

Diagnosing Native Crashes

tcrash-utility guide

ajinathkumbhar@gmail.com



1. Setup tcrash-utility workspace

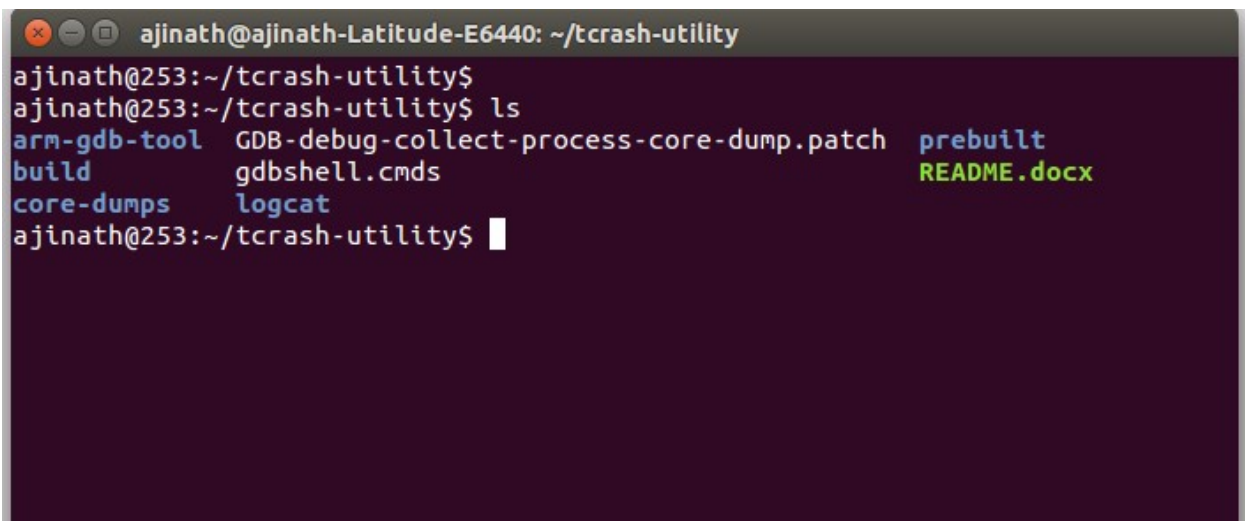
First copy the tcrash-utility tool in to local desktop with below steps.

Using git clone

2. Debug native crash with core dump file

Go to tcrash-utility

```
$ cd tcrash-utility
```



A terminal window titled 'ajinath@ajinath-Latitude-E6440: ~/tcrash-utility' shows the output of the 'ls' command. The directory contains files: 'arm-gdb-tool', 'build', 'core-dumps', 'GDB-debug-collect-process-core-dump.patch', 'gdbshell.cmds', 'logcat', 'prebuilt', and 'README.docx'.

```
ajinath@253:~/tcrash-utility$ ls
arm-gdb-tool  GDB-debug-collect-process-core-dump.patch  prebuilt
build         gdbshell.cmds                             README.docx
core-dumps   logcat
```

```
$ source build/envsetup.sh
```

We need three things

- Process name which one is crashed** (For process name check 'adb logcat' with DEBUG tag)
- Symbols** (Check build directory e.g. out/target/product/xxxx/symbols)
- Core dump of crashed process.** (ref. Document section 4 of **SIPL-AFW-01A** to collect core dump [Debug-process-crash-with-gdb.pdf])

Now run below command with arguments as process name and symbol path

```
$ crash-from-coredump.sh /system/bin/mm-qcamera-daemon
./distout/out/target/product/xxxx/symbols
```

```
$ Are you sure? [y/N]: y
```

Now gdb terminal started. Run below gdb command to load core dump file

```
(gdb) core-file /home/ajinath/distout/!system!bin!mm-qcamera-daemon.639.CAM_MctServ
```

gdb will load all required symbols. Now we can use gdb commands to debug crash e.g

(gdb) backtrace

```
(gdb) backtrace
#0  tgkill () at bionic/libc/arch-arm/syscalls/tgkill.S:10
#1  0xe9252516 in pthread_kill (t=<optimized out>, sig=6) at bionic/libc/bionic/pthread_kill.cpp:4
#2  0xe9228768 in raise (sig=7039) at bionic/libc/bionic/raise.cpp:34
#3  0xe92242ce in __libc_android_abort () at bionic/libc/bionic/abort.cpp:57
#4  0xe922230c in abort () at bionic/libc/arch-arm/bionic/abort_arm.S:43
#5  0xe854a1fc in __android_log_assert (cond=<optimized out>, tag=0xeb21157a "Ajinath", fmt=<optim
at system/core/liblog/logger_write.c:489
#6  0xeb20fd44 in s5k5e8_fill_exposure_array (gain=<optimized out>, digital_gain=<optimized out>,
fl_lines=<optimized out>, luma_avg=<optimized out>, hdr_param=<optimized out>, reg_setting=<op
at vendor/qcom/proprietary/mm-camera/mm-camera2/media-controller/modules/sensors/../../../../mm
ensor/libs/s5k5e8/s5k5e8_lib.c:199
```

3. Debug native crash with logcat file

We need two things

- Symbols** (Check build directory e.g. out/target/product/xxxx/symbols)
- Logcat of process crash** (adb logcat > logcat.txt).

Now run below command with arguments as process name and symbol path

```
$ crash-from-log.sh ../distout/out/target/product/xxxx/symbols/ ../distout/logcat.txt
```

```
ajinath@253:~/tcrash-utility$ crash-from-log.sh ../distout/out/target/product/r1mo02a/symbols/ ../distout/logcat.txt
found vendor lib
***** Crash dump: *****
Build fingerprint: 'Smartron/srtpphone/r1mo02a:7.1.1/NMF26F/akumbh05251013:userdebug/release-keys'
pid: 639, tid: 7039, name: CAM_MctServ >>> /system/bin/mm-qcamera-daemon <<<
signal 6 (SIGABRT), code -6 (SI_TKILL), fault addr 0x00000000
Stack frame #00 pc 00049d98 /system/lib/libc.so (tgkill+12)
Stack frame #01 pc 00047513 /system/lib/libc.so (pthread_kill+34)
Stack frame #02 pc 0001d765 /system/lib/libc.so (raise+10)
Stack frame #03 pc 000192a1 /system/lib/libc.so (__libc_android_abort+34)
Stack frame #04 pc 00017308 /system/lib/libc.so (abort+4)
Stack frame #05 pc 0000c1f9 /system/lib/libcutils.so (__android_log_assert+112)
Stack frame #06 pc 00000d41 /system/vendor/lib/libmmcamera_s5k5e8.so (s5k5e8_fill_exposure_array+472): Routine s5k5e8_fill_exposure_array at /proc/self/cwd/vendor/qcom/proprietary/mm-camera/mm-camera2/media-controller/modules/sensors/../../../../mm-camera2/media-controller/modules/sensors/sensor/libs/s5k5e8/s5k5e8_lib.c:199
Stack frame #07 pc 00021c15 /system/vendor/lib/libmmcamera2_sensor_modules.so: Routine sensor_apply_exposure at vendor/qcom/proprietary/mm-camera/mm-camera2/media-controller/modules/sensors/sensor/module/sensor.c:478
```

In output we will get exact routine name and line number where crash triggered.