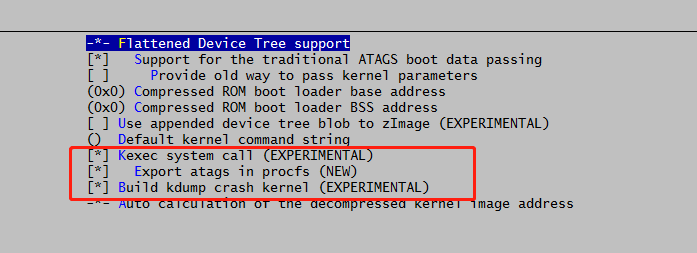
参考文章：

<https://biscuitos.github.io/blog/CRASH/>

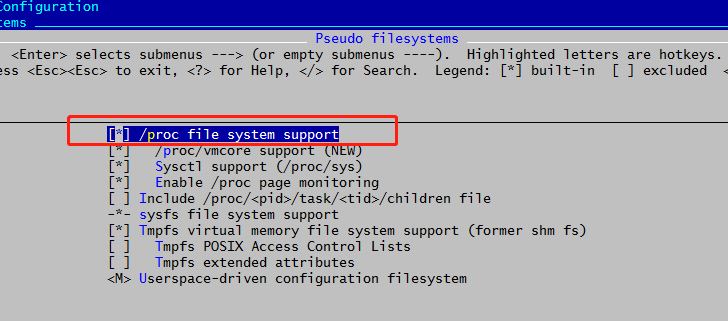
目前主流的方法获得 core dump 是通过 kexec 工具，该工具当内核核心转储时，其他 CPU 夯住，kexec 工具会在一个预留 CPU 上重启一个精简的内核。当精简内核启动之后，可以通过一定的命令将 core 写入到指定的文件，该文件就是核心转储文件。当获得核心转储文件之后，可以使用 CRASH 等工具进行问题分析。

Makemenuconfig:

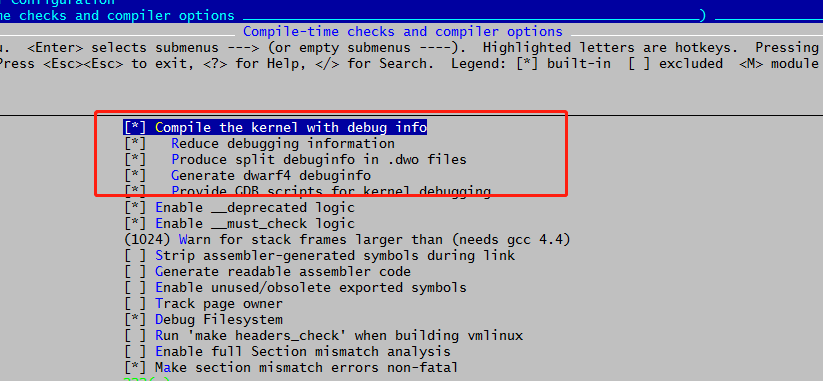
**CONFIG\_KEXEC:**



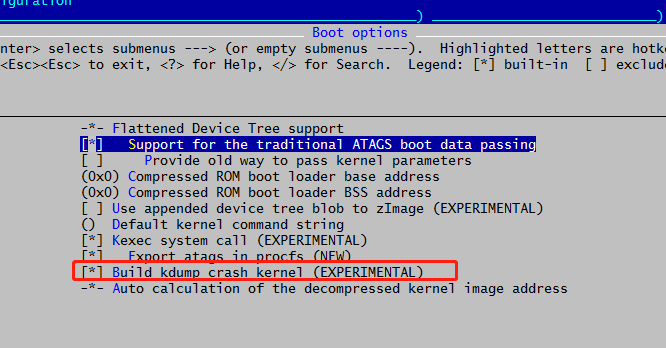
**CONFIG\_SYSFS:**



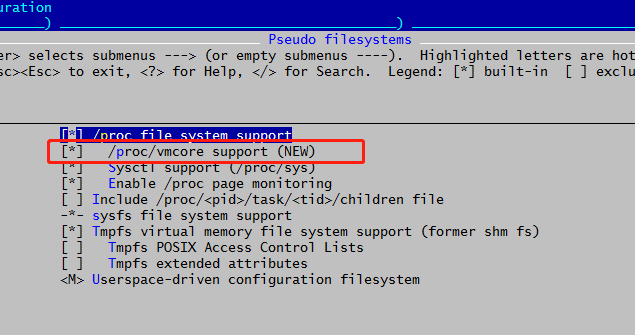
**CONFIG\_DEBUG\_INFO:**



**CONFIG\_CRASH\_DUMP:**



**CONFIG\_PROC\_VMCORE:**



**内核转储 Kdump CMDLINE 配置：**

内核启用相关的内核配置之后，重新编译内核之后需要在 CMDLINE 中配置 crash 内核占用的内存大小，其语法如下:

setenv bootargs\_sys1 'console=ttyS0,115200 mem=512M root=/dev/mmcblk1p1 rw rootwait init=/sbin/init earlyprintk crashkernel=128M'

**内核转储工具安装使用：**

git clone <http://kernel.org/pub/linux/utils/kernel/kexec/kexec-tools.tar.gz>

tar xf kexec-tools.tar.gz

cd kexec-tools-VERSION

./configure ARCH**=**arm --build**=**x86\_64-unknown-linux-gnu --host**=**arm-linux-gnueabi LDFLAGS**=**-static

make

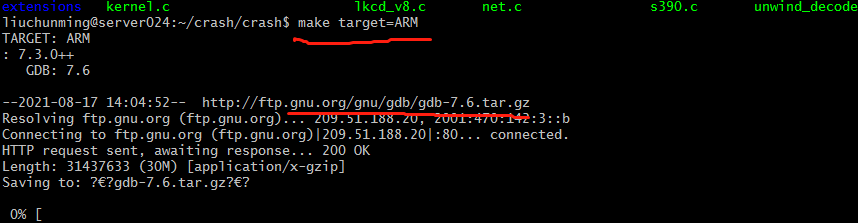
将build目录下的sbin及man copy到开发板的环境变量目录中。

**Crash**

git clone https://gitee.com/mirrors/crash.git

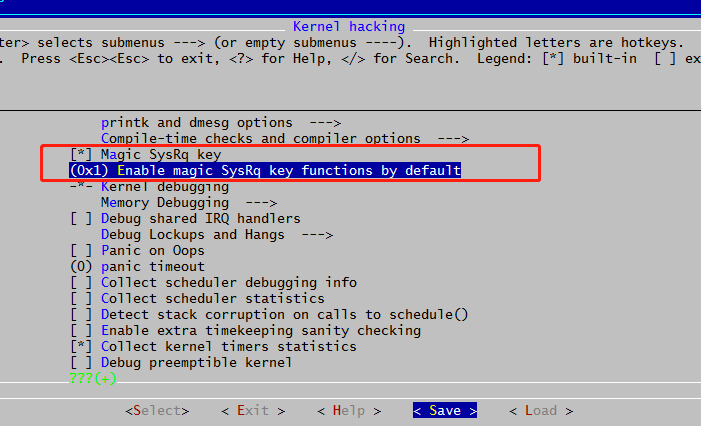
git clone <https://github.com/crash-utility/crash.gi>

make target**=**ARM



./configure ARCH**=**arm --build**=**x86\_64-linux-gnu --host**=** arm-xilinx-linux-gnueabi LDFLAGS**=**-static

出发异常用：

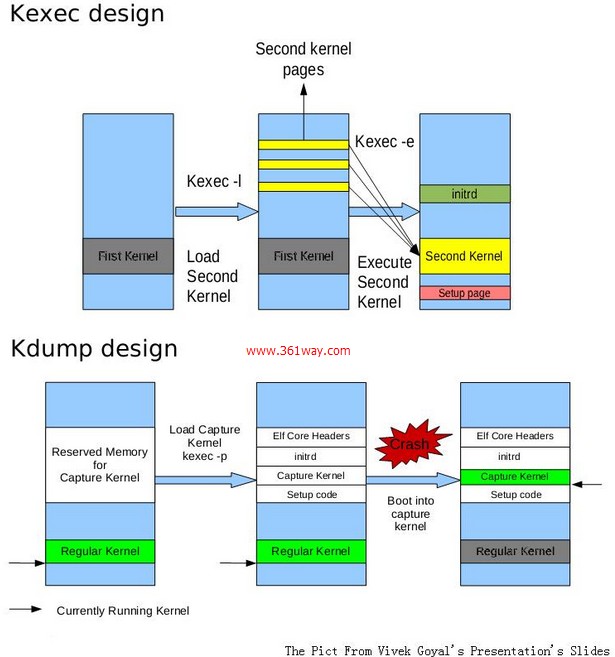


kexec -p <Dump-capture-kernel> --initrd=<initrd-for-Dump-capture-kernel> \

--append=<CMDLINE>



kexec --type zImage -p /data/zImage --dtb=/data/devicetree.dtb --append="ver=v001 console=ttyS0,115200 mem=256M root=/dev/mmcblk1p1 rw rootwait init=/sbin/init earlyprintk product=npes01h\_pro\_ant4\_S"



**kexec 内核加载流程**

1. 将内核镜像文件、根文件系统、命令行参数等segment加载到用户态内存；
2. 对segment sha256检查，确保内核数据没有被破坏；如果是kdump，备份相关数据到备份区（如i386，最开始的640K配置数据用于SMP内核启动，需要备份；或者powerpc，固定位置的异常向量等信息需要备份等）。这个环节又叫purgatory，其流程可以在用户态控制实现，也可以在内核态控制实现（如使能--kexec-file-syscall选项）；
3. 分配内核态页面，并将segment从用户态内存copy到内核态页面；如果使能--kexec-file-syscall选项，则跳过前面两步，直接将segment加载到内核页面，并进行purgatory
4. 分配页面并初始化image->control\_code\_page，对其建立页表，为下一步进行覆盖当前内核时代码寻址的页表映射。初始化LEVEL4/3/2/1 4层页表

代码解析：

发生panic后调用crash\_kexec开始启动新的内核

panic

crash\_kexec