# Modem crash分析

## 在线分析

* 使用jtag工具在线分析

主要使用trace32进行在线分析，详见高通参考文档说明。

* 使用QXDM log工具分析

## 静态分析

### Hexagon dsp cpu register

* LC0 [C1], SA0 [C0],LC1 [C3], SA1 [C2]: Loop registers
* PC [C9]: Program counter
* USR [C8]: User status register
* M0 [C6] M1 [C7]: Modifier registers (circular addressing)
* P3:0 [C4]: Predicate registers
* UGP [C10]: User General Pointer (TLS)
* GP [C11]: Global Pointer
* LR：返回地址

### 调用堆栈

● allocframe(size [u14])

– Push LR and FP to top of stack.

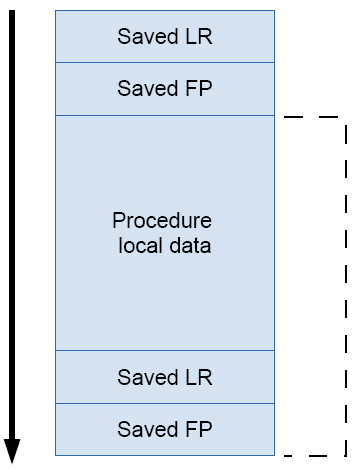
– Subtract size [8-byte aligned] from SP

– FP = addressof(oldFPonStack)

● deallocframe

– Load saved FP and LR values from address referenced at FP

– Restore SP to previous frame



### Dump分析

Dsp在进入异常状态后，会将cpu及栈的状态打印到内存中，一般上是ascii码格式。

我们平台的mem挂接在EBI1总线上。通过QPST dump出EBI1.BIN，实际上就是mem的内容。9x系列的各个core使用同一个mem，从其中可以找个各个core的数据。

使用UE 十六进制方式打开EBI1.BIN,在其中搜索crash，直到找到modem crash的信息如下：

分析过程：

1. 从（1）可以得出出错位置为fws\_task.c:246行
2. 从（2）LR为0x42275b5c可以得出返回指令位于err.c:2611

指令的位置在编译的时候已经确定，符号表中有明确的记录，使用如下指令得出指令位置对应的符号：

C:\Qualcomm\HEXAGON\_Tools\3.1.04\gnu\bin\

**qdsp6-addr2line –f –e elf镜像XXX 0x指令位置**

**也可以将objdump反汇编elf镜像。**

1. 从（3）PC为0x4198235c可以得出PC指向dsm.c:594
2. 观察栈的调用关系

根据2）提供的方法，确定栈的调用关系分析源代码

5）死机的同时保存QXDM log同时加上dump分析基本可以得出大部分crash的大致位置

**Error in file fws\_task.c, line 246 （1）**

**Error message: Firmware generated fatal error.**

Time of crash (m-d-y h:m:s): 09-01-2014 13:51:19

Uptime (h:m:s): 2:13:37

Build ID: M9615A-CETWTAZM-5.0.13059

REX\_TCB ptr: 0x45166e18

tcb.task\_name: IST 98

Coredump ARCH type is: ERR\_ARCH\_QDSP6

Register values from coredump:

QDSP6\_GP\_R0 : 0x00000000

QDSP6\_GP\_R1 : 0x4530df20

QDSP6\_GP\_R2 : 0x00000000

QDSP6\_GP\_R3 : 0x4507fb48

QDSP6\_GP\_R4 : 0x000000fe

QDSP6\_GP\_R5 : 0xd1718820

QDSP6\_GP\_R6 : 0x00000000

QDSP6\_GP\_R7 : 0x00000001

QDSP6\_GP\_R8 : 0xe353f7cf

QDSP6\_GP\_R9 : 0x20c49ba5

QDSP6\_GP\_R10 : 0xffdf7b00

QDSP6\_GP\_R11 : 0x00000000

QDSP6\_GP\_R12 : 0xffdf7b00

QDSP6\_GP\_R13 : 0x0004afff

QDSP6\_GP\_R14 : 0x447f8dbf

QDSP6\_GP\_R15 : 0xbbd872ca

QDSP6\_GP\_R16 : 0x43347c94

QDSP6\_GP\_R17 : 0x00000000

QDSP6\_GP\_R18 : 0x00000000

QDSP6\_GP\_R19 : 0x00000000

QDSP6\_GP\_R20 : 0x422b2110

QDSP6\_GP\_R21 : 0x00000000

QDSP6\_GP\_R22 : 0x00000000

QDSP6\_GP\_R23 : 0x00000000

QDSP6\_GP\_R24 : 0x00000000

QDSP6\_GP\_R25 : 0x00000000

QDSP6\_GP\_R26 : 0x00000000

QDSP6\_GP\_R27 : 0x00000000

QDSP6\_GP\_R28 : 0x00000000

QDSP6\_SP : 0x451676f8

QDSP6\_FP : 0x45167700

**QDSP6\_LR : 0x42275b5c err.c:2611 （2）**

**QDSP6\_PC : 0x4198235c dsm.c:594 （3）**

QDSP6\_USR : 0x00000000

QDSP6\_UGP : 0x00000000

QDSP6\_GP : 0x00000000

QDSP6\_LC0 : 0x00000000

QDSP6\_LC1 : 0x00000000

QDSP6\_SA0 : 0x00000000

QDSP6\_SA1 : 0x00000000

QDSP6\_M0 : 0x00000000

QDSP6\_M1 : 0x00000000

QDSP6\_P : 0x00000000

QDSP6\_SGP : 0x00000000

QDSP6\_SSR : 0x00000000

QDSP6\_IMASK : 0x00000000

QDSP6\_BADVA : 0x00000000

QDSP6\_ELR : 0x00000000

QDSP6\_TID : 0x00000000

QDSP6\_EVB : 0x00000000

QDSP6\_IPEND : 0x00000000

QDSP6\_SYSCFG : 0x00000000

QDSP6\_MODECTL : 0x00000000

QDSP6\_REV : 0x00000000

QDSP6\_TLBHI : 0x00000000

QDSP6\_TLBLO : 0x00000000

QDSP6\_TLBIDX : 0x00000000

QDSP6\_DIAG : 0x00000000

QDSP6\_IAD : 0x00000000

QDSP6\_IEL : 0x00000000

QDSP6\_IAHL : 0x00000000

QDSP6\_PCYCLEHI : 0x00000000

QDSP6\_PCYCLELO : 0x00000000

Stack Dump (from 0x451676f8):

Addr Data

0x451676f8 0x00000f50

0x451676fc 0x43d945ac

0x45167700 0x4333cb74

0x45167704 0x43d945b8

0x45167708 0x45167718

**0x4516770c 0x42275a18 err.c:989**

0x45167710 0x0000000f

0x45167714 0x43d945b8

0x45167718 0x45167760

**0x4516771c 0x422b21b0 gl1\_hw.c:2918**

0x45167720 0x0409020a

0x45167724 0x00000029

0x45167728 0x00000001

0x4516772c 0x00000004

0x45167730 0x0000000a

0x45167734 0x00000000

0x45167738 0x00000000

0x4516773c 0x00000000

0x45167740 0x00000000

0x45167744 0x00010484

0x45167748 0x11fc029f

0x4516774c 0x00000008

0x45167750 0x40780061

0x45167754 0x40780179

0x45167758 0x00000062

0x4516775c 0x43d945b8

0x45167760 0x45167788

**0x45167764 0x427b55a4 trees.c:467**

0x45167768 0x000014a0

0x4516776c 0x00000000

0x45167770 0x00000000

0x45167774 0x00000000

0x45167778 0x4437f528

0x4516777c 0x45167794

0x45167780 0x00000062

0x45167784 0x0000001f

0x45167788 0x451677a8

**0x4516778c 0x428be4f4 tramp\_qub3\_bsp.c:296**

0x45167790 0x45167798

0x45167794 0x0000001f

0x45167798 0x451677b4

0x4516779c 0x00000000

0x451677a0 0x45166e18

0x451677a4 0x45167838

0x451677a8 0x451677f0

**0x451677ac 0x42519364 rex\_qube.c:693**

0x451677b0 0x002001c1

0x451677b4 0x45167028

0x451677b8 0x00000000

0x451677bc 0x00000800

0x451677c0 0x00000014

0x451677c4 0x00000000

0x451677c8 0x000000ff

0x451677cc 0x20545349

0x451677d0 0x75003839

0x451677d4 0x44800073

0x451677d8 0x0000009d

0x451677dc 0x711f889b

0x451677e0 0x00000000

0x451677e4 0x00000000

0x451677e8 0x45167868

0x451677ec 0x00000000

0x451677f0 0x45167810

**0x451677f4 0x4250a464 ccGUgMuv.s:722**

0x451677f8 0x00000000

0x451677fc 0x00000000

0x45167800 0x20545349

0x45167804 0x00003839

0x45167808 0x4507fb48

0x4516780c 0x00000000

0x45167810 0x45167820

**0x45167814 0x421c78e4 blast\_thread.c:192**

0x45167818 0x00000000

0x4516781c 0x00000000

0x45167820 0x00000000

0x45167824 0x00000000

Dog Report Information (dog\_state\_table)

[idx] Task Name Pri Timeout Count Is\_Blocked

[ 0] time\_ipc 0 60 59 0

[ 1] diag 0 60 60 0

[ 2] tmr\_slave1 0 60 60 0

[ 3] tmr\_slave2 0 60 60 0

[ 4] tmr\_slave3 0 60 60 0

[ 5] modem\_cfg 0 60 56 0

[ 6] locotdoactr 0 60 59 0

[ 7] sm\_gm 0 60 56 0

[ 8] gnss\_msgr 0 60 59 0

[ 9] locotdoamp 0 60 59 0

[ 10] startup\_app 0 60 59 0

[ 11] DSMSGR RECV 0 60 59 0

[ 12] cm 0 60 60 0

[ 13] mmoc 0 60 55 0

[ 14] hdrmc 0 60 56 0

[ 15] hdrtx 0 60 55 0

[ 16] hdrrx 0 60 55 0

[ 17] hdrdec 0 60 55 0

[ 18] hitapp 0 60 55 0

[ 19] xtm 0 60 56 1

[ 20] gstk 0 60 57 0

[ 21] gsm\_l2 0 60 55 0

[ 22] gprs\_rlc\_ul 0 60 59 0

[ 23] gprs\_rlc\_dl 0 60 59 0

[ 24] gprs\_llc 0 60 55 0

[ 25] mm 0 60 57 0

[ 26] reg 0 60 56 0

[ 27] mn\_cnm 0 60 55 0

[ 28] sm 0 60 55 0

[ 29] cb 0 60 56 0

[ 30] tds\_l1 0 60 55 0

[ 31] tds\_mac\_hs\_ 0 60 55 0

[ 32] tds\_l2\_ul 0 60 59 0

[ 33] tds\_l2\_dl 0 60 59 0

[ 34] tc 0 60 55 0

[ 35] ps 0 60 60 0

[ 36] qmi\_modem 0 60 56 0

[ 37] dcc 0 60 60 0

[ 38] ds\_sig 0 60 56 0

[ 39] ps\_rm 0 60 59 0

[ 40] ds 0 60 60 0

[ 41] comp 0 60 59 0

[ 42] dswcsd\_ul 0 60 59 0

[ 43] dswcsd\_dl 0 60 59 0

[ 44] sm\_tm 0 60 59 0

[ 45] pdcommtcp 0 60 55 0

[ 46] pdcommwms 0 60 55 0

[ 47] loc\_middlew 0 60 55 0

[ 48] rf 0 60 60 0

[ 49] ims 0 60 56 0

[ 50] ims\_cb 0 60 56 0

[ 51] cxm 0 60 60 0

[ 52] qvp\_rtp 0 60 56 0

[ 53] qmi\_mmode 0 60 60 0

[ 54] qmi\_pbm 0 60 56 0

[ 55] ecall\_app 0 60 59 0

[ 56] ecall\_ivs 0 60 59 0

[ 57] tdso 0 60 59 0

[ 58] uim 0 60 56 0

[ 59] a2 0 60 55 0

[ 60] a2\_ul\_per 0 60 55 0

[ 61] mc 0 60 60 0

[ 62] tx 0 60 55 0

[ 63] rx 0 60 55 0

[ 64] srch 0 60 55 0

[ 65] rxtx 0 2 2 0

[ 66] hdrsrch 0 60 55 0

[ 67] auth 0 60 55 0

[ 68] dh 0 60 56 0

[ 69] wcdma\_l1 0 60 59 0

[ 70] wcdma\_l2\_ul 0 60 59 0

[ 71] wcdma\_l2\_dl 0 60 59 0

[ 72] wcdma\_mac\_h 0 60 55 0

[ 73] gprs\_mac 0 60 55 0

[ 74] rr 0 60 55 0

[ 75] pp 0 60 55 0

[ 76] lm 0 60 55 0

[ 77] gpsfft 0 60 55 0

[ 78] gnss\_sdp 0 60 55 0

[ 79] cc 0 60 56 0

[ 80] tds\_rrc 0 60 56 0

[ 81] LTE MAC UL 0 60 56 0

[ 82] tlm 0 60 54 1

[ 83] LTE MAC DL 0 60 56 0

[ 84] LTE RLC UL 0 60 56 0

[ 85] LTE MAC CTR 0 60 56 0

[ 86] LTE RLCDL 0 60 56 0

[ 87] LTE PDCP DL 0 60 56 0

[ 88] LTE PDCP UL 0 60 56 0

[ 89] gsdi 0 60 55 0

[ 90] nf 0 60 56 0

[ 91] pgi 0 60 56 0

[ 92] rrc 0 60 56 0

[ 93] mgpmc 0 60 60 0

[ 94] cd 0 60 56 0

[ 95] 0 0 -8011 0

[ 96] 0 0 -8011 0

[ 97] 0 0 -8011 0

[ 98] 0 0 -8011 0

[ 99] 0 0 -8011 0

[100] 0 0 -8011 0

[101] 0 0 -8011 0

[102] 0 0 -8011 0

[103] 0 0 -8011 0

[104] 0 0 -8011 0

[105] 0 0 -8011 0

[106] 0 0 -8011 0

[107] 0 0 -8011 0

[108] 0 0 -8011 0

[109] 0 0 -8011 0

[110] 0 0 -8011 0

[111] 0 0 -8011 0

[112] 0 0 -8011 0

[113] 0 0 -8011 0

[114] 0 0 -8011 0

[115] 0 0 -8011 0

[116] 0 0 -8011 0

[117] 0 0 -8011 0

[118] 0 0 -8011 0

[119] 0 0 -8011 0

[120] 0 0 -8011 0

[121] 0 0 -8011 0

[122] 0 0 -8011 0

[123] 0 0 -8011 0

[124] 0 0 -8011 0

[125] 0 0 -8011 0

[126] 0 0 -8011 0

[127] 0 0 -8011 0

[128] 0 0 -8011 0

[129] 0 0 -8011 0

[130] 0 0 -8011 0

[131] 0 0 -8011 0

[132] 0 0 -8011 0

[133] 0 0 -8011 0

[134] 0 0 -8011 0

[135] 0 0 -8011 0

[136] 0 0 -8011 0

[137] 0 0 -8011 0

[138] 0 0 -8011 0

[139] 0 0 -8011 0

[140] 0 0 -8011 0

[141] 0 0 -8011 0

[142] 0 0 -8011 0

[143] 0 0 -8011 0

[144] 0 0 -8011 0

[145] 0 0 -8011 0

[146] 0 0 -8011 0

[147] 0 0 -8011 0

[148] 0 0 -8011 0

[149] 0 0 -8011 0

[150] 0 0 -8011 0

[151] 0 0 -8011 0

[152] 0 0 -8011 0

[153] 0 0 -8011 0

[154] 0 0 -8011 0

[155] 0 0 -8011 0

[156] 0 0 -8011 0

[157] 0 0 -8011 0

[158] 0 0 -8011 0

[159] 0 0 -8011 0

[160] 0 0 -8011 0

[161] 0 0 -8011 0

[162] 0 0 -8011 0

[163] 0 0 -8011 0

[164] 0 0 -8011 0

[165] 0 0 -8011 0

[166] 0 0 -8011 0

[167] 0 0 -8011 0

[168] 0 0 -8011 0

[169] 0 0 -8011 0

[170] 0 0 -8011 0

[171] 0 0 -8011 0

[172] 0 0 -8011 0

[173] 0 0 -8011 0

[174] 0 0 -8011 0

[175] 0 0 -8011 0

[176] 0 0 -8011 0

[177] 0 0 -8011 0

[178] 0 0 -8011 0

[179] 0 0 -8011 0

[180] 0 0 -8011 0

[181] 0 0 -8011 0

[182] 0 0 -8011 0

[183] 0 0 -8011 0

[184] 0 0 -8011 0

[185] 0 0 -8011 0

[186] 0 0 -8011 0

[187] 0 0 -8011 0

[188] 0 0 -8011 0

[189] 0 0 -8011 0

[190] 0 0 -8011 0

[191] 0 0 -8011 0

[192] 0 0 -8011 0

[193] 0 0 -8011 0

[194] 0 0 -8011 0

[195] 0 0 -8011 0

[196] 0 0 -8011 0

[197] 0 0 -8011 0

[198] 0 0 -8011 0

[199] 0 0 -8011 0

End Dog Report

End of crash log report.

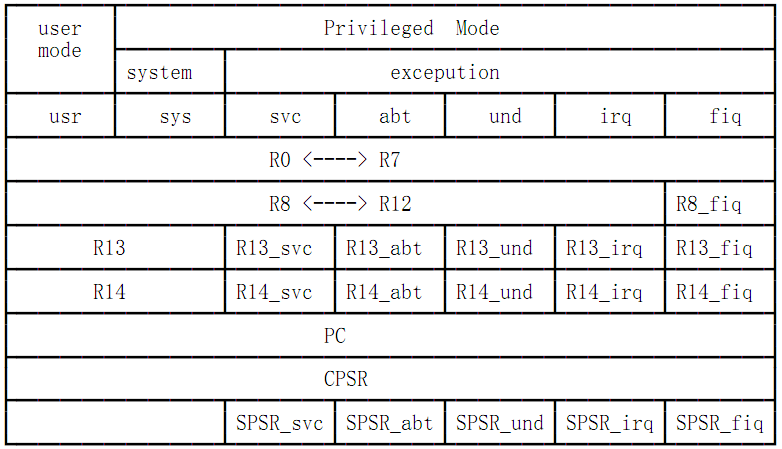
# Linux crash分析

## 在线分析

* 使用kgdb在线分析
* 使用log输出在线分析如printk

## 静态分析

### Cpu寄存器模型



勘误：R8\_fiq应为R8\_fiq~R12\_fiq

37个寄存器，31个通用寄存器，6个状态寄存器，R13堆栈指针sp，R14返回指针，R15为PC指针

### Dump分析

Dump分析方法同modem dump分析方法

# 注意事项

由于dump分析依赖elf镜像，在版本中必须将modem符号表，linux符号表加入其中，以便现场分析。