

通过 addr2line 分析 ZigBee JN516x 的 crash stack dump

(shaozhong.liang)

addr2line 是什么

addr2line（它是标准的 [GNU Binutils](#) 中的一部分）是一个可以将指令的地址和可执行映像转换成文件名、函数名和源代码行数的工具。

如何获得 addr2line

Linux 系统一般会集成这个工具，本文重点介绍 Windows 系统下如何获取该工具。方法很多，我这里仅介绍两种方式

- 第一种：安装 MinGW（网上教程很多，自行搜索），安装后在其安装目录的 bin 文件夹里会包含 addr2line.exe，此时只用保证环境变量 path 中包含该路径即可；
- 第二种（XP 平台除外）：在本项目的 tools 文件夹中已存放 addr2line.exe，可以将其直接拷贝至 C:\Windows 下，或者将 CmBacktrace 仓库的 tools 文件夹路径添加至到环境变量 path 中，这样都能保证命令行工具能正常使用 addr2line 命令。

addr2line 如何使用

使用 addr2line --help 可以看到如下介绍：

```
$addr2line --help
Usage: addr2line [option(s)] [addr(s)]
Convert addresses into line number/file name pairs.
If no addresses are specified on the command line, they will be read from stdin
The options are:
@<file>          Read options from <file>
-a --addresses    Show addresses
-b --target=<bfdname> Set the binary file format
-e --exe=<executable> Set the input file name (default is a.out)
-i --inlines      Unwind inlined functions
-j --section=<name> Read section-relative offsets instead of addresses
-p --pretty-print  Make the output easier to read for humans
-s --basenames    Strip directory names
-f --functions    Show function names
-C --demangle[=style] Demangle function names
-h --help         Display this information
-v --version      Display the program's version
```

addr2line: supported targets: pe-x86-64 pei-x86-64 pe-bigobj-x86-64 elf64-x86-64
elf64-l1om elf64-k1om pe-i386 pei-i386 elf32-i386 elf64-little elf64-big elf32-
little elf32-big plugin srec symbolsrec verilog tekhex binary ihex
Report bugs to <http://www.sourceware.org/bugzilla/>

这里常用的是以下参数

- -e : 指定可执行映像名称
- -a : 显示函数地址
- -f : 显示函数名称

例如命令 `addr2line -e CmBacktrace.elf -f 08000a60 08000141 0800313f` 将会显示名称为 `CmBacktrace.elf` 的可执行映像, 在地址为 `08000a60 08000141 0800313f` 对应的函数名称及源代码信息。执行结果如下:

```
$addr2line -e CmBacktrace.elf -a -f 08000a60 08000141 0800313f
fault_test_by_div0
D:\Program\CmBacktrace\demo\non_os\app\src\fault_test.c:38 main
D:\Program\CmBacktrace\demo\non_os\app\src\app.c:20 _call_main ????
```

通过 `addr2line` 分析 ZigBee JN516x 的 crash stack dump

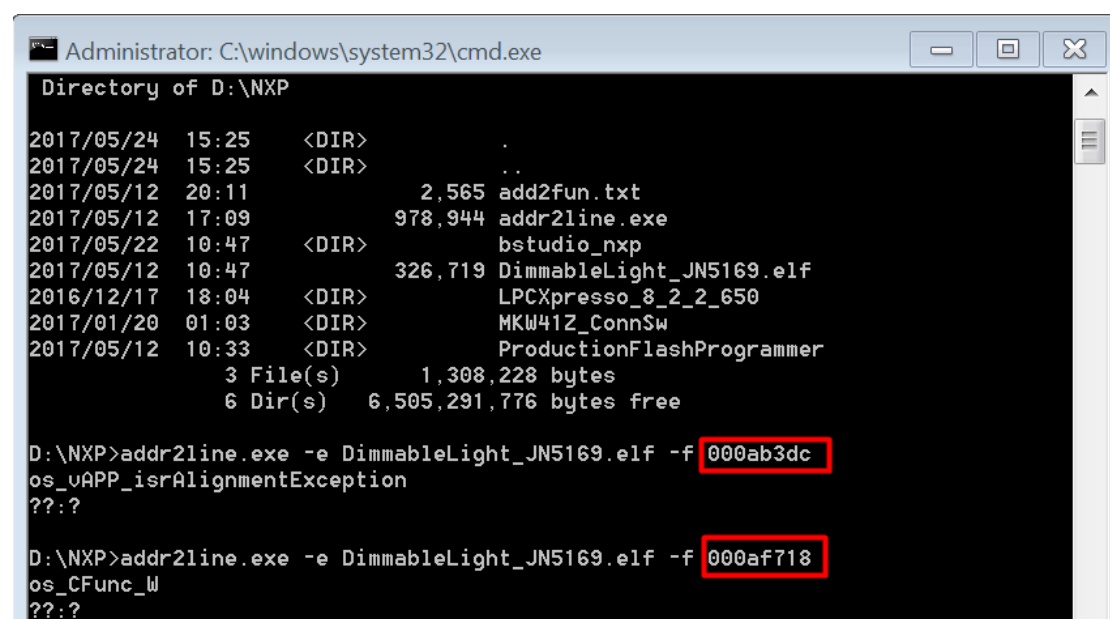
当 JN516x crash 后, 将在串口打印输出调用栈信息, 通过这些信息可以分析定位出现问题的函数。

APP: Light Power Up

EPCR = a9a2d : EEAR = 7

Stack dump:

```
4007ec0 : ffffffff
4007ec4 : 000ab3dc
4007ec8 : 00000000
4007ecc : 000af718
4007ed0 : 0000fffe
4007ed4 : 0000000c
4007ed8 : 000ab3d6
4007edc : 04000960
4007ee0 : 00000000
4007ee4 : ffffffff
```



```
Administrator: C:\windows\system32\cmd.exe
Directory of D:\NXP

2017/05/24  15:25    <DIR>          .
2017/05/24  15:25    <DIR>          ..
2017/05/12  20:11                2,565 add2fun.txt
2017/05/12  17:09           978,944 addr2line.exe
2017/05/22  10:47    <DIR>          bstudio_nxp
2017/05/12  10:47           326,719 DimmableLight_JN5169.elf
2016/12/17  18:04    <DIR>          LPCXpresso_8_2_2_650
2017/01/20  01:03    <DIR>          MKW41Z_ConnSw
2017/05/12  10:33    <DIR>          ProductionFlashProgrammer
               3 File(s)          1,308,228 bytes
               6 Dir(s)      6,505,291,776 bytes free

D:\NXP>addr2line.exe -e DimmableLight_JN5169.elf -f 000ab3dc
os_vAPP_isrAlignmentException
???:?

D:\NXP>addr2line.exe -e DimmableLight_JN5169.elf -f 000af718
os_CFunc_W
???:?
```