上电！**