
Linux Android Stability Issue Analysis



Qualcomm Technologies, Inc.

80-P7139-1 A

Confidential and Proprietary – Qualcomm Technologies, Inc.

Restricted Distribution: Not to be distributed to anyone who is not an employee of either Qualcomm Technologies, Inc. or its affiliated companies without the express approval of Qualcomm Configuration Management.



Confidential and Proprietary – Qualcomm Technologies, Inc.

QUALCOMM
2017-08-07 18:30:03 PDT
lilubao@gionee.com

NO PUBLIC DISCLOSURE PERMITTED: Please report postings of this document on public servers or websites to: DocCtrlAgent@qualcomm.com.

Not to be used, copied, reproduced, or modified in whole or in part, nor its contents revealed in any manner to others without the express written permission of Qualcomm Technologies, Inc.

Qualcomm is a trademark of Qualcomm Incorporated, registered in the United States and other countries. Other product and brand names may be trademarks or registered trademarks of their respective owners.

This technical data may be subject to U.S. and international export, re-export, or transfer (“export”) laws. Diversion contrary to U.S. and international law is strictly prohibited.

Qualcomm Technologies, Inc.
5775 Morehouse Drive
San Diego, CA 92121
U.S.A.

© 2016 Qualcomm Technologies, Inc. and/or its affiliated companies. All rights reserved.

Revision History

Revision	Date	Description
A	July 2016	Initial release

QUALCOMM
2017-08-07 18:30:03 PDT
lilubao@gionee.com

Contents

- Introduction
- Getting Full Crash Dump
- Parser Tool
- QCAP Environment Setup
- QCAP Interface
- QCAP Log Example
- Stability Issue Classification
- How to Raise a Stability Case
- Tracking Stability Issues Effectively
- References
- Questions?

Introduction

This document provides a summary about analysis of Android crash issues on Qualcomm platforms, and is meant for engineers who work on such issues.

QUALCOMM
2017-08-07 18:30:03 PDT
lilubao@gionee.com

Getting Full Crash Dump

- Theory
 - Kernel
 - msm-poweroff.c (msm-restart.c)
 - MSM_DLOAD_MODE
 - scm_set_dload_mode
 - SBL
 - WARM reset
 - [msm_restart_prepare](#)
- Hang issue
 - Long press power key to trigger dump
 - pull_down PS_HOLD in 200ms
 - Solution 00031242 How to collect log for a phone hang/screen freeze issue
 - For example, MSM8994:
 - kernel/arch/arm64/boot/dts/qcom/msm-pm8994.dtsi

```
qcom,pon_1 {
    qcom,pon-type = <0>;
    qcom,pull-up = <1>;
    linux,code = <116>;
    qcom,support-reset = <1>;
    qcom,s1-timer = <10256>;
    qcom,s2-timer = <2000>;
    qcom,s2-type = <1>;
};
qcom,pon_3 {
```

Parser Tool

- QCAP
 - Qualcomm web based parser tool (cap.qit.qualcomm.com)
 - Solution 00031425 -- How to use QCAP to parse a dump and raise a stability case correctly
- Ram parser
 - Qualcomm developed tools, parse Linux side dump, provide more information from kernel
 - Solution 00027972 -- How to use Linux Ramdump Parser (ramparse.py) to extract Linux Android logs
- Trace32 simulator
 - Used to perform dump analysis, check kernel structure, disassemble code, memory content
- Redhat Crash
 - Open source tools maintained by Redhat; provides similar features as the Trace32 simulator
 - Command line tools; could use remotely

QCAP Environment Setup

1. Internet Explorer; install latest Java (<http://java.com/en/download/>) 。
2. Restart Internet Explorer
3. QCAP : <https://cap.qti.qualcomm.com>。
4. Browser will prompt for running app


References:

- QCAP training video:
<https://virtuallearning.qualcomm.com/p7ssobajxig/>

QCAP documents:

- 80-NR964-54 QCAP_Start_Up_Guide
- 80-NR964-54SC QCAP_Start_Up_Guide (Chinese)
- VD80-NR964-54C QCAP Start-Up Training Video/Chinese



QCAP Interface

 **QUALCOMM® CRASH ANALYSIS PORTAL**

[START NEW ANALYSIS](#)

Welcome yaoli | [License](#) | [Feedback](#) | [Help](#) | [Log Out](#)

ANALYSIS QUEUE

Request	Progress	
<div>2016-05-16 10:14:27</div> <div>Product: MSM8996.LA.1.1</div>	<div></div> <div>Ready</div>	<div>Elapsed time: 00:05:54</div> <div> </div>
<div>Id: be233b86-91a4-4274-a16f-bf28ea5e128f</div> <div>Chipset: MSM8996</div> <div>Software Product: MSM8996.LA.1.1</div> <div>Log Location: C:\D\...pcie_8151_debugging\Port_COM23</div> <div>Build Location: C:\D\...pcie_8151_debugging\Port_COM23</div>		

QCAP Log Example

APPS

Core Summary

DMesg

Main Log

Radio Log

System Log

- RTB

msm rtb0

msm rtb1

msm rtb2

msm rtb3

- IPC

glink

smd

smsm

smem

pcie0-short

Core Summary

Build Info:

Version: Linux version 3.18.20-gfc9e53e-dirty () (gcc version 4.!

Built on: Fri May 13 17:45:28 CST 2016

Watchdog Context:

CPU	World	Received WDT Int?	Received SGI Int?	In Warm Boot?
0	non-secure world	no	yes	no
1	non-secure world	no	yes	no
2	non-secure world	no	no	no
3	non-secure world	no	yes	no

CPU 0 Call Stacks (dumped by TZ):

-000 run_timer_softirq()

-001 do_softirq()

-002 irq_exit()

-003 handle_domain_irq()

-004 gic_handle_irq()

-005 eli_irq()

-006 cpu_do_idle()

-007 arch_cpu_idle()

-008 cpu_startup_entry()

---- end of frame

CPUERRSR_EL1: 0x0

L2MERRSR_EL1: 0x0

Stability Issue Classification

- Panic
 - Bug_on
 - Null pointer
 - Invalid instruction
- Non secure dog bark
- Non secure dog bite
- Secure dog bite
 - Secure dog bark is used to kick dog
- Freeze/hang
 - Adb login ok
 - USB port enumerate
 - No USB port
- Subsystem crash

How to Raise a Stability Case

Go to <https://createpoint.qti.qualcomm.com> and click Cases

- Description
 - How did it happen? Scenario
 - Could be reproduced?
 - Only on specific phone or phones?
- Initial parser
 - QCAP and ram parser result
- Initial analysis
 - Extract key information
- Raise a clear case title
 - Behavior, Position, Step, and Other Info is useful

This helps to quickly find the relationship between different crashes from the same OEM and similar issues from different OEMs

- **Behaviour:** BugON|Data abort|Null Point|Prefetch abort|dog bark|NS Dogbite|S Dogbite|Hang|L1 cache error|XPU|NOC
- **Position:** C function name|C file name|process name|CPU No
- **Step:** monkey |aging test|standby|resume|reboot test|daily use|market return|camera|play video
- **Other info:** Only 1 phone, 1 time, Random, 100% reproduce, 3 in 10 times, 24 hours, e.g.

Null point in msm_poweroff.c+121 |msm_restart_prepare() in reboot test of 24 hours

Tracking Stability Issues Effectively

To effectively track one-time issues or hard to reproduce issues:

1. Record useful information
 - Build ID
 - Chip/device id/IMEI
 - Case number
 - Test step
 - Crash signature
2. Keep dump/elf symbols
 - Modify your build script to keep each build symbol file

References

Title	Number
Qualcomm Technologies, Inc.	
QCAP_Start_Up_Guide	80-NR964-54N
QCAP_Start_Up_Guide (Chinese)	80-NR964-54SC
QCAP Start-Up Training Video/Chinese	VD80-NR964-54C

Acronym or term	Definition
QCAP	Qualcomm Crash Analysis Portal
SBL	Secondary Boot Loader

QUALCOMM®
2017-08-07 18:30:03 PDT
lilubao@gionee.com

Questions?

<https://createpoint.qti.qualcomm.com>

