the keys to homebrew

running custom code on bmw display key

BMW introduces the Key fob with touchscreen display

The innovative premium key fob will be available as an option for the BMW i8 from autumn 2015.

bmw display key

- whoami
- what
- motivation
- process

jeffrey crowell <crowell@bu.edu>

automotive/r2 enthusiast.


512
8D7U834


HOLD
HOLD

Low Technology


05:06:17 PM
Vehicle secured
Trunk
Closed
Alarm
On
Interior and tilt sensor
Off

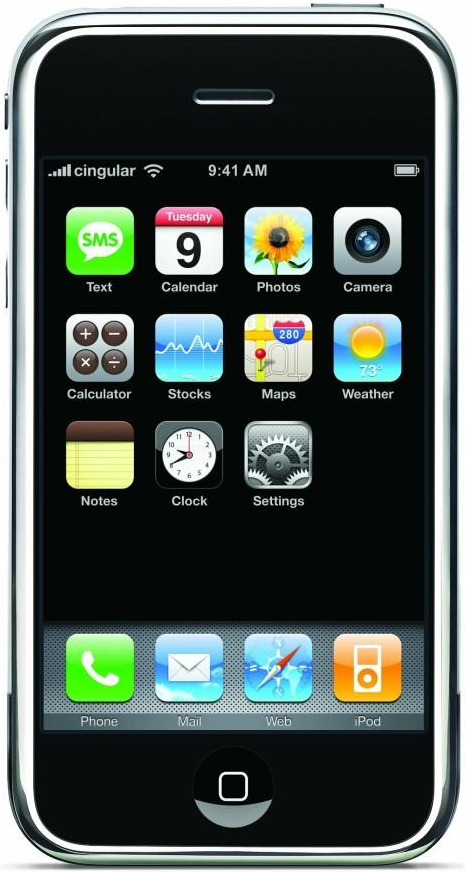
100% Higher Technology

MCIMX285AVM4B
M06Z
CTLU1525E
CHINA
JH60600065QV

- NXP MCIMX285AVM4B (ARM926EJ)
- Cypress S25FL512S 512 Mbit (64 Mbyte SPI Flash)
- 128 MB mDDR Memory

Operating Characteristics

Parameter	Value
Core Type	Arm9
Operating Frequency [Max] (MHz)	454
Core: Number of cores (SPEC)	1


cingular
9:41 AM
Text
Tuesday
9
Calendar
Photos
Camera
Calculator
Stocks
280
Maps
73°
Weather
Notes
Clock
Settings
Phone
Mail
Web
iPod

Apple iPhone: Mid 2007

Samsung ARM SoC 620 MHz 1176 running at 412 Mhz + PowerVR MBX 3D GPU

128MB RAM

8 or 16GB Flash storage

320×480 3.5” display with finger multitouch input

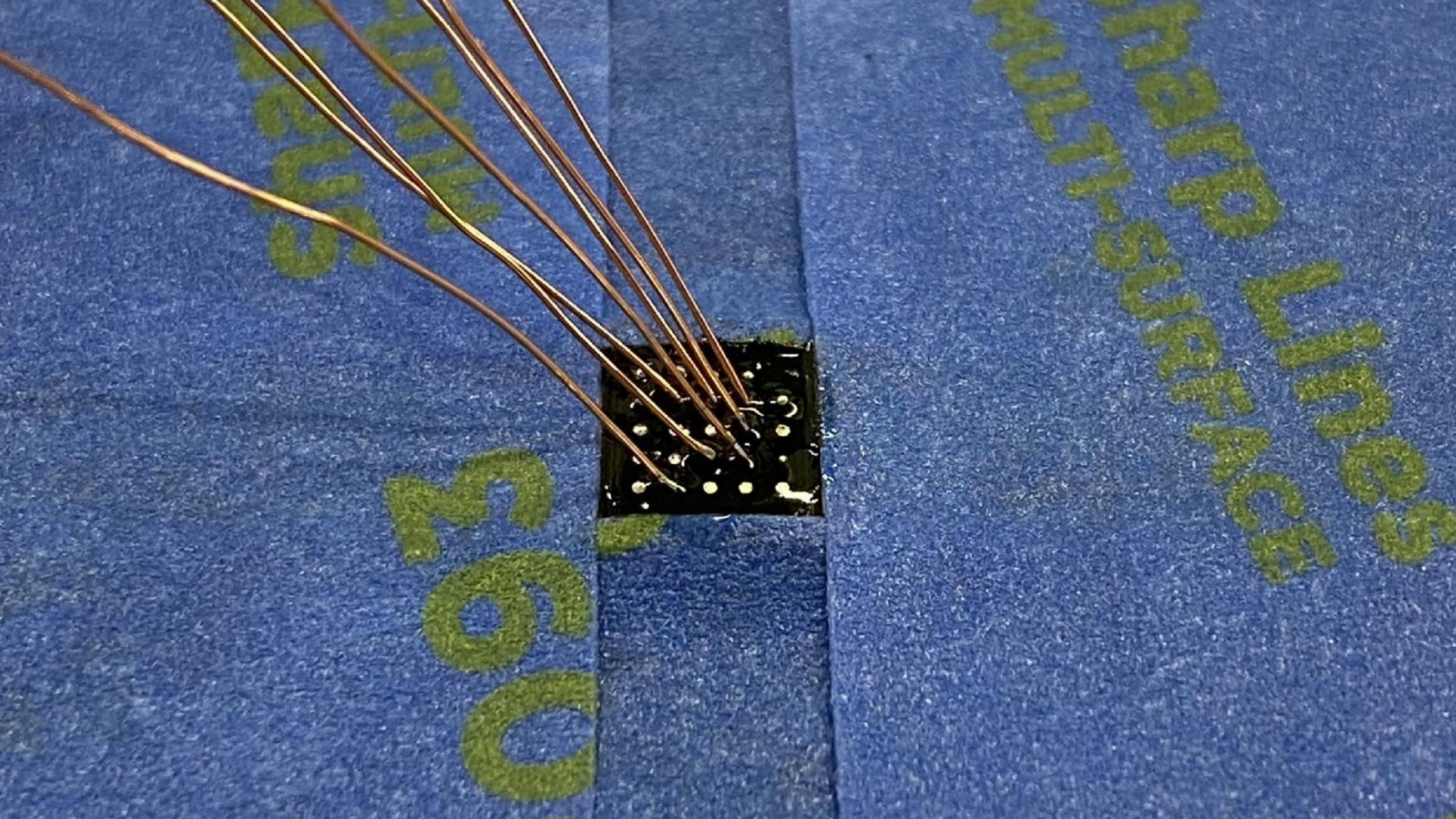
Accelerometers for direct physical control

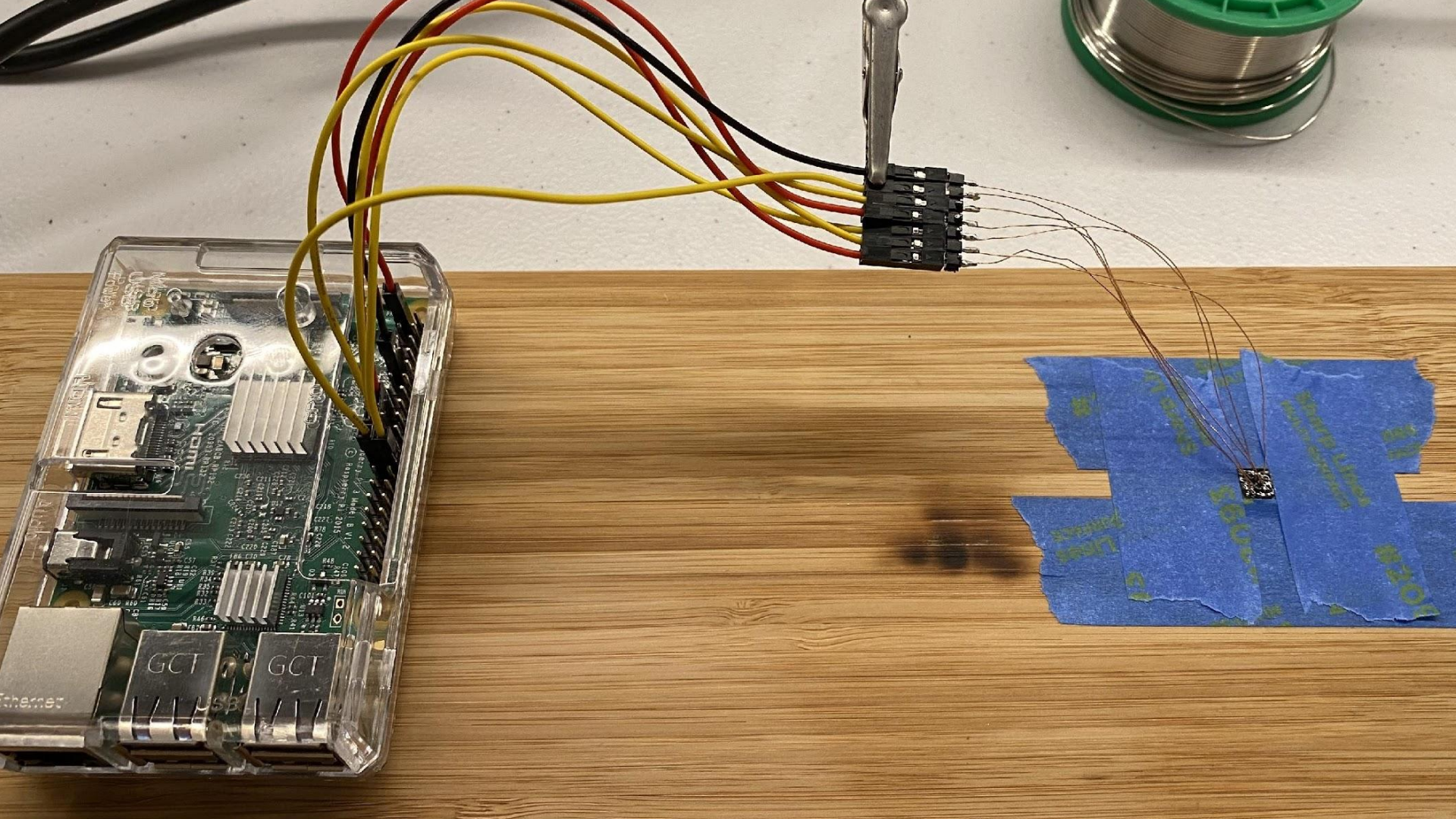
2 Megapixel camera

Quad band GSM + EDGE

WiFi 802.11 b/g

BlueTooth 2.0 EDR


Sharp Lines
Multi-Surface

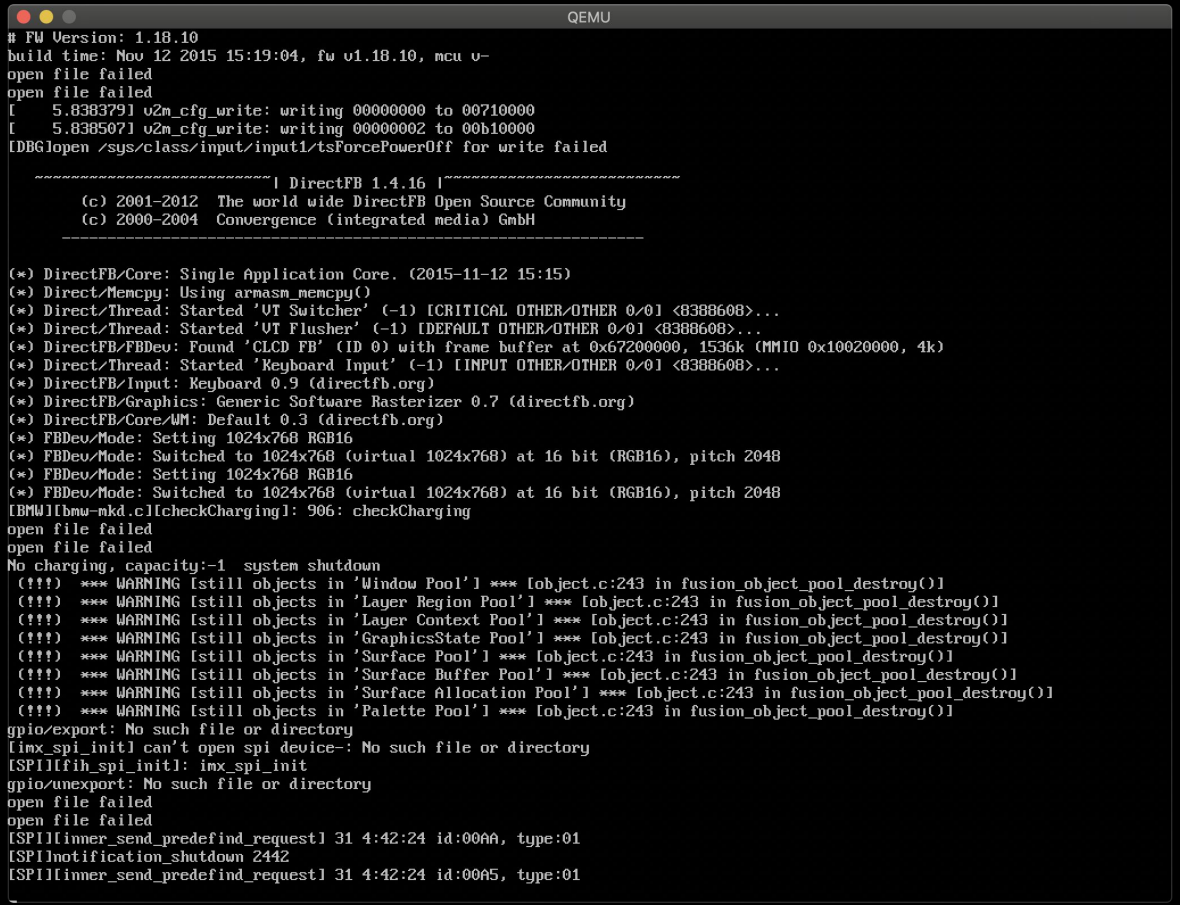

GCT
GCT
USB

```
jeff@busytown ~/Downloads $ binwalk bmw.bin | head -n 10

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
524288        0x80000         uImage header, header size: 64 bytes, header CRC: 0x48E757, created: 2015-
11-12 15:20:08, image size: 1145056 bytes, Data Address: 0x40008000, Entry Point: 0x40008000, data CRC:
0x510ECE89, OS: Linux, CPU: ARM, image type: OS Kernel Image, compression type: none, image name: "Linux
-2.6.35.3-1129-g691c08a"
524352        0x80040         Linux kernel ARM boot executable zImage (little-endian)
541021        0x8415D         gzip compressed data, maximum compression, from Unix, last modified: 2015-
11-12 15:13:08
2883584       0x2C0000        Linux EXT filesystem, blocks count: 32714, image size: 33499136, rev 0.0,
ext2 filesystem data, UUID=00000000-0000-0000-0000-000000000000
53215232      0x32C0000       JFFS2 filesystem, little endian
54001872      0x33800D0       Zlib compressed data, compressed
54003560      0x3380768       Zlib compressed data, compressed
Exception ignored in: <_io.TextIOWrapper name='<stdout>' mode='w' encoding='utf-8'>
BrokenPipeError: [Errno 32] Broken pipe
jeff@busytown ~/Downloads $
```

Danger of overheating

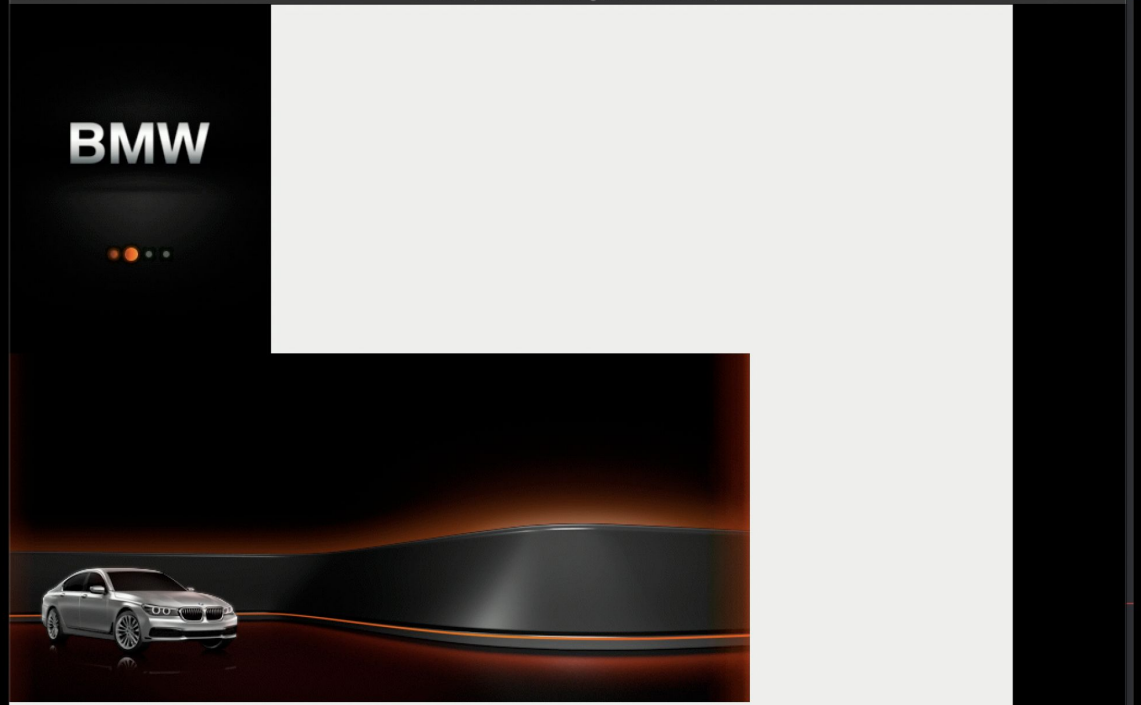
Key needs to
cool down


QEMU


QEMU
FW Version: 1.18.10
build time: Nov 12 2015 15:19:04, fw v1.18.10, mcu v-
open file failed
open file failed
[5.838379] v2m_cfg_write: writing 00000000 to 00710000
[5.838507] v2m_cfg_write: writing 00000002 to 00b10000
[DBG]open /sys/class/input/input1/tsForcePowerOff for write failed
~~~~~~~~~~~~~~~~~~~~~~~~~~| DirectFB 1.4.16 |~~~~~~~~~~~~~~~~~~~~~~~~~~
(c) 2001-2012 The world wide DirectFB Open Source Community
(c) 2000-2004 Convergence (integrated media) GmbH
(*) DirectFB/Core: Single Application Core. (2015-11-12 15:15)
(*) Direct/Memcpy: Using armasm_memcpy()
(*) Direct/Thread: Started 'VT Switcher' (-1) [CRITICAL OTHER/OTHER 0/0] <8388608>...
(*) Direct/Thread: Started 'VT Flusher' (-1) [DEFAULT OTHER/OTHER 0/0] <8388608>...
(*) DirectFB/FBDev: Found 'CLCD FB' (ID 0) with frame buffer at 0x67200000, 1536k (MMIO 0x10020000, 4k)
(*) Direct/Thread: Started 'Keyboard Input' (-1) [INPUT OTHER/OTHER 0/0] <8388608>...
(*) DirectFB/Input: Keyboard 0.9 (directfb.org)
(*) DirectFB/Graphics: Generic Software Rasterizer 0.7 (directfb.org)
(*) DirectFB/Core/WM: Default 0.3 (directfb.org)
(*) FBDev/Mode: Setting 1024x768 RGB16
(*) FBDev/Mode: Switched to 1024x768 (virtual 1024x768) at 16 bit (RGB16), pitch 2048
(*) FBDev/Mode: Setting 1024x768 RGB16
(*) FBDev/Mode: Switched to 1024x768 (virtual 1024x768) at 16 bit (RGB16), pitch 2048
[BMW][bmw-mkd.c][checkCharging]: 906: checkCharging
open file failed
open file failed
No charging, capacity:-1 system shutdown
(!!!) *** WARNING [still objects in 'Window Pool'] *** [object.c:243 in fusion_object_pool_destroy()]
(!!!) *** WARNING [still objects in 'Layer Region Pool'] *** [object.c:243 in fusion_object_pool_destroy()]
(!!!) *** WARNING [still objects in 'Layer Context Pool'] *** [object.c:243 in fusion_object_pool_destroy()]
(!!!) *** WARNING [still objects in 'GraphicsState Pool'] *** [object.c:243 in fusion_object_pool_destroy()]
(!!!) *** WARNING [still objects in 'Surface Pool'] *** [object.c:243 in fusion_object_pool_destroy()]
(!!!) *** WARNING [still objects in 'Surface Buffer Pool'] *** [object.c:243 in fusion_object_pool_destroy()]
(!!!) *** WARNING [still objects in 'Surface Allocation Pool'] *** [object.c:243 in fusion_object_pool_destroy()]
(!!!) *** WARNING [still objects in 'Palette Pool'] *** [object.c:243 in fusion_object_pool_destroy()]
gpio/export: No such file or directory
[imx_spi_init] can't open spi device-: No such file or directory
[SPI][fih_spi_init]: imx_spi_init
gpio/unexport: No such file or directory
open file failed
open file failed
[SPI][inner_send_predefind_request] 31 4:42:24 id:00AA, type:01
[SPI]notification_shutdown 2442
[SPI][inner_send_predefind_request] 31 4:42:24 id:00A5, type:01
~~~~~~~~~~~~~~~~~~~~~~~~~~

Done

QEMU - (Press ctrl + alt + g to release Mouse)



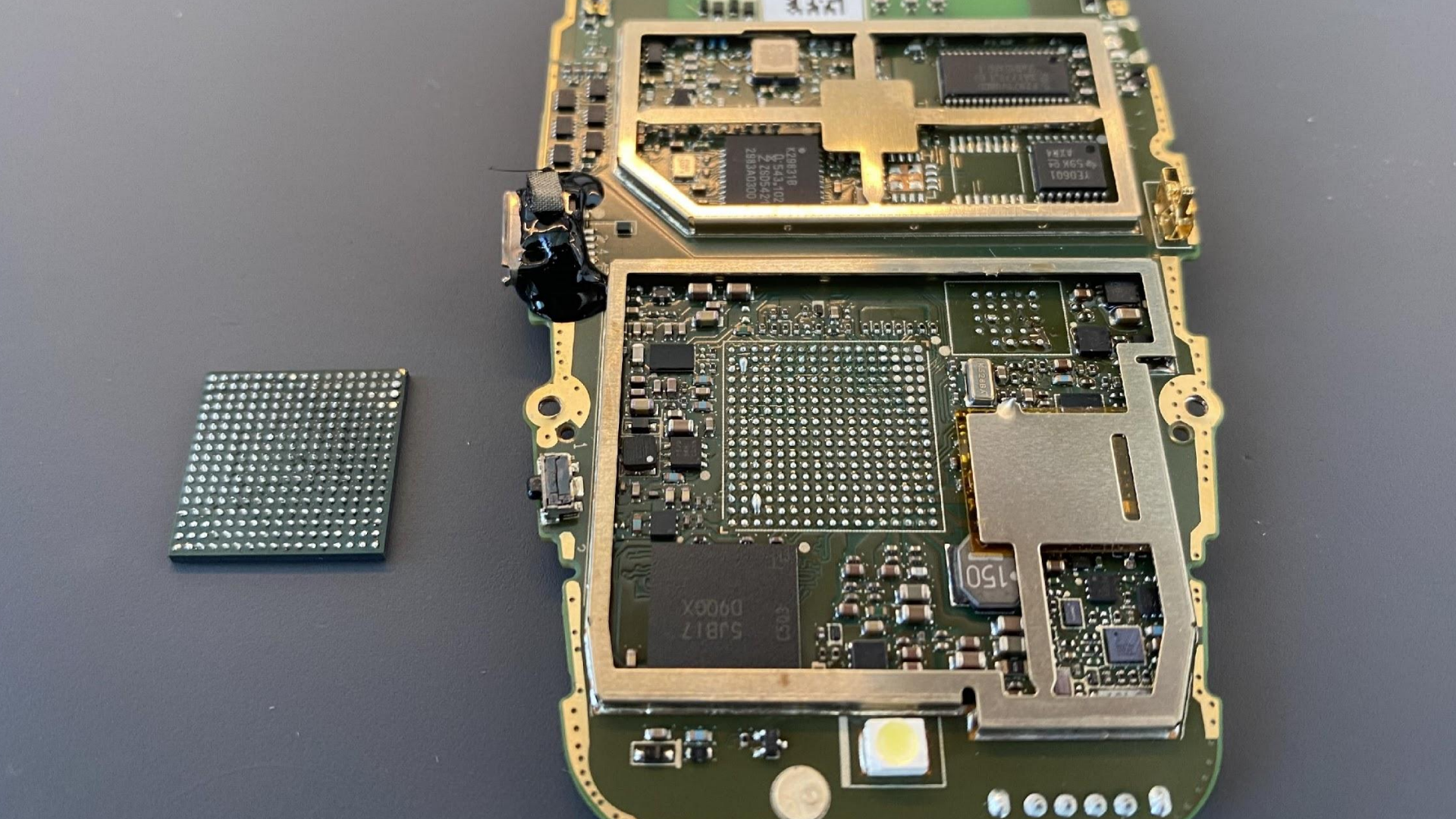
00:06 -00:03

QEMU

```
specifying one with the '-iwad' command line parameter.


^C
/fbdoom_dist # LD_LIBRARY_PATH=$(pwd) ./ld-linux-armhf.so.3 ./fbdoom  -iwad ../
```


```
I_InitGraphics: Auto-scaling factor: 3
101-key keyboard found.
Using keyboard on /dev/tty.
Ready to read keycodes. Press Backspace to exit.
```

MCIMX28SAVM4B
M06Z
CTLU1525E
CHINA



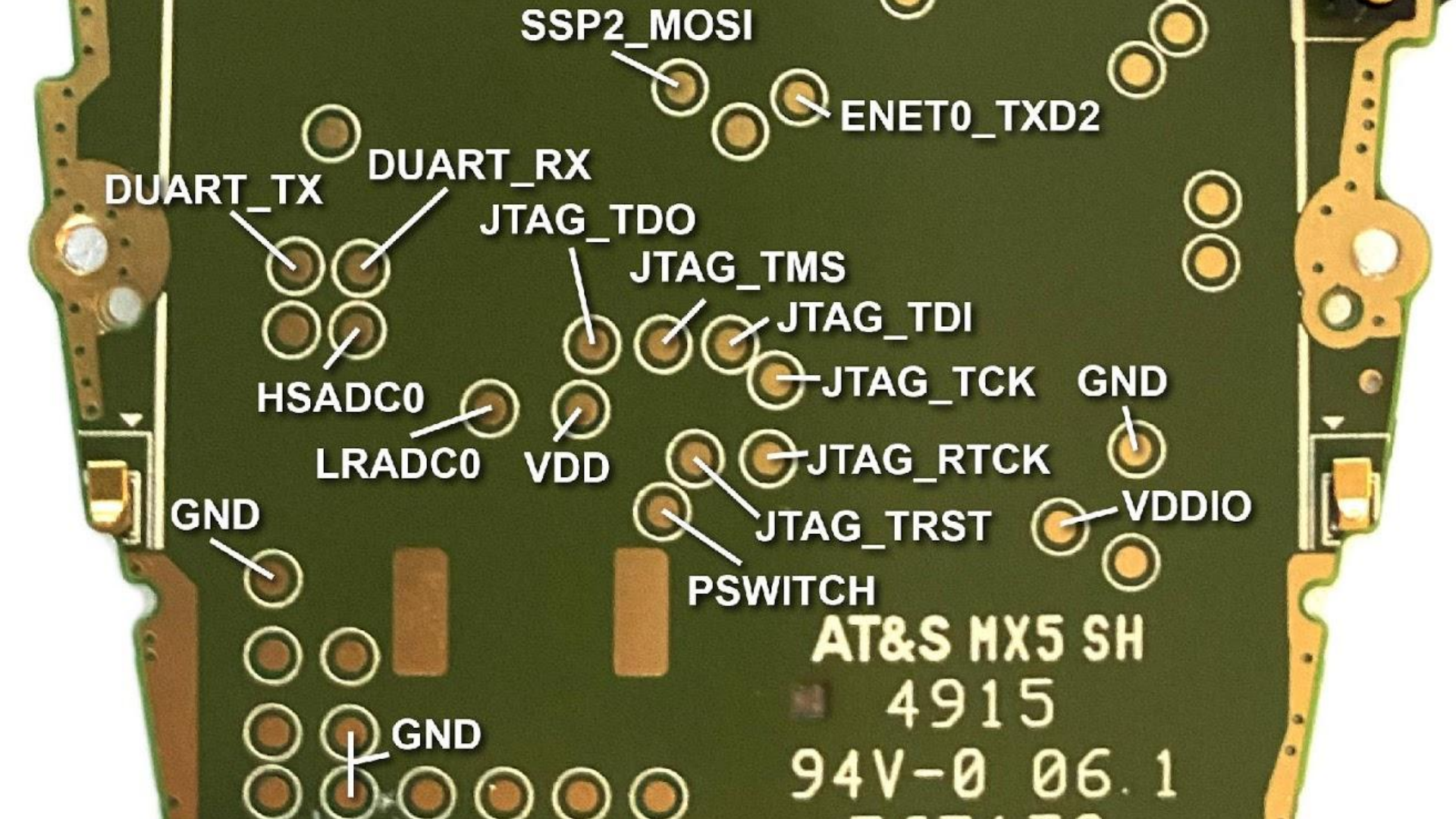
	U	T	R	P	N	M	L	K	J	H	G	F	E	D	C	B	A	
1	VSS	LCD_D12	LCD_D10	LCD_D07	NC	NC	NC	LCD_WR_RWN	ENET0_RXD2	ENET0_RXD0	ENET0_TXD2	ENET0_TXD0	NC	NC	NC	NC	VSS	1
2	LCD_D14	LCD_D13	LCD_D11	LCD_D08	LCD_D06	LCD_D04	LCD_D02	LCD_D00	ENET0_RXD3	ENET0_RXD1	ENET0_TXD3	ENET0_TXD1	ENET_CLK	NC	NC	NC	NC	2
3	LCD_D15	LCD_D16	LCD_D17	LCD_D09	VDDIO33	LCD_D05	LCD_D03	LCD_D01	ENET0_CRS	VSS	VDDIO33	ENET0_RX_CLK	ENET0_TX_CLK	SSP2_SS1	SSP2_MOSI	SSP2_MISO	SSP2_SCK	3
4	LCD_D18	LCD_D19	LCD_D20	LCD_RD_E	VSS	LCD_RS	AUART1_RX	AUART1_TX	ENET0_COL	ENET0_MDIO	ENET0_MDC	ENET0_TX_EN	ENET0_RX_EN	SSP2_SS2	SSP2_SS0	SSP0_DATA7	SSP0_CMD	4
5	LCD_D21	LCD_D22	LCD_D23	LCD_CS	NC	NC	NC	NC	NC	AUART0_TX	AUART0_RX	NC	VSS	SSP0_DATA6	SSP0_DATA5	SSP0_DATA4	SSP0_DATA3	5
6	GPMI_D06	GPMI_D07	GPMI_RDN	GPMI_ALE	GPMI_RDY0	LCD_RESET	NC	NC	AUART0_CTS	NC	SAIF0_LRCLK	NC	VDDIO33	SSP0_DATA2	SSP0_DATA1	SSP0_DATA0	SSP0_SCK	6
7	GPMI_D03	GPMI_D04	GPMI_D05	GPMI_CLE	GPMI_CE0N	GPMI_CE2N	PWM1	PWM0	AUART0_RTS	NC	SAIF0_MCLK	SAIF0_BITCLK	SAIF0_SDATA0	SPDIF	I2C0_SCL	VSS	VDDIO33	7
8	GPMI_D00	GPMI_D01	GPMI_D02	GPMI_WRN	GPMI_RDY1	GPMI_RDY2	GPMI_RDY3	PWM2	VDDIO33	VDDIO33	VDDIO18	VDDIO18	SAIF1_SDATA0	I2C0_SDA	LRADC2	USB1DM	USB1DP	8
9	EMI_A08	EMI_A13	EMI_A06	EMI_CE1N	GPMI_CE1N	GPMI_CE3N	GPMI_RESETN	VSS	VDDIO33	VSS	VDDIO18	VDDIO18	PWM3	LRADC3	LRADC1	DEBUG	VSS	9
10	EMI_A04	EMI_A11	VSSIO_EMI	EMI_A09	EMI_A14	VDDIO_EMI	VSS	VSS	VDDIO33	VSS	VDDD	VDDD	PWM4	SSP0_			USB0DM	10
11	EMI_A12	EMI_A03	EMI_A05	VDDIO_EMI	EMI_A07	VDDIO_EMI	VSS	VSS	VSS	VSS	VDDD	VDDD	JTAG_TCK	RTC			PSWITCH	11
12	EMI_A01	EMI_BA1	VSSIO_EMI	EMI_CE0N	EMI_BA2	VDDIO_EMI	VSSIO_EMI	VDDD	VSS	VSS			JTAG_TDI	JTAG_TMS	VDDXTAL	XTALO	XTALI	12
13	EMI_A10	EMI_CKE	VDDIO_EMI	EMI_D04	VDDIO_EMI	EMI_D01	VDDIO_EMI	EMI_VREF1	VDDIO_EMIQ	EMI_D12			JTAG_TDO	LRADC4	VDDA1	VSSA1	VDD4P2	13
14	EMI_A02	VSSIO_EMI	EMI_VREF0	VSSIO_EMI	EMI_D03	VSS	EMI_D06	EMI_DDR_OPEN	EMI_D11	VSSIO_EMI	EMI_D10	VSSIO_EMI	JTAG_RTCK	JTAG_TRST	LRADC6	HSADC0	RESETN	14
15	EMI_A00	EMI_WEN	VDDIO_EMIQ	EMI_D02	VDDIO_EMI	EMI_DQM0	EMI_DDR_OPEN_FB	VDDIO_EMIQ	VSS	EMI_D09	VDDIO_EMI	EMI_DQM1	VSS	LRADC5	LRADC0	DCDC_BATT	BATTERY	15
16	EMI_CASN	EMI_BA0	EMI_RASN	VSSIO_EMI	EMI_D00	VSSIO_EMI	EMI_CLKN	EMI_DQS0N	EMI_DQS1N	VSS	EMI_D08	VSSIO_EMI	VDDIO33	VDD1P5	VSS	DCDC_VDDA	DCDC_LP	16
17	VSSIO_EMI	EMI_ODT1	EMI_ODT0	EMI_D05	VDDIO33_EMI	EMI_D07	EMI_CLK	EMI_DQS0	EMI_DQS1	EMI_D13	VDDIO_EMI	EMI_D15	VDD5V	DCDC_VDDD	DCDC_VDDIO	DCDC_LN1	DCDC_GND	17
	U	T	R	P	N	M	L	K	J	H	G	F	E	D	C	B	A	

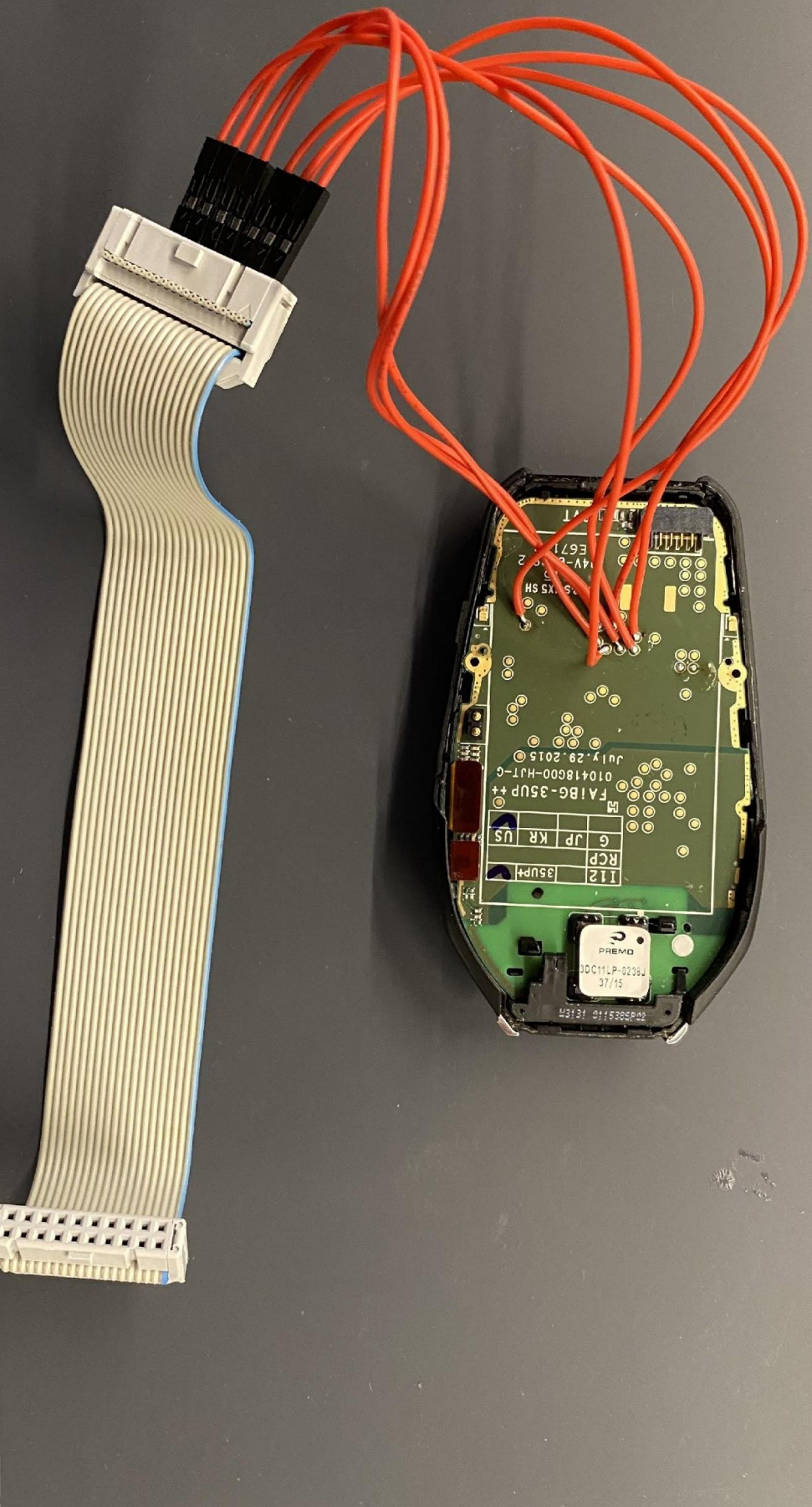
JTAG

PSWITCH

Table 67. 289-Pin i.MX28S MAPBGA Ball Map

PSWITCH - "The pin is used for chip power on or recovery. VDDIO can be applied to PSWITCH through a 10 kΩ resistor. This is necessary in order to enter the chip’s firmware recovery. The on-chip circuitry prevents the actual voltage on the pin from exceeding acceptable levels."

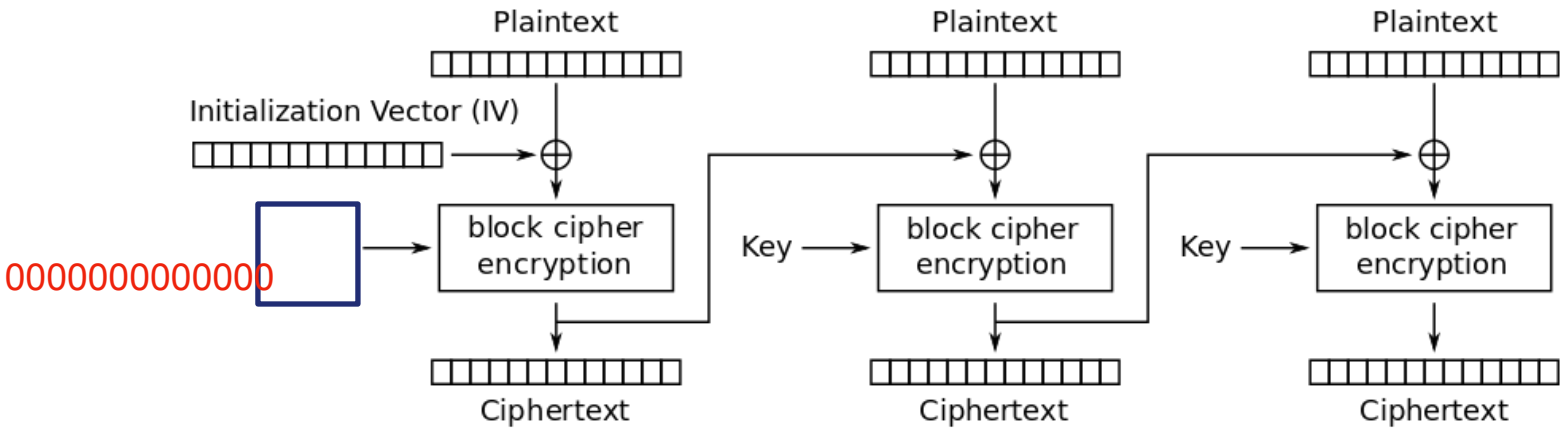

SSP2_MOSI
ENET0_TXD2
DUART_TX
DUART_RX
JTAG_TDO
JTAG_TMS
JTAG_TDI
JTAG_TCK
GND
HSADC0
LRADC0
VDD
JTAG_RTCK
VDDIO
GND
JTAG_TRST
PSWITCH
AT&S MX5 SH
4915
94V-0 06.1
GND


PREMO

```
0xc003eafc in ?? ()
(gdb) i r
r0             0xea60              60000
r1             0x60000013
1610612755
r2             0x1000              4096
r3             0x60000093
1610612883
r4             0xc024e000
3223642112
r5             0xc0252438
3223659576
r6             0xc026a044
3223756868
r7             0xc0252430
3223659568
r8             0x4001b8c8
1073854664
r9             0x41069265
1090949733
r10            0x4001b75c
1073854300
r11            0xc024ff94
3223650196
r12            0xc024ff98
3223650200
sp             0xc024ff88
0xc024ff88
lr             0xc00345d4
3221439956
```

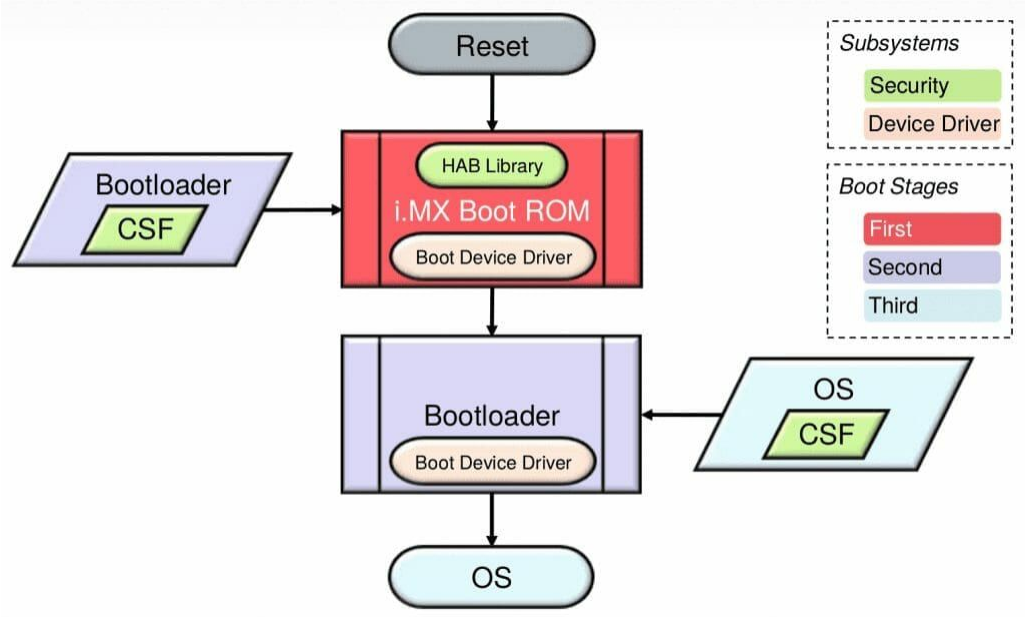
JTAG debugging

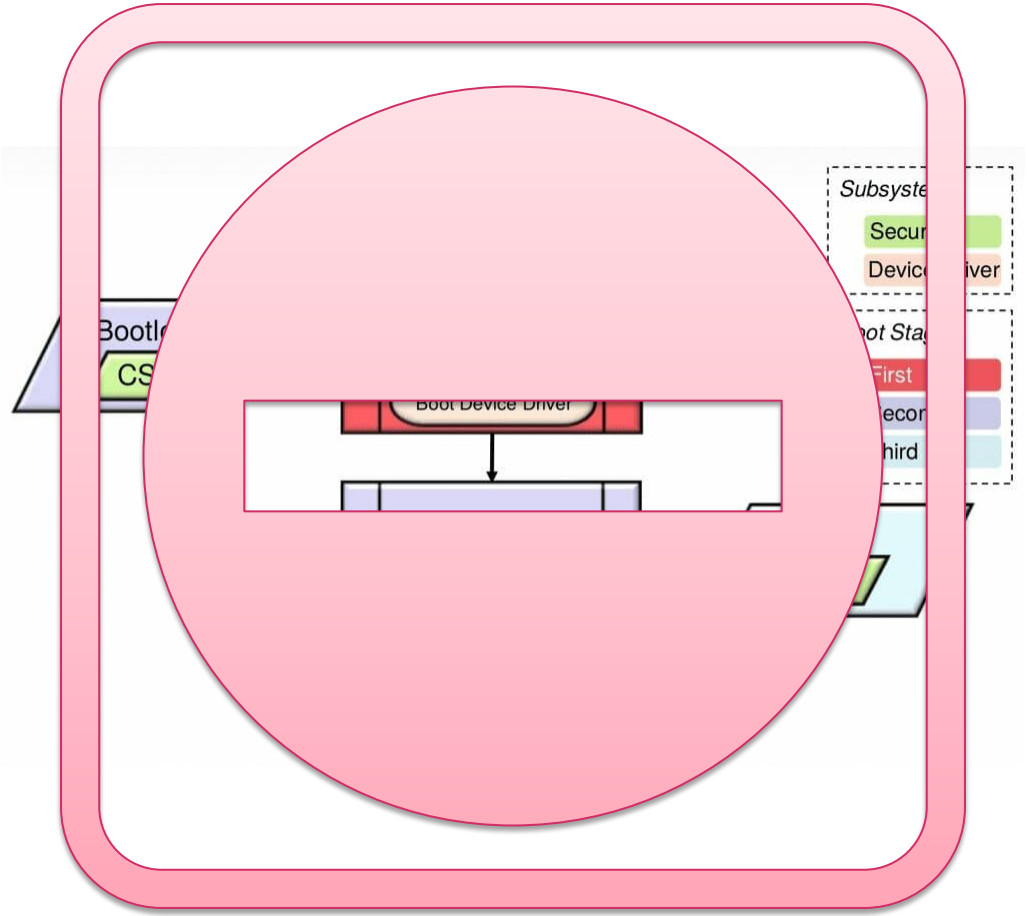
```
Setting breakpoint @ address 0x42000000, Size = 4, BPHandle = 0x0001
Starting target CPU...
ERROR: Bad JTAG communication: Write to IR: Expected 0x1, got 0x2
(TAP Command : 2) @ Off 0x5
```



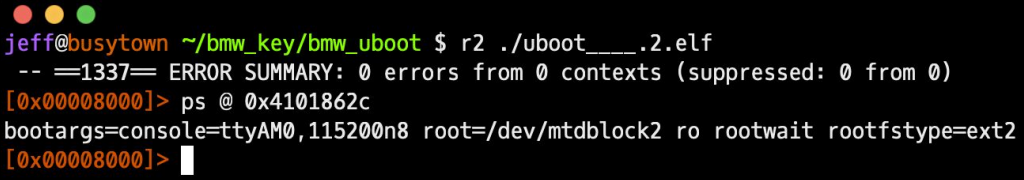
Cipher Block Chaining (CBC) mode encryption

```
$ strings firmware____.0.elf
33333
"""""
Battery is too low,need charging......(3.4V)
BATT:
Battery Voltage =
Error: tried to enable 5VCTRL ENABLE_DCDC before                        enabling DCDC4P2 ENABLE_DCDC.
Enabling of DCDC failed at setting of 5VCTRL ENABLE_DCDC.  The only 5V power supply operating is the linear regulators.
Enabling of DCDC failed at setting of                   DCDC4P2 ENABLE_DCDC.  Only 5V power supply                        operating is the linear regulators.
boot from battery. 5v input not detected
Chargeable battery detected but                                 the voltage is too low for battery                                      powered operation.Booting from 5V              power source.
No battery or bad battery                                       detected!!!.Disabling battery                                   voltage measurements./r/n
5v source detected.Valid battery                                voltage detected.Booting from battery                           voltage source.
PowerPrep start initialize power...
.shstrtab
.text0
.text78
.bss0
```


Reset
Subsystems
Security
Device Driver
Boot Stages
First
Second
Third
Bootloader
CSF
HAB Library
i.MX Boot ROM
Boot Device Driver
Bootloader
Boot Device Driver
OS
CSF
OS


Subsyste
Secur
Devic
iver
Bootl
CS
ot Sta
First
ecor
hird
Boot Device Driver

U-Boot


jeff@busytown ~/bmw_key/bmw_uboot $ r2 ./uboot____.2.elf
-- ==1337== ERROR SUMMARY: 0 errors from 0 contexts (suppressed: 0 from 0)
[0x00008000]> ps @ 0x4101862c
bootargs=console=ttyAM0,115200n8 root=/dev/mtdblock2 ro rootwait rootfstype=ext2
[0x00008000]>

```
113 export TSLIB_CALIBFILE='/etc/conf/pointercal'
114 export TSLIB_CONFFILE='/etc/ts.conf'
115 export TSLIB_FBDEVICE='/dev/fb0'
116 export TSLIB_ROOT='/usr/lib/ts/'
117 export TSLIB_TSDEVICE='/dev/input/event1'
118 export POINTERCAL_FILE='/etc/pointercal'
119
120 if [ -f "/etc/conf/pointercal" ]; then
121     `rm -r /etc/conf/pointercal`
122 fi
123
124 FTM=`cat /proc/cmdline | grep ftm`
125
126 #Copy Default RUNIN list to /Factory
127 file1=/factory/runinTest.list
128 file2=/etc/runinTest.list
129 file3=/factory/runinTest_HL_Temp.list
130 file4=/etc/runinTest_HL_Temp.list
131 if [ -f $file1 ]; then
132     echo "$file1 is exist"
133 else
134     echo "copy $file2 to $file1"
135     cp $file2 $file1
NORMAL  rcS                                   unix | utf-8 | sh   52%  124:1
[1:rcS ]
```

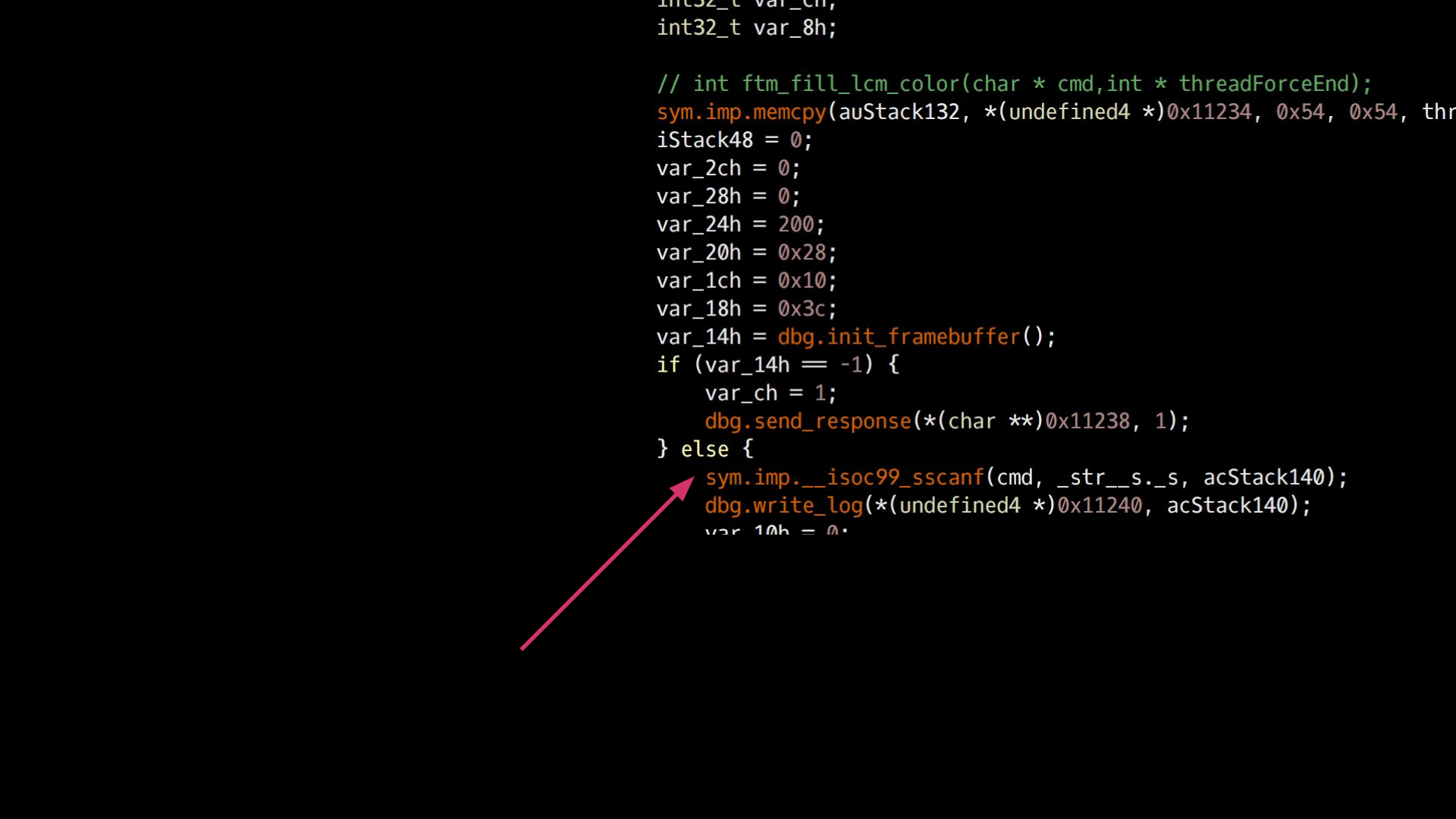
```
183     fi
184     USB=`cat /sys/class/power_supply/usb/online`
185
186     if [ "$USB" == "1" ]; then
187         modprobe g_serial #Normal USB Cable, do probe g_serial
188     fi
189
190     echo "mount /last_log..."
191     mount -t jffs2 /dev/mtdblock3 /last_log/
192     sleep 5
193     if [ "$USB" == "1" ]; then
194         echo "FTM USB Cable"
195         /bin/ftm & #FTM USB Cable,background execute FTM
196     else
197         echo "UART"
198         /bin/ftm   #UART, foregraound execute FTM
199     fi
200 fi
201
202 #fw_setenv check_boot_status 0 &  #For firmware recovery mode
203
204 # Init NFC
205 # /usr/bin/nfc_cardmode_PN65O.sh &   //Removed, due to change to UART1
V-LINE  rcS                                   unix | utf-8 | sh   82%  195:37
-- VISUAL LINE --                                                    1
```

```
jeff@busytown ~/bmw_key/bmw_fs/mounted $ file bin/ftm
bin/ftm: ELF 32-bit LSB executable, ARM, EABI5 version 1 (SYSV), dynamically linked, interpreter /lib/ld
-linux.so.3, for GNU/Linux 2.6.26, with debug_info, not stripped
jeff@busytown ~/bmw_key/bmw_fs/mounted $
```

```
void main(undefined4 argc)
{
    undefined4 *placeholder_3;
    undefined4 uVar1;
    int32_t iVar2;
    int64_t iVar3;
    undefined4 in_stack_fffffef0;
    char *in_stack_fffffef4;
    int32_t var_108h;
    int32_t var_104h;

    uVar1 = sym.serial_init();
    **(undefined4 **)0x9e04 = uVar1;
    iVar3 = sym.fih_spi_init();
    placeholder_3 = *(undefined4 **)0x9e08;
    if (iVar3 < 0) {
        uVar1 = 0;
        **(undefined4 **)0x9e08 = 0;
        sym.write_log(*(undefined4 *)0x9e0c, (int32_t)iVar3, 0, placeholder_3, in_stack_fffffef0, in_stack_fffffef4,
                      var_108h);
    } else {
        uVar1 = 1;
        **(undefined4 **)0x9e08 = 1;
    }
    sym.write_log(*(undefined4 *)0x9e14, **(undefined4 **)0x9e10, uVar1, **(undefined4 **)0x9e10, in_stack_fffffef0,
                  in_stack_fffffef4, var_108h);
    iVar2 = sym.wait_for_connected();
    if (**(char **)0x9e18 == '\0') {
        iVar2 = sym.imp.pthread_create(&stack0xfffffef4, 0, *(undefined4 *)0x9e1c, 0);
    }
    do {
        do {
            iVar2 = sym.get_loop_status(iVar2);
        } while (iVar2 != 0);
        if (**(int32_t **)0x9e20 == 1) {
            sym.serial_read(&var_108h);
            sym.chomp((char *)&var_108h);
            iVar2 = sym.parse_cmd((char *)&var_108h);
        }
    } while( true );
}
[0x00009d1c]>
```


[0x00009950]> 0x9950 # sym.wait_for_connected ();
[0x9950]
; CALL XREF from sym.monitor_usb_status_func @ 0x9cac
; CALL XREF from main @ 0x9d80
184: sym.wait_for_connected ();
; var char *s1 @ fp-0x108
; var int32_t var_8h @ fp-0x8
push {fp, lr}
add fp, sp, 4; /home/vagrant/dkey/base/movial/hw-test/ftm.c:176
sub sp, sp, 0x108; /home/vagrant/dkey/base/movial/hw-test/ftm.c:177
sub r3, fp, 8
mov r0, r3; /home/vagrant/dkey/base/movial/hw-test/ftm.c:178
mov r1, 0
; [0x9a08:4]=0x9824 sym.send_ready_func
ldr r2, [sym.send_ready_func]; /home/vagrant/dkey/base/movial/hw-test/ftm.c:180
mov r3, 0
bl sym.imp.pthread_create; /home/vagrant/dkey/base/movial/hw-test/ftm.c:181;[oa]
b 0x997c
0x997c [of]
; CODE XREF from sym.wait_for
sub r3, fp, 0x108
; void *arg1
mov r0, r3
bl sym.serial_read;[od]
sub r3, fp, 0x108; /home/vagr
; const char *s1
mov r0, r3
; const char *s2
; [0x29738:4]=0x204d5446
; "FTM Alive"
ldr r1, [str.FTM_Alive]; /home/vagrant/dkey/base/movial/hw-test/ftm.c:185
mov r2, 9
; int strncasecmp(const char *s1, const char *s2, size_t n)
bl sym.imp.strncasecmp;[oe]
mov r3, r0
cmp r3, 0
bne 0x9978; /home/vagrant/dkey/base/movial/hw-test/ftm.c:186
interactive!
t f
0x9978 [oc]
; CODE XREF from sym.wait_for_connected @ 0x99a4
mov r0, r0
0x99a8 [ok]
; [0x29744:4]=0x20627375
; "usb cable connected\n"
ldr r0, [str.usb_cable_connected]
bl sym.write_log;[og]
; [0x9a14:4]=0x38c08 obj.connected
ldr r3, [obj.connected]
mov r2, 1; /home/vagrant/dkey/base/movial/hw-test/ftm.c:194
str r2, [r3]; /home/vagrant/dkey/base/movial/hw-test/ftm.c:196
; 8
ldr r3, [var_8h]; /home/vagrant/dkey/base/movial/hw-test/ftm.c:200
mov r0, r3
mov r1, 0
bl sym.imp.pthread_join;[oh]
; [0x2975c:4]=0x76636552
; "Recv:\r\nusb cable connected\r\n"
ldr r0, [str.Recv:___usb_cable_connected]; /home/vagrant/dkey/base/movial/hw-test/f
bl sym.send_result; /home/vagrant/dkey/base/movial/hw-test/ftm.c:205;[oi]
bl sym.get_loop_status;[oj]
; 0x2975c
; "Recv:\r\nusb cable connected\r\n"
mov r3, r0; /home/vagrant/dkey/base/movial/hw-test/ftm.c:207
cmp r3, 0
bne 0x99f0
f t
0x99e4 [om]
mov r0, 0
mov r1, 0
bl sym.send_response; /home/vagrant/dkey/base/movial/hw-test/ftm.c:213;[ol]

```
[0x00010338]> pdg

// WARNING: Variable defined which should be unmapped: var_8h
// WARNING: [r2ghidra] Failed to match type __fd_mask[32] of member __fds_bits in struct type_0x7812

undefined4 ftm_fill_lcm_color(uint8_t *cmd, int32_t *threadForceEnd)
{
    undefined uVar1;
    undefined4 uVar2;
    int32_t iVar3;
    int32_t var_94h;
    char *format;
    char acStack140 [4];
    int32_t var_88h;
    undefined auStack132 [4];
    void *s2;
    int32_t iStack48;
    int32_t var_2ch;
    int32_t var_28h;
    int32_t var_24h;
    int32_t var_20h;
    int32_t var_1ch;
    int32_t var_18h;
    int32_t var_14h;
    int32_t var_10h;
    int32_t var_ch;
    int32_t var_8h;

    // int ftm_fill_lcm_color(char * cmd,int * threadForceEnd);
    sym.imp.memcpy(auStack132, *(undefined4 *)0x11234, 0x54, 0x54, threadForceEnd);
    iStack48 = 0;
    var_2ch = 0;
    var_28h = 0;
    var_24h = 200;
    var_20h = 0x28;
    var_1ch = 0x10;
    var_18h = 0x3c;
    var_14h = dbg.init_framebuffer();
    if (var_14h == -1) {
        var_ch = 1;
        dbg.send_response(*(char **)0x11238, 1);
    } else {
        sym.imp.__isoc99_sscanf(cmd, _str__s._s, acStack140);
        dbg.write_log(*(undefined4 *)0x11240, acStack140);
        var_10h = 0;
```


int32_t var_8h;
// int ftm_fill_lcm_color(char * cmd,int * threadForceEnd);
sym.imp.memcpy(auStack132, *(undefined4 *)0x11234, 0x54, 0x54, thr
iStack48 = 0;
var_2ch = 0;
var_28h = 0;
var_24h = 200;
var_20h = 0x28;
var_1ch = 0x10;
var_18h = 0x3c;
var_14h = dbg.init_framebuffer();
if (var_14h == -1) {
var_ch = 1;
dbg.send_response(*(char **)0x11238, 1);
} else {
sym.imp.__isoc99_sscanf(cmd, _str__s._s, acStack140);
dbg.write_log(*(undefined4 *)0x11240, acStack140);

stack bof!

- can it really be so simple?

ftm doesn't fork, one crash and you are dead

back to the drawing board

rebuild u-boot from source

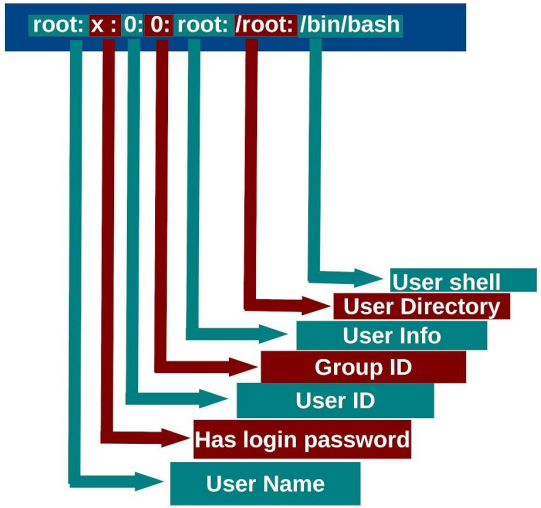
oh shit no support for this hardware

```
-               &pinctrl_regs->hw_pinctrl_emi_ds_ctrl_set);
+#ifndef CONFIG_SYS_MXS_mDDR
+       /* Set DDR2 mode */
+       writel(PINCTRL_EMI_DS_CTRL_DDR_MODE_DDR2,
+               &pinctrl_regs->hw_pinctrl_emi_ds_ctrl_set);
+#else
+       /* Set mDDR mode */
+       writel(PINCTRL_EMI_DS_CTRL_DDR_MODE_mDDR,
+               &pinctrl_regs->hw_pinctrl_emi_ds_ctrl_set);
+
+       writel( PINCTRL_EMI_DS_CTRL_ADDRESS_MA_MASK |
+               PINCTRL_EMI_DS_CTRL_CONTROL_MA_MASK |
+               PINCTRL_EMI_DS_CTRL_DUALPAD_MA_MASK |
+               PINCTRL_EMI_DS_CTRL_SLICE3_MA_MASK |
+               PINCTRL_EMI_DS_CTRL_SLICE2_MA_MASK |
+               PINCTRL_EMI_DS_CTRL_SLICE1_MA_MASK |
+               PINCTRL_EMI_DS_CTRL_SLICE0_MA_MASK,
+        &pinctrl_regs->hw_pinctrl_emi_ds_ctrl);
+
+       /* Configure Pins 0-15 as EMI pins */
+       writel(0, &pinctrl_regs->hw_pinctrl_muxsel10);
+       writel(0, &pinctrl_regs->hw_pinctrl_muxsel11);
+       writel(0, &pinctrl_regs->hw_pinctrl_muxsel12);
+       writel(0, &pinctrl_regs->hw_pinctrl_muxsel13);
+#endif

:
```

```
+
+static int do_spi_flash_dump(int argc, char *const argv[]) {
+       int ret = 1;
+       const loff_t len = 0x200;
+       unsigned long addr = 0x08000000;
+
+       char *buf = map_physmem(addr, len, MAP_WRBACK);
+       if (!buf && addr) {
+               puts("Failed to map physical memory\n");
+               return 1;
+       }
+
+       printf("Dumping %u bytes:", flash->size);
+
+       for(loff_t offset = 0; offset < flash->size; ) {
+               ret = spi_flash_read(flash, offset, len, buf);
+               if(ret) {
+                       continue;
+               }
+               for(int i = 0; i < len; i++) {
+                       putc2(buf[i]);
+               }
+               offset += len;
+       }
+       printf("End of dump\n");
+
:
```

```
+
 sources {
        u_boot_spl="spl/u-boot-spl.bin";
        u_boot="u-boot.bin";
 }

 section (0) {
-       load u_boot_spl > 0x0000;
-       load ivt (entry = 0x0014) > 0x8000;
+       load u_boot_spl > 0x1000;
+       load ivt (entry = 0x1044) > 0x8000;
        hab call 0x8000;

-       load u_boot > 0x40000100;
-       load ivt (entry = 0x40000100) > 0x8000;
+       load u_boot > 0x40002000;
+       load ivt (entry = 0x40002000) > 0x8000;
        hab call 0x8000;
 }
diff --git a/arch/arm/mach-imx/mxs/Kconfig b/arch/arm/mach-imx/mxs/Kconfig
index b90d7b6e41..40bd77fe89 100644
--- a/arch/arm/mach-imx/mxs/Kconfig
+++ b/arch/arm/mach-imx/mxs/Kconfig
@@ -63,16 +63,25 @@ config TARGET_TS4600
 config TARGET_XEA
        bool "Support XEA"
:
```

```
jeff@ubuntu:~/bmw/u-boot$ git status
On branch master
Your branch is up to date with 'origin/master'.

Changes not staged for commit:
  (use "git add <file>..." to update what will be committed)
  (use "git restore <file>..." to discard changes in working directory)
        modified:   Makefile
        modified:   arch/arm/cpu/arm926ejs/mxs/spl_boot.c
        modified:   arch/arm/cpu/arm926ejs/mxs/spl_mem_init.c
        modified:   arch/arm/cpu/arm926ejs/mxs/u-boot-imx28.bd
        modified:   arch/arm/mach-imx/mxs/Kconfig
        modified:   cmd/Kconfig
        modified:   cmd/Makefile
        modified:   cmd/sf.c
        modified:   drivers/mtd/spi/spi-nor-core.c
        modified:   drivers/serial/serial.c
        modified:   drivers/serial/serial_pl01x.c
        modified:   scripts/config_whitelist.txt

Untracked files:
  (use "git add <file>..." to include in what will be committed)
        1.diff
        :wq
        board/bmw/
        cmd-send.patch.1
        cmd/send.c
```



Untitled_0

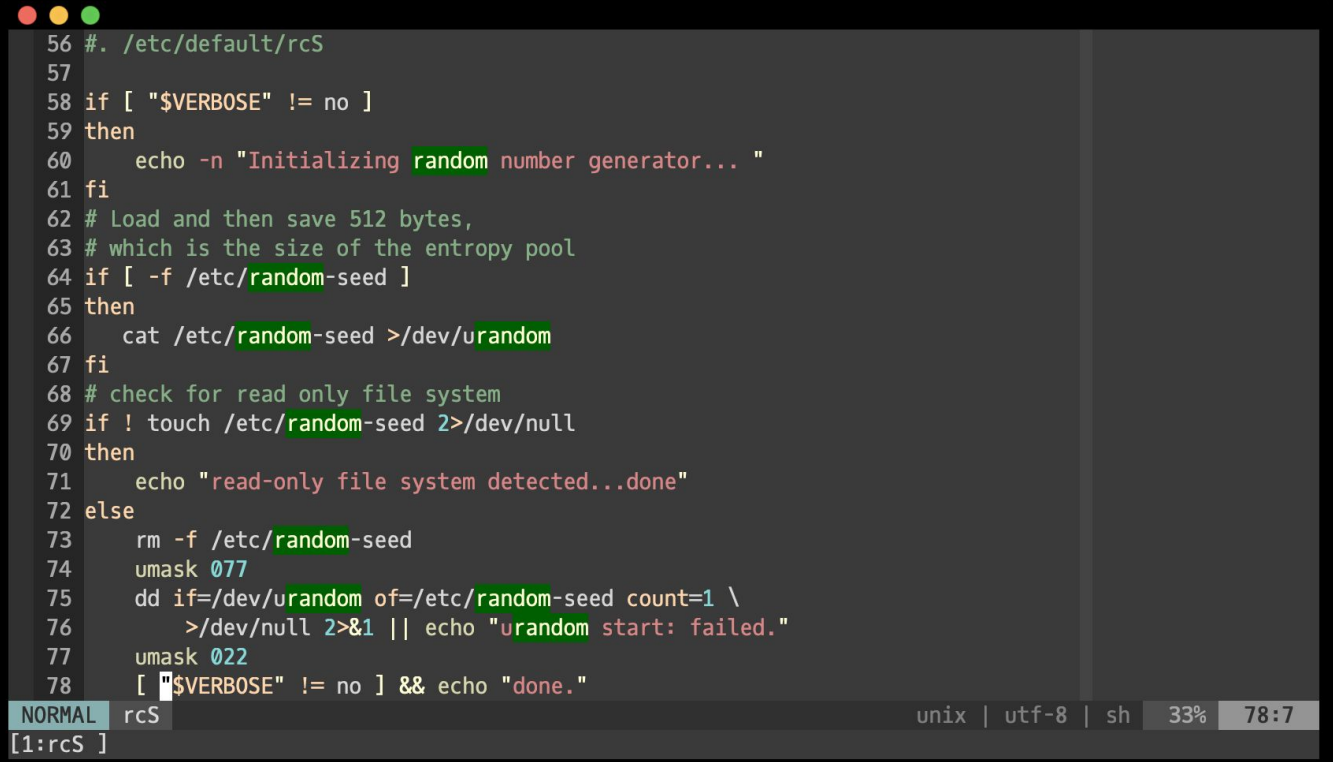
New Open Save Connect Disconnect Clear Data Options View Hex Help

```
(none) login:

Welcome to Buildroot

(none) login: root
Password:
Login incorrect
(none) login: root

Password:
Login incorrect
(none) login:

Login timed out after 60 seconds



Welcome to Buildroot

(none) login: root
Password:
#
# id
uid=0(root) gid=0(root) groups=0(root),10(wheel)
#
#
```

usbmodem143101 / 115200 8-N-1
Connected 00:00:08, 124 / 16 bytes

TX RX RTS CTS DTR DSR DCD RI


LIL' FLIP
713
GAME OVER (FLIP)
PARENTAL
ADVISORY
EXPLICIT CONTENT


#. /etc/default/rcS
if ["$VERBOSE" != no]
then
echo -n "Initializing random number generator... "
fi
Load and then save 512 bytes,
which is the size of the entropy pool
if [-f /etc/random-seed]
then
cat /etc/random-seed >/dev/urandom
fi
check for read only file system
if ! touch /etc/random-seed 2>/dev/null
then
echo "read-only file system detected...done"
else
rm -f /etc/random-seed
umask 077
dd if=/dev/urandom of=/etc/random-seed count=1 \
>/dev/null 2>&1 || echo "urandom start: failed."
umask 022
["$VERBOSE" != no] && echo "done."
NORMAL rcS
unix | utf-8 | sh 33% 78:7
[1:rcS]

```
[0x00000000]> px 512
- offset -   0 1  2 3  4 5  6 7  8 9  A B  C D  E F  0123456789ABCDEF
0x00000000  3401 1bc8 c908 e13b 656d 2f4d e919 a580  4......;em/M....
0x00000010  9482 f99c 72dc 05e1 a66b 54fc 5cde e6ad  ....r....kT.\...
0x00000020  4f64 6058 8d70 fd99 f3d8 39f9 3837 b0ec  Od`X.p....9.87..
0x00000030  85d8 a411 120e a096 493b c8eb cb0e 3897  ........I;....8.
0x00000040  b522 6679 2b88 485d 8707 e69a 9817 a4af  ."fy+.H]........
0x00000050  2f75 5fda 2e3d 774f 2e53 265c eaaf 8da5  /u_..=wO.S&\....
0x00000060  59a6 2941 2a1e 1ca1 13c5 84d5 36ae ad3f  Y.)A*.......6..?
0x00000070  765b 6ec7 4aab a854 fa3f 758f b1b3 7456  v[n.J..T.?u...tV
0x00000080  88ef 60d0 1dda 0cb8 35fd 0d33 a691 17a2  ..`.....5..3....
0x00000090  3d98 0bb0 44b0 bfc4 3e64 1f72 42df 6a3f  =...D...>d.rB.j?
0x000000a0  47af 45d0 42c8 1ce9 6128 23a5 0e48 156b  G.E.B...a(#..H.k
0x000000b0  1111 46b2 a5d1 bc1b 50a0 f56a b83e 2b65  ..F.....P..j.>+e
0x000000c0  d50c 172a b30b 12d9 848b e9ba a697 c420  ...*........... 
0x000000d0  61d8 9570 7317 4f47 ee71 7dd2 4dab a830  a..ps.OG.q}.M..0
0x000000e0  354a 4285 517b f7f8 4505 8154 df80 5299  5JB.Q{..E..T..R.
0x000000f0  ee61 d9ab 9445 6e81 26db 1448 6fdd b9c6  .a...En.&..Ho...
0x00000100  21f0 47e7 76bd 2c0a 0d77 4f83 d90e eb4e  !.G.v.,..wO....N
0x00000110  c7bb cfc4 12de 005d 5242 8fde 2026 9222  .......]RB.. &."
0x00000120  cdb1 cda5 dd36 b025 2bfb 268e 64d3 887a  .....6.%+.&.d..z
0x00000130  5eec 99f1 7e2d 22d6 60da 2da4 7b2a 79d8  ^...~-".`.-.{*y.
0x00000140  5dc2 c509 9f6d 8c21 9986 f626 fd4b 81be  ]....m.!...&.K..
0x00000150  f2c9 9c3b 6ed2 1898 cde8 f726 a796 dcf9  ...;n......&....
0x00000160  904b ffe8 7d06 6e07 3b77 f106 31e0 d297  .K..}.n.;w..1...
0x00000170  ccde 5c92 90fb fb64 7896 eaf7 6699 f887  ..\....dx...f...
0x00000180  cf50 8ac7 c1ff 93fe b532 46c3 43f7 2e10  .P.......2F.C...
0x00000190  7afd 788a 73ab 32cd f90b a97d 7453 cb73  z.x.s.2....}tS.s
0x000001a0  7604 2d80 a2fe 16ac 3284 d5c1 d861 9367  v.-.....2....a.g
0x000001b0  1d39 8920 50f8 ea4d 6eea 5ae8 bf4c b46f  .9. P..Mn.Z..L.o
0x000001c0  4e67 82a1 fdd3 df85 361b 5b46 c6ed c891  Ng......6.[F....
0x000001d0  b303 d53b 9574 159a 82a2 f05f bd8c 9279  ...;.t....._...y
0x000001e0  c7a7 64c7 8616 6d5b 719b cc6c 27b5 e64d  ..d...m[q..l'..M
0x000001f0  275e 894f fe3e 27aa 7566 9442 1a08 5d58  '^.O.>'.uf.B..]X
[0x00000000]>
```