DEVICE DRIVERS

Presented By

Lajul Soni
Mounika Gopagani
Keerthi Kumari Cheguri
Chaithanya Mekala
Vijay Dhoki

AIM:

To create the kernel oops and debugging the kernel opps by using the gdb tool.

Requirements

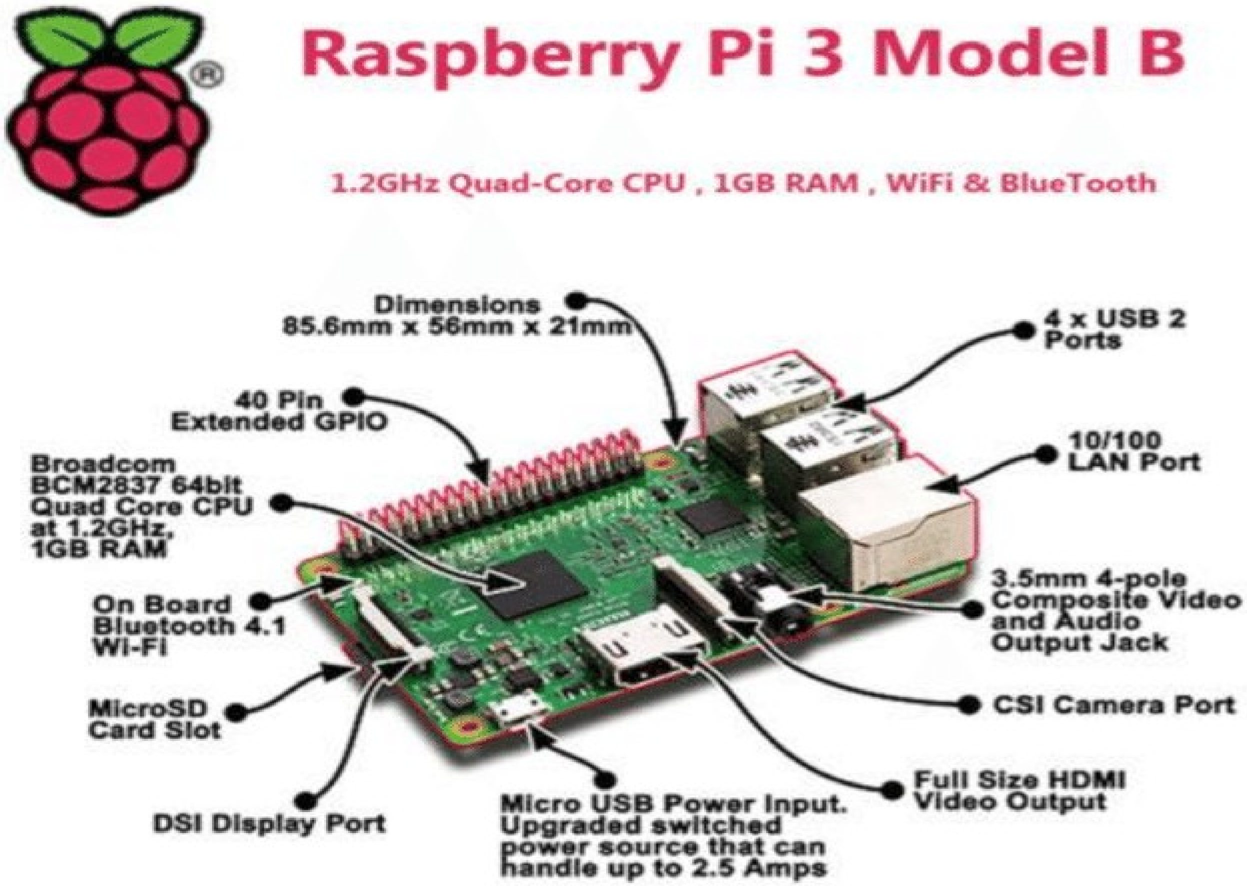
Hardware :

1. Raspberry pi board.
2. HDMI ,USB cables and Adaptor
3. Card reader,SD card(32gb).

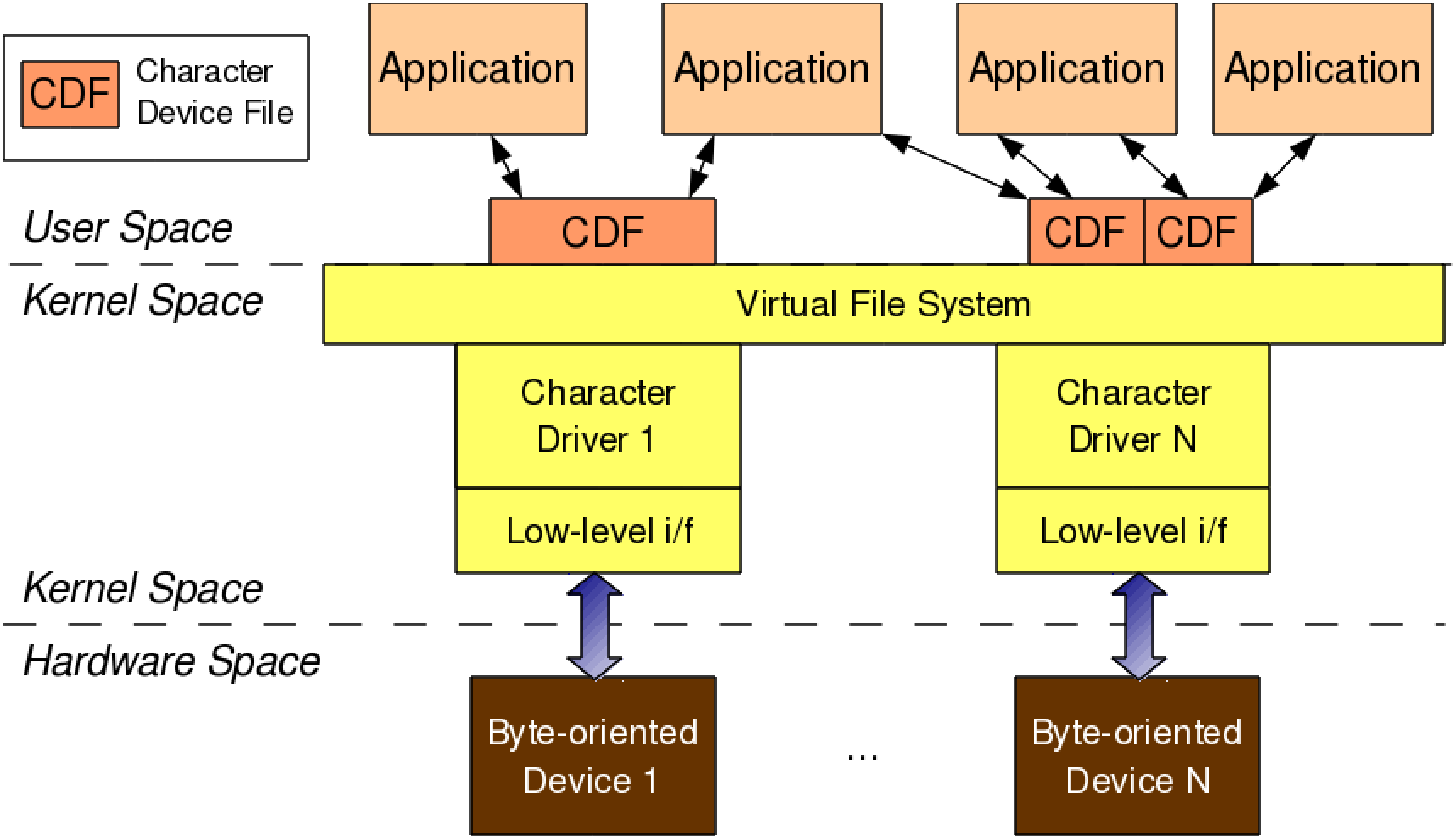
Software :

1. Raspbian OS
2. GDBTools
3. Tool Chains

what is Raspberry Pi Board.

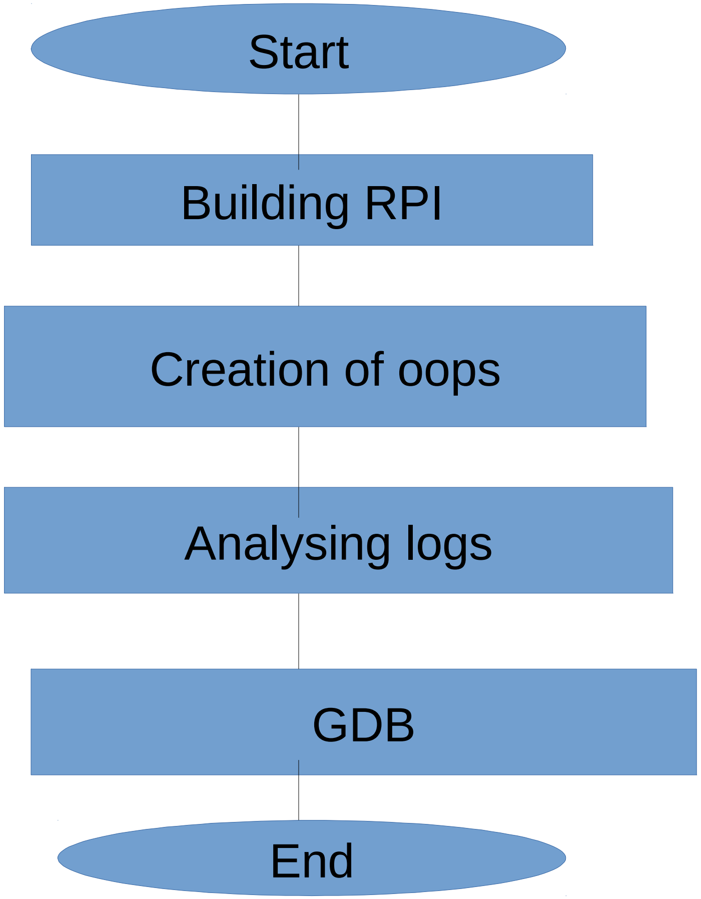

Raspberry Pi 3 Model B
1.2GHz Quad-Core CPU , 1GB RAM , WiFi & BlueTooth
Dimensions 85.6mm x 56mm x 21mm
4 x USB 2 Ports
40 Pin Extended GPIO
10/100 LAN Port
Broadcom BCM2837 64bit Quad Core CPU at 1.2GHz, 1GB RAM
3.5mm 4-pole Composite Video and Audio Output Jack
On Board Bluetooth 4.1 Wi-Fi
CSI Camera Port
MicroSD Card Slot
Full Size HDMI Video Output
DSI Display Port
Micro USB Power Input. Upgraded switched power source that can handle up to 2.5 Amps

what is Device Driver



Design Work

Flow chart :



Kernel Building for Raspberry Pi

1. Clone the Raspbian source code and Tool chain from Git.

2. Look for system architecture and set the tool chain

3. Set default config for raspberry pi 3.

4. Compile Zimage , Dtbs and Modules using cross compiler

5. Copy kernel image and modules to raspberry pi /boot folder.

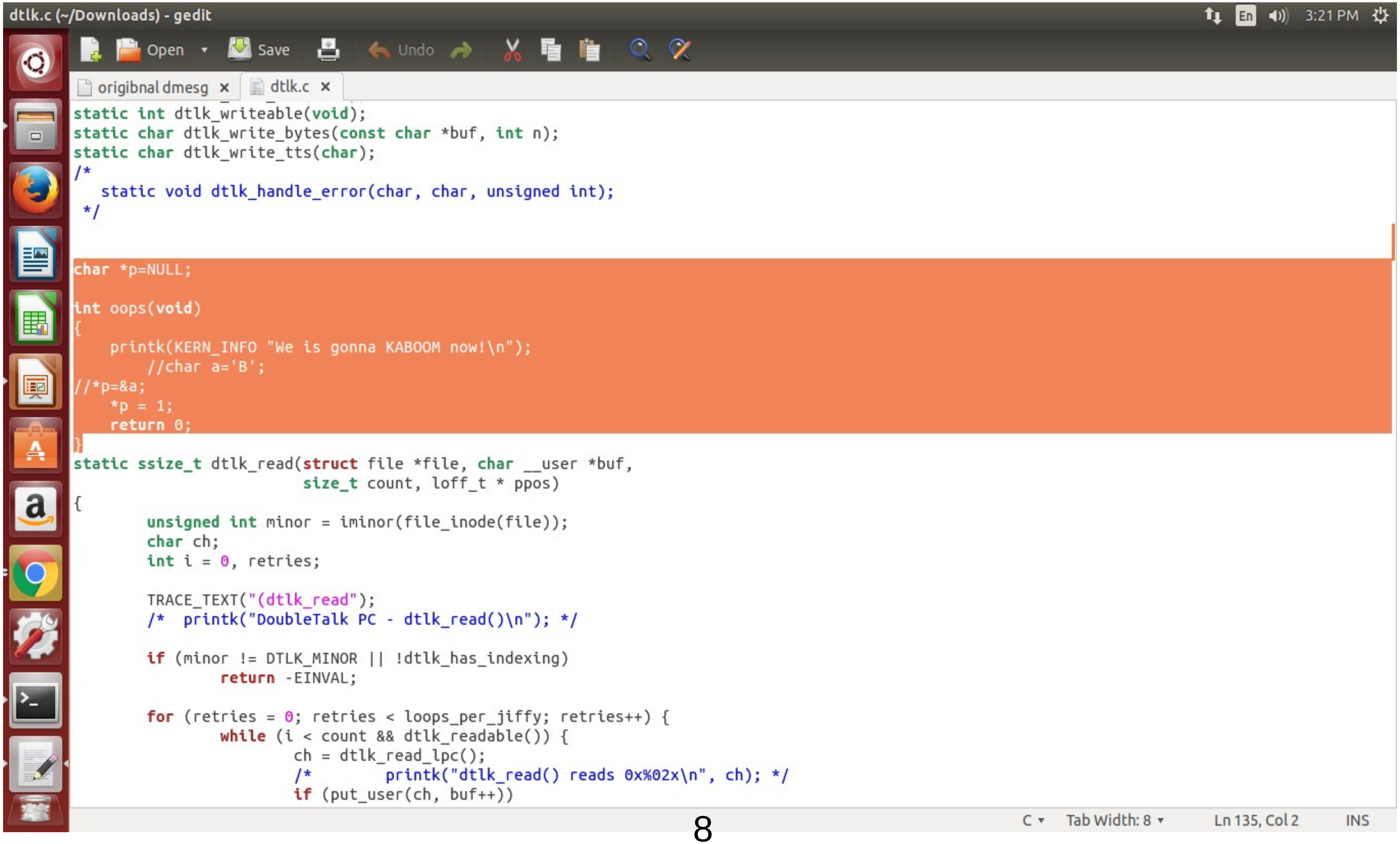
6. Reboot Raspberry pi 3

Oops Creation and Dmesg

1. Taking one existing Driver from raspbian source code

2. Creating the Kernel Oops in driver

Coding/Implementation



```
static int dtlk_writeable(void);
static char dtlk_write_bytes(const char *buf, int n);
static char dtlk_write_tts(char);
/*
   static void dtlk_handle_error(char, char, unsigned int);
 */


char *p=NULL;

int oops(void)
{
    printk(KERN_INFO "We is gonna KABOOM now!\n");
        //char a='B';
//*p=&a;
    *p = 1;
    return 0;
}
static ssize_t dtlk_read(struct file *file, char __user *buf,
                         size_t count, loff_t * ppos)
{
        unsigned int minor = iminor(file_inode(file));
        char ch;
        int i = 0, retries;

        TRACE_TEXT("(dtlk_read");
        /*  printk("DoubleTalk PC - dtlk_read()\n"); */

        if (minor != DTLK_MINOR || !dtlk_has_indexing)
                return -EINVAL;

        for (retries = 0; retries < loops_per_jiffy; retries++) {
                while (i < count && dtlk_readable()) {
                        ch = dtlk_read_lpc();
                        /*        printk("dtlk_read() reads 0x%02x\n", ch); */
                        if (put_user(ch, buf++))
```

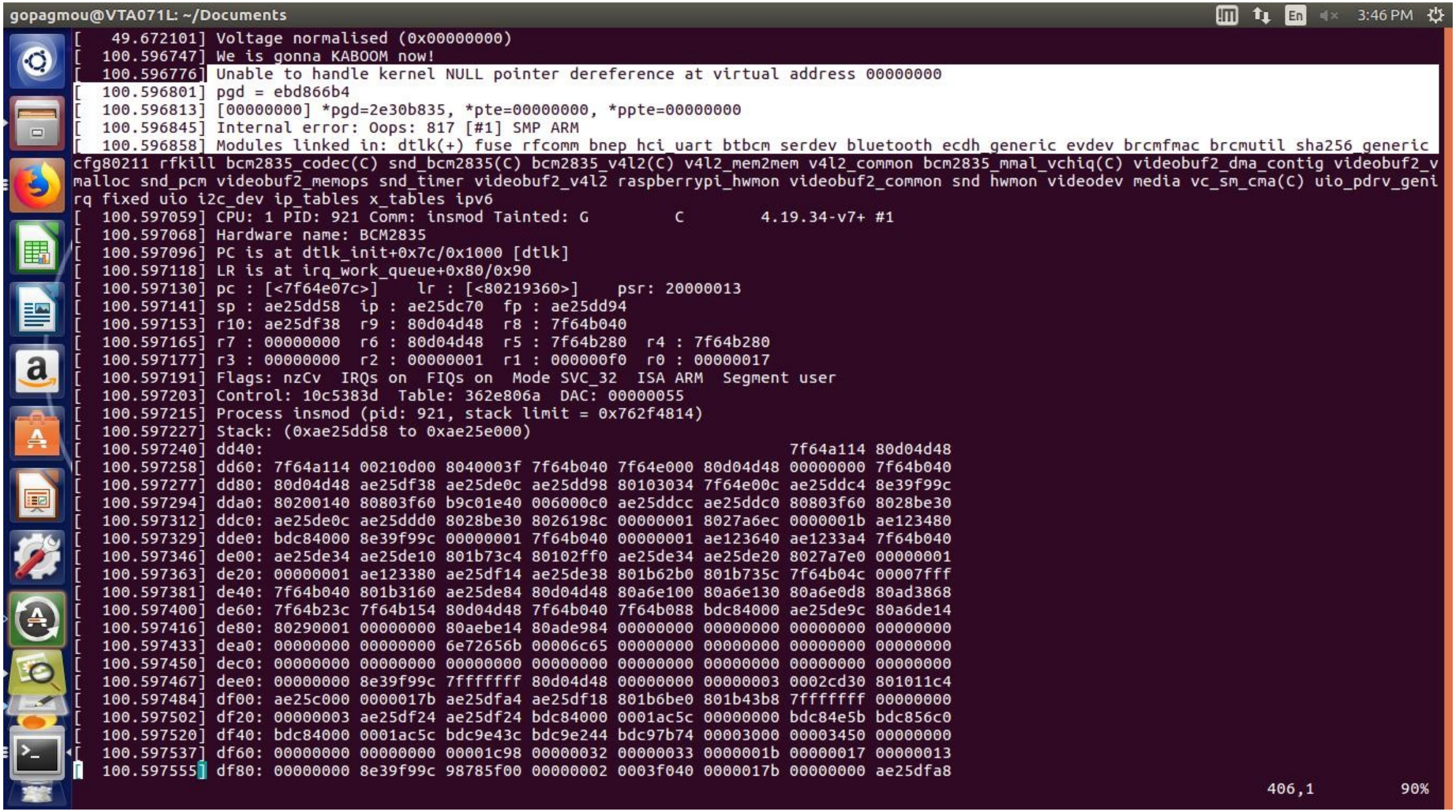
Testing

1. Tested by module

2.Tested by existing driver

3. Tested by own driver

Analysis of Logs from Dmesg



```
[   49.672101] Voltage normalised (0x00000000)
[  100.596747] We is gonna KABOOM now!
[  100.596776] Unable to handle kernel NULL pointer dereference at virtual address 00000000
[  100.596801] pgd = ebd866b4
[  100.596813] [00000000] *pgd=2e30b835, *pte=00000000, *ppte=00000000
[  100.596845] Internal error: Oops: 817 [#1] SMP ARM
[  100.596858] Modules linked in: dtlk(+) fuse rfcomm bnep hci_uart btbcm serdev bluetooth ecdh_generic evdev brcmfmac brcmutil sha256_generic
cfg80211 rfkill bcm2835_codec(C) snd_bcm2835(C) bcm2835_v4l2(C) v4l2_mem2mem v4l2_common bcm2835_mmal_vchiq(C) videobuf2_dma_contig videobuf2_v
malloc snd_pcm videobuf2_memops snd_timer videobuf2_v4l2 raspberrypi_hwmon videobuf2_common snd hwmon videodev media vc_sm_cma(C) uio_pdrv_geni
rq fixed uio i2c_dev ip_tables x_tables ipv6
[  100.597059] CPU: 1 PID: 921 Comm: insmod Tainted: G         C        4.19.34-v7+ #1
[  100.597068] Hardware name: BCM2835
[  100.597096] PC is at dtlk_init+0x7c/0x1000 [dtlk]
[  100.597118] LR is at irq_work_queue+0x80/0x90
[  100.597130] pc : [<7f64e07c>]    lr : [<80219360>]    psr: 20000013
[  100.597141] sp : ae25dd58  ip : ae25dc70  fp : ae25dd94
[  100.597153] r10: ae25df38  r9 : 80d04d48  r8 : 7f64b040
[  100.597165] r7 : 00000000  r6 : 80d04d48  r5 : 7f64b280  r4 : 7f64b280
[  100.597177] r3 : 00000000  r2 : 00000001  r1 : 000000f0  r0 : 00000017
[  100.597191] Flags: nzCv  IRQs on  FIQs on  Mode SVC_32  ISA ARM  Segment user
[  100.597203] Control: 10c5383d  Table: 362e806a  DAC: 00000055
[  100.597215] Process insmod (pid: 921, stack limit = 0x762f4814)
[  100.597227] Stack: (0xae25dd58 to 0xae25e000)
[  100.597240] dd40:                                                       7f64a114 80d04d48
[  100.597258] dd60: 7f64a114 00210d00 8040003f 7f64b040 7f64e000 80d04d48 00000000 7f64b040
[  100.597277] dd80: 80d04d48 ae25df38 ae25de0c ae25dd98 80103034 7f64e00c ae25ddc4 8e39f99c
[  100.597294] dda0: 80200140 80803f60 b9c01e40 006000c0 ae25ddcc ae25ddc0 80803f60 8028be30
[  100.597312] ddc0: ae25de0c ae25ddd0 8028be30 8026198c 00000001 8027a6ec 0000001b ae123480
[  100.597329] dde0: bdc84000 8e39f99c 00000001 7f64b040 00000001 ae123640 ae1233a4 7f64b040
[  100.597346] de00: ae25de34 ae25de10 801b73c4 80102ff0 ae25de34 ae25de20 8027a7e0 00000001
[  100.597363] de20: 00000001 ae123380 ae25df14 ae25de38 801b62b0 801b735c 7f64b04c 00007fff
[  100.597381] de40: 7f64b040 801b3160 ae25de84 80d04d48 80a6e100 80a6e130 80a6e0d8 80ad3868
[  100.597400] de60: 7f64b23c 7f64b154 80d04d48 7f64b040 7f64b088 bdc84000 ae25de9c 80a6de14
[  100.597416] de80: 80290001 00000000 80aebe14 80ade984 00000000 00000000 00000000 00000000
[  100.597433] dea0: 00000000 00000000 6e72656b 00006c65 00000000 00000000 00000000 00000000
[  100.597450] dec0: 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
[  100.597467] dee0: 00000000 8e39f99c 7fffffff 80d04d48 00000000 00000003 0002cd30 801011c4
[  100.597484] df00: ae25c000 0000017b ae25dfa4 ae25df18 801b6be0 801b43b8 7fffffff 00000000
[  100.597502] df20: 00000003 ae25df24 ae25df24 bdc84000 0001ac5c 00000000 bdc84e5b bdc856c0
[  100.597520] df40: bdc84000 0001ac5c bdc9e43c bdc9e244 bdc97b74 00003000 00003450 00000000
[  100.597537] df60: 00000000 00000000 00001c98 00000032 00000033 0000001b 00000017 00000013
[  100.597555] df80: 00000000 8e39f99c 98785f00 00000002 0003f040 0000017b 00000000 ae25dfa8
                                                                                          406,1          90%
```

Debugging by Gdb

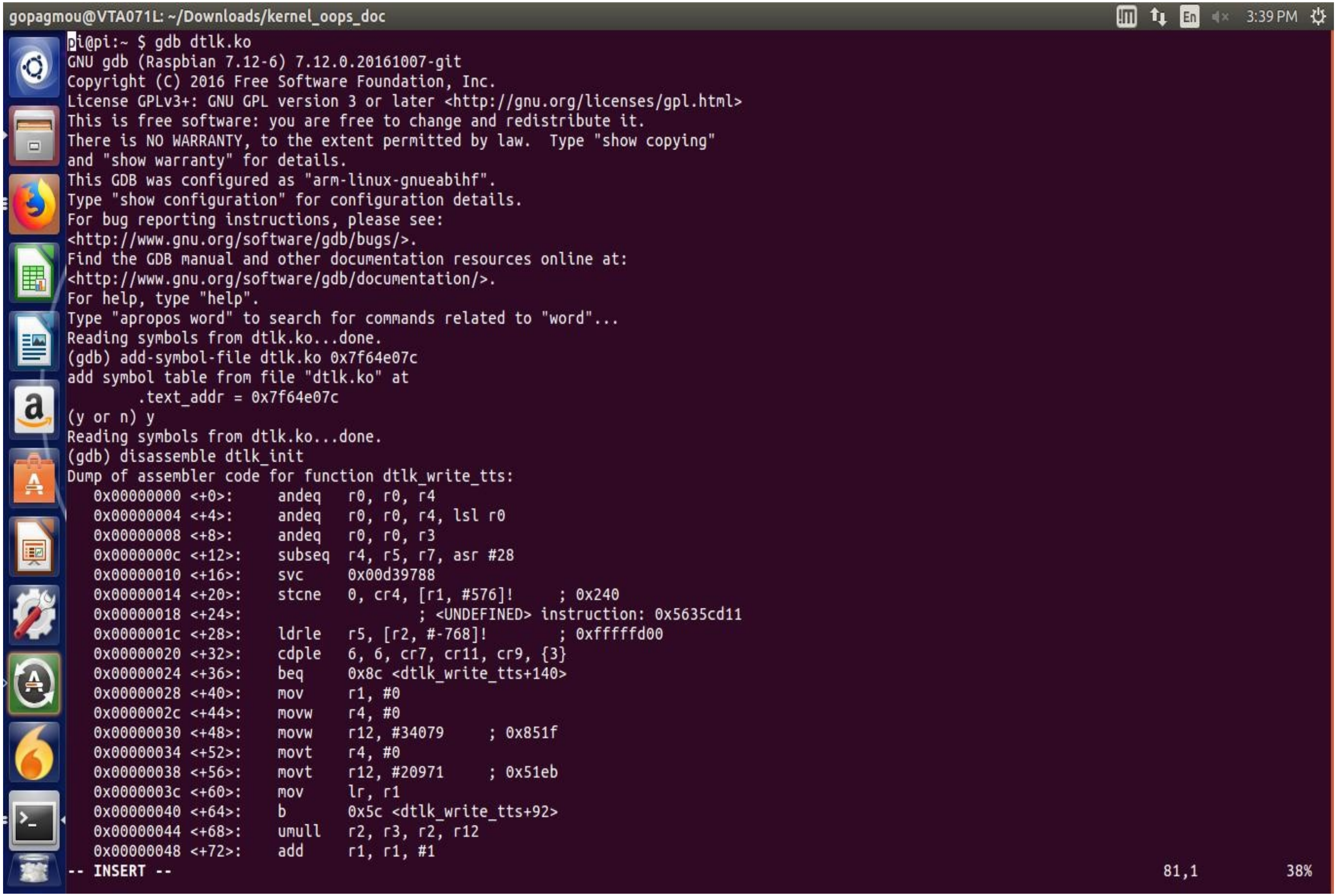
Commands are:

```
>  gdb oops.ko

> add-symbol-file  oops.ko address

> disassemble function name

> list *address
```



```
pi@pi:~ $ gdb dtlk.ko
GNU gdb (Raspbian 7.12-6) 7.12.0.20161007-git
Copyright (C) 2016 Free Software Foundation, Inc.
License GPLv3+: GNU GPL version 3 or later <http://gnu.org/licenses/gpl.html>
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.  Type "show copying"
and "show warranty" for details.
This GDB was configured as "arm-linux-gnueabihf".
Type "show configuration" for configuration details.
For bug reporting instructions, please see:
<http://www.gnu.org/software/gdb/bugs/>.
Find the GDB manual and other documentation resources online at:
<http://www.gnu.org/software/gdb/documentation/>.
For help, type "help".
Type "apropos word" to search for commands related to "word"...
Reading symbols from dtlk.ko...done.
(gdb) add-symbol-file dtlk.ko 0x7f64e07c
add symbol table from file "dtlk.ko" at
        .text_addr = 0x7f64e07c
(y or n) y
Reading symbols from dtlk.ko...done.
(gdb) disassemble dtlk_init
Dump of assembler code for function dtlk_write_tts:
   0x00000000 <+0>:     andeq   r0, r0, r4
   0x00000004 <+4>:     andeq   r0, r0, r4, lsl r0
   0x00000008 <+8>:     andeq   r0, r0, r3
   0x0000000c <+12>:    subseq  r4, r5, r7, asr #28
   0x00000010 <+16>:    svc     0x00d39788
   0x00000014 <+20>:    stcne   0, cr4, [r1, #576]!     ; 0x240
   0x00000018 <+24>:                    ; <UNDEFINED> instruction: 0x5635cd11
   0x0000001c <+28>:    ldrle   r5, [r2, #-768]!        ; 0xfffffd00
   0x00000020 <+32>:    cdple   6, 6, cr7, cr11, cr9, {3}
   0x00000024 <+36>:    beq     0x8c <dtlk_write_tts+140>
   0x00000028 <+40>:    mov     r1, #0
   0x0000002c <+44>:    movw    r4, #0
   0x00000030 <+48>:    movw    r12, #34079     ; 0x851f
   0x00000034 <+52>:    movt    r4, #0
   0x00000038 <+56>:    movt    r12, #20971     ; 0x51eb
   0x0000003c <+60>:    mov     lr, r1
   0x00000040 <+64>:    b       0x5c <dtlk_write_tts+92>
   0x00000044 <+68>:    umull   r2, r3, r2, r12
   0x00000048 <+72>:    add     r1, r1, #1
-- INSERT --                                                                 81,1          38%
```

THANK YOU