

# Linux Firmware Debug Kit

A convenient way to debug HW code

***Merck Hung***  
COSCU 2009



# Merck Hung (洪豪謙)

現職於: ASUS (Cell Phone)

歷任於:

MiTAC (Linux Storage)

GIGA-BYTE (Linux & BIOS)

專長與興趣:

x86/ARM Bootloader, Linux Kernel & Driver  
, Operating System Development, and Android OS.

作品:

1. OluxOS (<http://sourceforge.net/projects/oluxkernel/>)
2. LFDK (<http://sourceforge.net/projects/lfdk/>)
3. Embedded Linux iSCSI/NAS (Undergoing to be Open Source)
4. Embedded Linux Bootloader resided in BIOS (Patent)

# OluxOS

```
QEMU
Copyright (C) 2006 - 2008, Olux Organization all rights reserved.
Olux Operating System version 0.1.0

Found SMBIOS AnchorString
Total Memory Size: 255 MB
E820: 0x00000000_00000000 - 0x00000000_0009FBFF <Memory>
E820: 0x00000000_0009FC00 - 0x00000000_0009FFFF <Reserved>
E820: 0x00000000_000E8000 - 0x00000000_000FFFFFF <Reserved>
E820: 0x00000000_00100000 - 0x00000000_0FFEFFFF <Memory>
E820: 0x00000000_0FFF0000 - 0x00000000_0FFFFFFF <ACPI>
E820: 0x00000000_FFFC0000 - 0x00000000_FFFFFFFF <Reserved>
Kernel PDE Pointer Addr = 0x00200000
Initialize Master i8259
Initialize Slave i8259
IntRegInterrupt: IRQ 0x0, Comm 0x101da0, Hw 0x101d20
IntRegInterrupt: IRQ 0x1, Comm 0x101db0, Hw 0x1015b0

OluxOS > _
```

# iSCSI/NAS

172.16.66.129 - lynx-dvt: MiTAC Filer Manager 1.0 - Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://172.16.66.129/cgi-bin/index.cgi

Google

- Filer
- Volumes
  - Add
  - Manage
- Aggregates
  - Add
  - Manage
  - Setup
- Storage
  - Disk
  - Adapters
    - Report
- CIFS
- NFS
- LUNs
  - Enable/Disable
  - Manage
  - Add
  - Initiators
  - iSCSI
    - Manage Names

### Add Aggregate

**RAID Level**  
Choose a level of RAID to assemble Disk aggregate.

RAID 5 - Parity

Aggregate Size : 256.00 MB

**Select Disks**  
Select disks to assemble a RAID Group.  
For RAID 2, 2 disks at least.  
For RAID 5, 3 disks at least.

sdc - VMware Virtual S 128.0  
sdk - VMware Virtual S 128.0  
sde - VMware Virtual S 128.0

<--

-->

sdi - VMware Virtual S 128.0  
sdj - VMware Virtual S 128.0  
sdd - VMware Virtual S 128.0  
sdl - VMware Virtual S 128.0  
sdf - VMware Virtual S 128.0  
sdm - VMware Virtual S 128.0  
sdg - VMware Virtual S 128.0  
sdn - VMware Virtual S 128.0

Create

Done

mlterm mlterm mlterm mlterm MSML - VM... 172.16.66... 10:22

# Linux Firmware Debug Kit

```
mterm
Linux Firmware Debug Kit 2.0.0pre Merck Hung <merckhung@gmail.com>
Vendor: Intel Corporation
Device: Mobile 4 Series Chipset Memory Controller Hub

0000 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F Refresh : ON
0000 36 80 40 2A 06 01 90 20 07 00 00 06 00 00 00 00
0010 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 Data Width : 8 bits
0020 00 00 00 00 00 00 00 00 00 00 00 00 AA 17 E0 20
0030 00 00 00 00 E0 00 00 00 00 00 00 00 00 00 00 00 VID:PID = 8086:2A40
0040 01 90 D1 FE 00 00 00 00 01 00 D1 FE 00 00 00 00 Rev ID : 07
0050 00 00 50 0B 59 00 00 00 00 00 00 00 00 00 00 00 Int Line (IRQ): 00
0060 01 00 00 E0 00 00 00 00 01 80 D1 FE 00 00 00 00 Int Pin : 00
0070 01 00 00 C2 00 00 00 00 01 10 00 00 00 00 00 00
0080 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 Mem: 00000000 00000000
0090 10 11 11 01 30 11 11 00 40 00 4E 00 00 1A 3B 00 Mem: 00000000 00000000
00A0 20 00 C0 13 00 00 00 00 00 00 00 00 00 00 00 00 Mem: 00000000 00000000
00B0 00 C0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 Mem: 00000000 00000000
00C0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 Mem: 00000000 00000000
00D0 00 00 00 00 00 00 00 00 00 00 00 00 70 02 00 00 Mem: 00000000 00000000
00E0 09 00 0A 11 88 64 00 1C 01 00 00 00 00 00 00 00
00F0 01 00 00 00 00 00 00 00 00 A0 0F 07 00 00 00 00 ROM: 00000000

Type: PCI Bus 00 Device 00 Function 00
(Q)uit (P)CI (M)emory (I)O (C)MOS 23:31:33
```



撰寫 **LFDK** 的動機 ??



# 撰寫 LFDK 的動機

1. 有鑒於 **BIOS** 的 **debug** 工具豐富



# 撰寫 LFDK 的動機

1. 有鑒於 **BIOS** 的 **debug** 工具豐富
2. 爲了盡量避免 **recompile code**





# 撰寫 LFDK 的動機

1. 有鑒於 **BIOS** 的 **debug** 工具豐富
2. 爲了盡量避免 **recompile code**
3. **Embedded Device** 速度較慢



# 撰寫 LFDK 的動機

1. 有鑒於 **BIOS** 的 **debug** 工具豐富
2. 爲了盡量避免 **recompile code**
3. **Embedded Device** 速度較慢
4. 吸引 **BIOS** 正妹的注意



使用 **LFDK** 的時機？



# Driver Code 其實區分

## 1. **Kernel Driver Facilities**

SpinLock, MutexLock, WorkQueue, KThread, .....

## 2. **Driver Subsystem**

Wi-Fi, SCSI, IDE, USB, I2C, SPI, .....

## 3. **HW Register Operation**

如何操作 **specific IC chip** 的暫存器.



# Debug 的方式

## 1. **Kernel Driver Facilities**

觀念弄清楚, printk, Remote KGDB, JTAG  
And Recompile the code

## 2. **Driver Subsystem**

經驗的累積, printk, Remote KGDB, JTAG  
And Recompile the code

## 3. 如何操作 **specific IC chip** 的暫存器.

SPEC.看更仔細, 推敲方法1, 2, 3, 4, 測試驗證  
And Recompile the code

# 推敲方法1, 2, 3, 4, 測試驗證

Step	LDN	Index	Value	Description
1	All	0x07h	<b>0x04h</b>	Select LDN to Environment registers, P.35
2	<b>0x04h</b>	0x30h	0x01h	Enable Environment Controller functions, P.55
3	<b>0x04h</b>	0x70h	0x0Ch	Select EC interrupt level to GPIO14, P.55
4	All	0x07h	<b>0x07h</b>	Select LDN to GPIO registers, P.36
5	All	0x2Bh	Value & 0xEFh	Unlock EC registers, P.45
6	All	0x2Ah	Value   0x10h	Enable GPIO14 multifunction, P.44
7	All	0x25h	Value   0x10h	Setup GPO14(EXTSMI) as General Purpose I/O 14, P.41
8	<b>0x07h</b>	0xB8h	Value   0x10h	Internal Pull-up GIPO14
9	<b>0x07h</b>	0xC0h	Value & 0xEFh	Set GPIO14 to Alternative function
10	<b>0x07h</b>	0xC8	Value   0x10h	Set GPIO14 to Output mode
11	<b>0x07h</b>	0xF4h	0x0Ch	Map SMI# Pin Location to GPIO14, P.64
12	<b>0x07h</b>	0xF1h	Value   0xC0h	Force Clear all SMI# status and set to level trigger, P.63
13	<b>0x07h</b>	0xF0h	Value   0x10h	Enable SMI# due to Environment Controller's IRQ, P.63



**Try & Error 要很久**  
**有沒有節省時間的方法呢？**



# YES

答案就是……



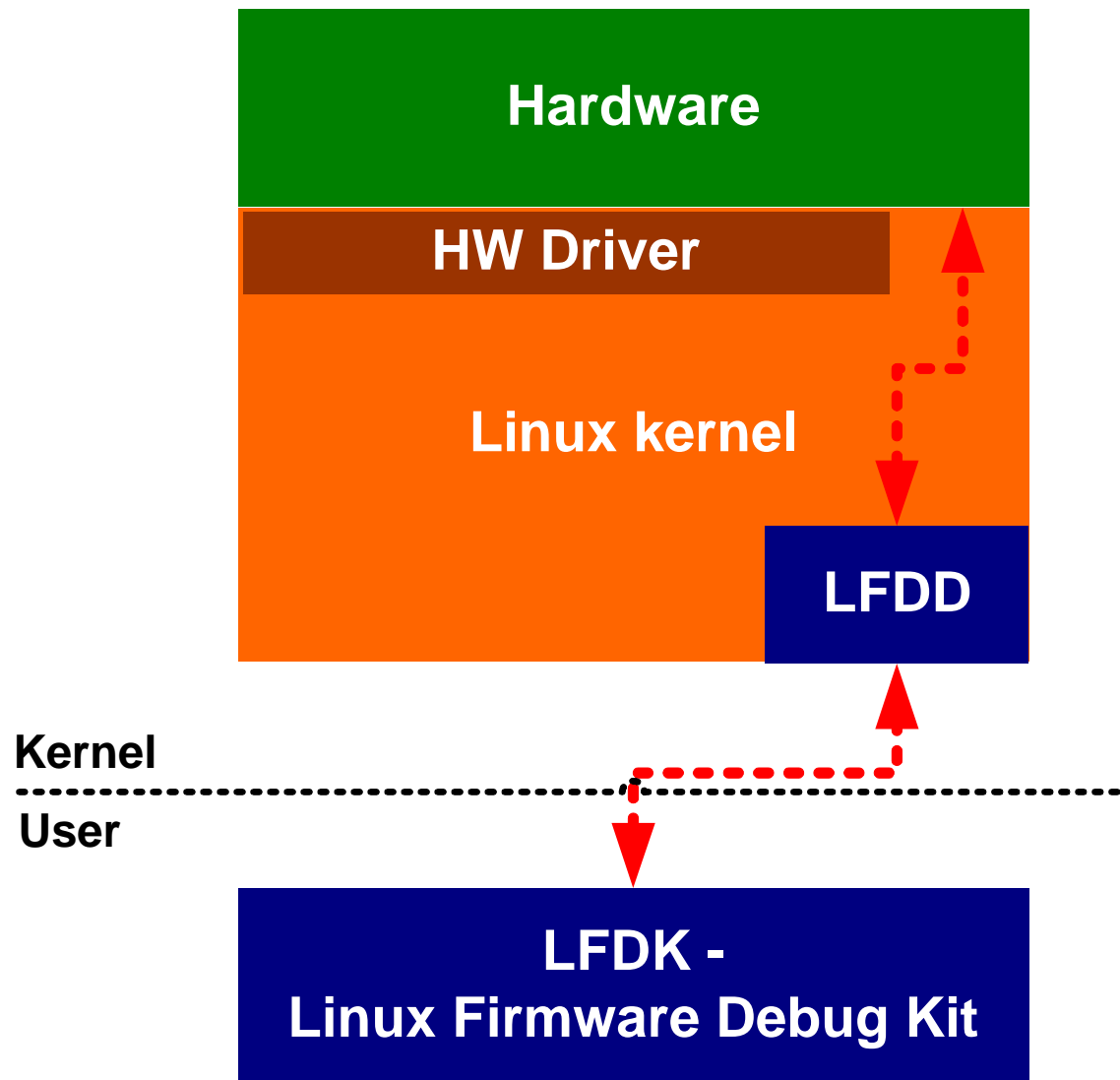
# Linux Firmware Debug Kit

```
mterm
Linux Firmware Debug Kit 2.0.0pre Merck Hung <merckhung@gmail.com>
Vendor: Intel Corporation
Device: Mobile 4 Series Chipset Memory Controller Hub

0000 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F Refresh : ON
0000 36 80 40 2A 06 01 90 20 07 00 00 06 00 00 00 00
0010 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 Data Width : 8 bits
0020 00 00 00 00 00 00 00 00 00 00 00 00 AA 17 E0 20
0030 00 00 00 00 E0 00 00 00 00 00 00 00 00 00 00 00 VID:PID = 8086:2A40
0040 01 90 D1 FE 00 00 00 00 01 00 D1 FE 00 00 00 00 Rev ID : 07
0050 00 00 50 0B 59 00 00 00 00 00 00 00 00 00 00 00 Int Line (IRQ): 00
0060 01 00 00 E0 00 00 00 00 01 80 D1 FE 00 00 00 00 Int Pin : 00
0070 01 00 00 C2 00 00 00 00 01 10 00 00 00 00 00 00 00
0080 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 Mem: 00000000 00000000
0090 10 11 11 01 30 11 11 00 40 00 4E 00 00 1A 3B 00 Mem: 00000000 00000000
00A0 20 00 C0 13 00 00 00 00 00 00 00 00 00 00 00 00 Mem: 00000000 00000000
00B0 00 C0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 Mem: 00000000 00000000
00C0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 Mem: 00000000 00000000
00D0 00 00 00 00 00 00 00 00 00 00 00 00 70 02 00 00 Mem: 00000000 00000000
00E0 09 00 0A 11 88 64 00 1C 01 00 00 00 00 00 00 00
00F0 01 00 00 00 00 00 00 00 00 A0 0F 07 00 00 00 00 ROM: 00000000

Type: PCI Bus 00 Device 00 Function 00
(Q)uit (P)CI (M)emory (I)O (C)MOS 23:31:33
```

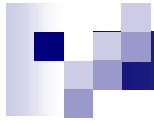
# Software Arch of LFDK





# DEMO

我一秒鐘都不能等!!!



**Thank you**

***Merck Hung***  
**COSCUP 2009**