Reverse Engineering Flash Memory for Fun and Benefit

Jeong Wook (Matt) Oh / 2014

oh@hp.com
oh.jeongwook@gmail.com
NAND Flash Memory is everywhere

NAND Flash is used in:

- USB Sticks
- Phones
- Cameras
- Embedded devices
- Smart appliances
- IoT
- …
Even in the POS devices at the grocery store...
The targeted device

CPU: ARM (S3C2410AL-20)

DRAMs

NAND Flash Memory
NAND Flash memory pins and names

1. R/B
2. RE
3. CE
4. Vcc
5. Vss
6. CLE
7. ALE
8. WE
9. WP
10. I/O7
11. I/O6
12. I/O5
13. I/O4
14. I/O3
15. I/O2
16. I/O1
17. I/O0
18. Vcc
19. Vss
De-soldering
Failed attempt – want to avoid de-soldering?

Pins essential to advanced operations are missing and other chips on the board may be woken up by the electric current supplied by the external device:

• This interferes with our custom operations
Failed attempt – want to use de-solder wire?

It’s tough to remove after de-soldering
Equipment & supplies

Use an SMT Rework station with a hot air blower:

- The solder alloy melts at around 180 to 190°C (360 and 370°F), but I recommend setting the temperature higher
- Use insulation tape to minimize heat damage
De-soldering

Apply heat over the pin area

• It usually takes 1 to 2 minutes to fully de-solder the chip
Too much heat?
Demo: The de-soldering process
FTDI FT2232H & NAND Flash Memory
Failed attempt – modding an SD reader
FTDI FT2232H breakout board

A chip for USB communication
- Provides USB 2.0 Hi-Speed (480Mb/s) to UART/FIFO IC

Note: Put female pin headers on each port extension
FTDI FT2232H breakout board

- ADBUS0-3 (16-19)
- ADBUS4-7 (21-24)
- ACBUS0-4 (26-30)
- ACBUS5-7 (32-34)
- BDBUS0-3 (38-41)
- BDBUS4-7 (43-46)
- BCBUS0 (48)
- BCBUS1-4 (52-55)
- BCBUS5-7 (57-59)
- PWREN# (60)
- EEDATA
- EECLK
- EECS
- VPHY
- VPLL
- VREGIN (50)
- VREGOUT (49)
- GROUND
- 3.3 V input
- 1.8 V Input
- AGND
- DM
- DP
- EEDATA
- EEC
- EEN
- EROS
- PWREN#
MCU Host Bus Emulation Mode

FTDI FT2232H supports multiple modes
• Use ‘MCU Host Bus Emulation Mode’ for this case

The FTDI chip emulates an 8048/8051 MCU host bus
## FT2232H commands

<table>
<thead>
<tr>
<th>Commands</th>
<th>Operation</th>
<th>Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x90</td>
<td>Read</td>
<td>8bit address</td>
</tr>
<tr>
<td>0x91</td>
<td>Read</td>
<td>16bit address</td>
</tr>
<tr>
<td>0x92</td>
<td>Write</td>
<td>8bit address</td>
</tr>
<tr>
<td>0x93</td>
<td>Write</td>
<td>16bit address</td>
</tr>
<tr>
<td>0x82</td>
<td>Set</td>
<td>High byte (BDBUS6, 7)</td>
</tr>
<tr>
<td>0x83</td>
<td>Read</td>
<td>High byte (BDBUS6, 7)</td>
</tr>
</tbody>
</table>

By sending commands and retrieving results, the software reads or writes bits through I/O lines.

- See FTDI’s [note](#) for more detail
Connection between FT2232H and NAND Flash Memory

The connections are mostly based on information from SpriteMod, but there is a slight modification between BDBUS6 and the CE (9) connection.
## Data lines

<table>
<thead>
<tr>
<th>FT2232H</th>
<th>Use</th>
<th>NAND Flash</th>
<th>Pin number</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ADBUS0</td>
<td>Bit0</td>
<td>I/O0</td>
<td>29</td>
<td></td>
</tr>
<tr>
<td>ADBUS1</td>
<td>Bit1</td>
<td>I/O1</td>
<td>30</td>
<td>DATA INPUT/OUTPUT</td>
</tr>
<tr>
<td>ADBUS2</td>
<td>Bit2</td>
<td>I/O2</td>
<td>31</td>
<td>Input command, address and data</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Output data during read operations</td>
</tr>
<tr>
<td>ADBUS3</td>
<td>Bit3</td>
<td>I/O3</td>
<td>32</td>
<td></td>
</tr>
<tr>
<td>ADBUS4</td>
<td>Bit4</td>
<td>I/O4</td>
<td>41</td>
<td></td>
</tr>
<tr>
<td>ADBUS5</td>
<td>Bit5</td>
<td>I/O5</td>
<td>42</td>
<td></td>
</tr>
<tr>
<td>ADBUS6</td>
<td>Bit6</td>
<td>I/O6</td>
<td>43</td>
<td></td>
</tr>
<tr>
<td>ADBUS7</td>
<td>Bit7</td>
<td>I/O7</td>
<td>44</td>
<td></td>
</tr>
</tbody>
</table>

**Low byte**
- 0x90,0x91,0x92,0x93 commands can be used to set values
## Data control lines

<table>
<thead>
<tr>
<th>FT2232H</th>
<th>Use</th>
<th>NAND Flash</th>
<th>Pin number</th>
<th>Description</th>
</tr>
</thead>
</table>
| ACBUS5  | Bit13 | WP | 19 | WRITE PROTECT  
Write operations fail when this is not high |
| ACBUS6  | Bit14 | CLE | 16 | COMMAND LATCH ENABLE  
When this is high, commands are latched into the command register through the I/O ports |
| ACBUS7  | Bit15 | ALE | 17 | ADDRESS LATCH ENABLE  
When this is high, addresses are latched into the address registers |

### High byte
- 0x91, 0x93 can be used to set values
## I/O and strobe lines

<table>
<thead>
<tr>
<th>FT2232H</th>
<th>Use</th>
<th>NAND Flash</th>
<th>Pin number</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>BDBUS6</td>
<td>I/O0</td>
<td>CE</td>
<td>9</td>
<td>CHIP ENABLE Low state means the chip is enabled.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>This pin indicates the status of the device operation. Low=busy, High=ready.</td>
</tr>
<tr>
<td>BDBUS7</td>
<td>I/O1</td>
<td>RB</td>
<td>7</td>
<td>READY/BUSY OUTPUT</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>This pin indicates the status of the device operation. Low=busy, High=ready.</td>
</tr>
<tr>
<td>BDBUS2</td>
<td>Serial Data In (RD#)</td>
<td>RE</td>
<td>8</td>
<td>READ ENABLE Serial data-out control. Enable reading data from the device.</td>
</tr>
<tr>
<td>BDBUS3</td>
<td>Serial Signal Out (WR#)</td>
<td>WE</td>
<td>18</td>
<td>WRITE ENABLE Commands, addresses and data are latched on the rising edge of the WE pulse.</td>
</tr>
</tbody>
</table>

- BDBUS6 (I/O0), BDBUS7 (I/O1) is controlled by the 0x83, 0x82 command
- RD#, WR# is connected to the RE, WE pin on NAND Flash
## Power lines

<table>
<thead>
<tr>
<th>Use</th>
<th>NAND Flash</th>
<th>Pin number</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>3v3</td>
<td>POWER</td>
<td>3v3</td>
<td>12</td>
</tr>
<tr>
<td>GND</td>
<td>GROUND</td>
<td>GND</td>
<td>13</td>
</tr>
<tr>
<td>3v3</td>
<td>POWER</td>
<td>3v3</td>
<td>36</td>
</tr>
<tr>
<td>GND</td>
<td>GROUND</td>
<td>GND</td>
<td>37</td>
</tr>
</tbody>
</table>

- Power lines
Read operation example

- CLE and ALE go high - the controller is sending commands and addresses
- The RE changes phases when page data is read from the NAND Flash chip
- The R/B line goes low during the busy state and back up to high when the NAND chip is ready
Basic command sets for usual NAND Flash memory (small blocks)

<table>
<thead>
<tr>
<th>Function</th>
<th>1st cycle</th>
<th>2nd cycle</th>
</tr>
</thead>
<tbody>
<tr>
<td>Read 1</td>
<td>00h/01h</td>
<td>-</td>
</tr>
<tr>
<td>Read 2</td>
<td>50h</td>
<td>-</td>
</tr>
<tr>
<td>Read ID</td>
<td>90h</td>
<td>-</td>
</tr>
<tr>
<td>Page Program</td>
<td>80h</td>
<td>10h</td>
</tr>
<tr>
<td>Block Erase</td>
<td>60h</td>
<td>D0h</td>
</tr>
<tr>
<td>Read Status</td>
<td>70h</td>
<td></td>
</tr>
</tbody>
</table>

There are more complicated commands available depending on the chipsets.

- The pins and other descriptions presented here are mostly focused on small block NAND Flash models (512 bytes of data with 16 bytes OOB)
- The model with a large block size uses a different set of commands, but the principle is the same
To read a page, it uses the Read 1 (00h, 01h) and Read 2 (50h) functions

To read a full page with OOB data from small block Flash memory, you need to read it 3 times:
- The 00h command is used to read the first half of the page data (A area)
- The 01h command is used to read the second half of the page data (B area)
- Finally, the 50h command is used to retrieve the OOB of the page (spare C area)
Read operation

<table>
<thead>
<tr>
<th></th>
<th>CLE</th>
<th>1</th>
<th>0</th>
</tr>
</thead>
<tbody>
<tr>
<td>ALE</td>
<td>0</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>R/B</td>
<td>1 (Ready)</td>
<td>R/B=0 (busy)</td>
<td>1 (Ready)</td>
</tr>
<tr>
<td>RE</td>
<td>1</td>
<td></td>
<td>Falling for each bytes</td>
</tr>
<tr>
<td>WE</td>
<td>Rising for each bytes</td>
<td></td>
<td>1</td>
</tr>
<tr>
<td>I/O0~7</td>
<td>00h/01h</td>
<td>Start Address</td>
<td>Data Output</td>
</tr>
<tr>
<td></td>
<td>50h</td>
<td>A0 – A7</td>
<td>A9 – A25</td>
</tr>
</tbody>
</table>

- CLE is set to high (1) when commands (00h, 01h, 50h) are passed
- ALE is set to high (1) when addresses are transferred
- R/B pin is set to low (0) when the chip is busy preparing the data

**RE and WE are used to indicate the readiness of the data operation on the I/O lines:**
- When the WE signal is rising, new bytes (command and address in this case) are sent to the I/O pins
- When the RE signal is falling, new bytes come from the NAND Flash memory chip if any data is available
1. First, the WE and CLE logic changes to send commands.
2. Next, the WE and ALE changes state to send addresses.
3. Finally, RE is used to signal the reading of each byte.
Reading a small block page

- NAND_CMD_READ0 (00h)
- NAND_CMD_READ1 (01h)
- NAND_CMD_READOOB (50h)

```python
self.sendCmd(self.NAND_CMD_READ0)
self.waitReady()
self.sendAddr(pageno<<8,self.AddrCycles)
self.waitReady()
bytes+=self.readData(self.PageSize/2)

self.sendCmd(self.NAND_CMD_READ1)
self.waitReady()
self.sendAddr(pageno<<8,self.AddrCycles)
self.waitReady()
bytes+=self.readData(self.PageSize/2)

self.sendCmd(self.NAND_CMD_READOOB)
self.waitReady()
self.sendAddr(pageno<<8,self.AddrCycles)
self.waitReady()
bytes+=self.readData(self.OOBSize)
```
Place your NAND Flash chip inside the TSOP48 socket:

- This socket is very useful
- Use it to directly interact with the extended pins and avoid touching and possibly damaging any Flash memory chip pins
NAND Flash reader/writer

You need an FTDI FT2232H breakout board, a USB cable, a TSOP48 socket and wires
DumpFlash – enhanced Flash reader/writer software

DumpFlash – Python implementation of Flash reader/writer software

- [https://github.com/ohjeongwook/DumpFlash](https://github.com/ohjeongwook/DumpFlash)
- Python implementation of original SpirteMod code and more
- Read/Write support
- Flash image manipulation tool (ECC, Bad block check)
- Fast sequential row read mode support
- More experimental code coming
- Automatic U-Boot image extraction
- JFFS2 parsing and extraction
- Uses enhanced schematics

Install prerequisite packages like `pyftdl` and `libusbx`.

- Pyftdi: a python wrapper around the FTDI library
- Libusbx: a library that provides USB level access to user applications
DumpFlash: Show basic information

With everything set up, you can query basic Flash information using the –i option
DumpFlash: Read data

You can also read raw data with the \(-r\) option.
It takes time to retrieve all the data depending on the size of the memory.
DumpFlash: Read data in sequential row read mode

DumpFlash supports sequential row read mode. Specify the –s option and it increases reading performance. Reading is 5-6 times faster than in normal page-by-page mode.
Demo: DumpFlash in action

Basic DumpFlash operations
Write operation pin states

<table>
<thead>
<tr>
<th>CLE</th>
<th>1</th>
<th>0</th>
<th>1</th>
</tr>
</thead>
<tbody>
<tr>
<td>ALE</td>
<td>0</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>R/B</td>
<td>1 (Ready)</td>
<td>R/B=0 (busy)</td>
<td>1 (Ready)</td>
</tr>
<tr>
<td>RE</td>
<td>1</td>
<td></td>
<td>Falling</td>
</tr>
<tr>
<td>WE</td>
<td>Rising for each bytes</td>
<td>1</td>
<td>Rising</td>
</tr>
<tr>
<td>I/O0~7</td>
<td>80h</td>
<td>Address Input A0 – A7 A9 – A25</td>
<td>Page + OOB data</td>
</tr>
</tbody>
</table>

The writing operation is done through sequence-in command (80h) and program command (10h):

- The read status command (70h) is used to retrieve the result of the write operation
- If I/O0 is 0, the operation was successful
Writing a small block page with spare C area
Writing data

After the command and address are sent, WE fluctuates repeatedly to send bytes.
Working with a bare metal image
### Page+OOB

<table>
<thead>
<tr>
<th>Offset (h)</th>
<th>00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F</th>
</tr>
</thead>
<tbody>
<tr>
<td>00000000</td>
<td>0F 00 00 EA 18 FO 9F ES 18 FO FO 0F ES 18 FO FO ES</td>
</tr>
<tr>
<td>00000010</td>
<td>18 FO 9F ES 18 FO ES 18 FO ES 18 FO ES 18 FO ES</td>
</tr>
<tr>
<td>00000020</td>
<td>18 FO 9F ES 00 00 00 00 00 00 00 00 00 00 00 00 00</td>
</tr>
<tr>
<td>00000030</td>
<td>00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00</td>
</tr>
<tr>
<td>00000040</td>
<td>00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00</td>
</tr>
<tr>
<td>00000050</td>
<td>00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00</td>
</tr>
<tr>
<td>00000060</td>
<td>00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00</td>
</tr>
<tr>
<td>00000070</td>
<td>00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00</td>
</tr>
<tr>
<td>00000080</td>
<td>00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00</td>
</tr>
<tr>
<td>00000090</td>
<td>00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00</td>
</tr>
<tr>
<td>000000A0</td>
<td>00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00</td>
</tr>
<tr>
<td>000000B0</td>
<td>00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00</td>
</tr>
<tr>
<td>000000C0</td>
<td>00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00</td>
</tr>
<tr>
<td>000000D0</td>
<td>00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00</td>
</tr>
<tr>
<td>000000E0</td>
<td>00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00</td>
</tr>
<tr>
<td>000000F0</td>
<td>00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00</td>
</tr>
</tbody>
</table>

#### ECC
- Bad Block Marker
- OOB Area
- Data

---

© Copyright 2014 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice.
ECC (Error Correction Code)

Failures occur with data on memory:
- A checksum can be useful to detect these errors

ECC (Error Correction Code) is a way to correct one bit of failure from a page:
- Besides detecting errors, ECC can correct them too (if they are minor)
- Uses the concept of Hamming code

Modern Flash memories use various ECC algorithms that have their roots in Hamming code:
- Even similar chipsets from the same vendor may have slightly different ECC algorithms
- Differences are generally minor (tweaks of XOR or shifting orders or methods)
- You need to figure out the correct algorithm to verify the validity of each page and to generate ECC
ECC calculation table

Representation of bits on a page with size of 512. Each bit is represented by a cell and each row is one byte. From this matrix, you can calculate various checksums across bits.
Example - P8' calculation

P8' checksum is calculated by XOR-ing all the bits in red
Example - P16' calculation

- Uses bits from byte[0], bytes[1], byte[4], byte[5] and so on until byte[508] and byte[509] for checksum calculation
- Other column checksums like P8, P16’, P16, P32’, P32, P2048’ and P2048 are calculated in the same manner
Code for calculating row checksums

```c
if (i & 0x01 == 0x01):
    p8 = xor_bit ^ p8
else:
    p8_ = xor_bit ^ p8_

if (i & 0x02 == 0x02):
    p16 = xor_bit ^ p16
else:
    p16_ = xor_bit ^ p16_

if (i & 0x04 == 0x04):
    p32 = xor_bit ^ p32
else:
    p32_ = xor_bit ^ p32_

if (i & 0x08 == 0x08):
    p64 = xor_bit ^ p64
else:
    p64_ = xor_bit ^ p64_

if (i & 0x10 == 0x10):
    p128 = xor_bit ^ p128
else:
    p128_ = xor_bit ^ p128_
```

```c
else:
    p128_ = xor_bit ^ p128_

if (i & 0x20 == 0x20):
    p256 = xor_bit ^ p256
else:
    p256_ = xor_bit ^ p256_

if (i & 0x40 == 0x40):
    p512 = xor_bit ^ p512
else:
    p512_ = xor_bit ^ p512_

if (i & 0x80 == 0x80):
    p1024 = xor_bit ^ p1024
else:
    p1024_ = xor_bit ^ p1024_

if (i & 0x100 == 0x100):
    p2048 = xor_bit ^ p2048
else:
    p2048_ = xor_bit ^ p2048_
```
Example - P2 calculation

The column checksums are calculated over the same bit locations over all the bytes in the page.

The picture shows how P2 can be calculated by taking bits 2,3,6,7 from each byte.
Row checksum calculation code

\begin{verbatim}
131  p1 = bit7 ^ bit5 ^ bit3 ^ bit1 ^ p1
132  p1_ = bit6 ^ bit4 ^ bit2 ^ bit0 ^ p1_
133  p2 = bit7 ^ bit6 ^ bit3 ^ bit2 ^ p2
134  p2_ = bit5 ^ bit4 ^ bit1 ^ bit0 ^ p2_
135  p4 = bit7 ^ bit6 ^ bit5 ^ bit4 ^ p4
136  p4_ = bit3 ^ bit2 ^ bit1 ^ bit0 ^ p4_
\end{verbatim}
### ECC calculation code

<table>
<thead>
<tr>
<th>Line</th>
<th>Code</th>
</tr>
</thead>
<tbody>
<tr>
<td>138</td>
<td>( \text{ecc0} = (p64 \ll 7) + (p64_ \ll 6) + (p32 \ll 5) + (p32_ \ll 4) + (p16 \ll 3) + (p16_ \ll 2) + (p8 \ll 1) + (p8_ \ll 0) )</td>
</tr>
<tr>
<td>139</td>
<td>( \text{ecc1} = (p1024 \ll 7) + (p1024_ \ll 6) + (p512 \ll 5) + (p512_ \ll 4) + (p256 \ll 3) + (p256_ \ll 2) + (p128 \ll 1) + (p128_ \ll 0) )</td>
</tr>
<tr>
<td>140</td>
<td>( \text{ecc2} = (p4 \ll 7) + (p4_ \ll 6) + (p2 \ll 5) + (p2_ \ll 4) + (p1 \ll 3) + (p1_ \ll 2) + (p2048 \ll 1) + (p2048_ \ll 0) )</td>
</tr>
</tbody>
</table>

You need to calculate 3 ECC values based on the checksums calculated.

The row and column checksum methods are very similar for different NAND Flash memory models, but ECC calculations tend to be slightly different across different models.
Bad blocks

• The notion of ‘bad blocks’ is a very generic concept that is also used with hard disk technology
• With Flash memory, if errors are more than the ECC can handle, the entire block is marked as bad
• Bad blocks are isolated from other blocks and are no longer used
• According to the ONFI standard, the first or last pages are used for marking bad blocks
Example bad block check routine

Some vendors use their own scheme for marking bad blocks:

- Ex) If the 6th byte from the OOB data of the first or second page for each block has non FFh values, it is recognized as a bad block (Samsung and Micron).

```python
def IsBadBlock(self, block):
    for page in range(0, 2):
        self.fd.seek(block_offset + self.PageSize + 5)
        bad_block_byte = self.fd.read(1)

        if not bad_block_byte:
            return self.ERROR

        if bad_block_byte == '\xff':
            return self.CLEAN_BLOCK

    return self.BAD_BLOCK
```
How a bad block is marked

Start of a bad block
Bad block marker ≠ 0xFF
OOB

© Copyright 2014 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice.
Demo: DumpFlash for ECC and bad block detections
Reverse engineering Flash memory data
An example of Flash memory layout

Usual structure of NAND Flash memory used for booting up embedded systems:
- The first block is always loaded to address 0x00000000
- When boot loading, code and U-Boot images are read only

The JFFS2 file system is used for read and write:
- When a file is saved, it goes to the JFFS2 file system
Low level initialization of the system

This boot loader does low level initialization:
- It loads up the next level boot loader

Note: The image I worked on showed very interesting strings, like the name of the 1st boot loader and some log messages
U-boot boot code

After the 1st stage boot loader, there is a next level boot loader that performs various, more complex operations:

- The kernel image and actual file system are placed inside
Custom boot code
U-Boot image header structure

The important value in retrieving the whole image file is the image length:
- The header size is 0x40 and the image length is 0x28A03B in this case. This makes total image size 0x28A07B.
U-Boot image disassembly

IDA doesn’t do well with multi-file images
Multi-file image

This image has two images inside it with lengths of 0x000E9118 and 0x001A0F17

```
U-Boot header

Multi-file image

1st image length
2nd image length
End of image length
```

```
readimage: # mkeimage -I Dump-00001800-UBOOT.dag
Image Name: Mx00004US 03.00 Qlf Alt
Created: Thu Jan 8 13:01:25 2009
Image Type: ARM Linux Multi-File image (uncompressed)
Data Size: 2658499 Bytes = 2630.06 kB = 2.54 MB
Load Address: 30108000
Entry Point: 30108000
Contents:
  Image 0: 95464B Bytes = 922.27 kB = 0.91 MB
  Image 1: 1707799 Bytes = 1687.77 kB = 1.59 MB
```
DumpFlash – Extracting U-Boot images

C:\mat\Analysis\WAND_Flash\DumpFlash>c:\python27\python DumpFlash.py -U
U-Boot Image found at block 0xc
Magic: 0x27051956
RCRC: 0xa85da14d
Time: 0x496669a5
Size: 0x28a03d
Load: 0x30108000
EP: 0x30108000
DCRC: 0x2975d991
OS: 0x5 (Linux)
Arch: 0x2 (ARM)
Type: 0x4 (Multi-File Image)
Comp: 0x0 (None)
Name: fx000400 03.00 01f Alt

Found multi image of length 0xe9118
Found multi image of length 0xda0f17
Extracting to U-Boot-00.dmp-00
Extracting to U-Boot-00.dmp-01
U-Boot Image found at block 0xcc
Magic: 0x27051956
RCRC: 0x2bbaced7
Time: 0x496669a6
Size: 0xe9118
Load: 0x30108000
EP: 0x30108000
DCRC: 0x2855374a
OS: 0x5 (Linux)
Arch: 0x2 (ARM)
Type: 0x2 (OS Kernel Image)
Comp: 0x0 (None)
Name: fx000400 03.00 01f

Extracting to U-Boot-01.dmp-00
Mounting RAMdisk image

When image 0 looks like a code file, image 1 has more interesting contents:

- You can identify that it is gzip compressed
- After decompression, if you run the `file` command on the file, it shows that the file is an ext2 file system file
Mounting RAMdisk image

After pushing the image, you can mount the MTD block device using the mount command and browse and modify the file.
mkimage information for the 2nd U-Boot image

IDA loads this image up without any issues. There are no hidden images.

- Unfortunately the code shown by IDA is the bootstrapping code that decompresses following the gzipped kernel image
- To identify the start of the kernel image, search for the gzip image magic value (0x8b1f)
Kernel image disassembly
Demo: Extracting and analyzing U-Boot code
JFFS2 erase marker location from a page and spare column bytes

Identifying the JFFS2 file system from the raw NAND Flash image is relatively easy. Usually JFFS2 puts specialized erasemarker inside the spare column of each page.

<table>
<thead>
<tr>
<th>Erasemaker</th>
<th>ECC</th>
<th>Bad block indicator</th>
<th>(FF=Clean)</th>
</tr>
</thead>
<tbody>
<tr>
<td>OOB</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

```
| O05E1A00 |  85 19 02 E0 46 00 00 00 96 33 FE 32 B1 00 00 00 | ...%1...-3p2... |
| O05E1A10 |  56 00 00 00 B6 21 00 00 00 00 00 00 00 00 00 00 | V...%1........... |
| O05E1A20 |  D7 50 0C 46 D7 50 0C 46 15 CF 05 53 00 00 00 00 | ..P..F.P..F..I.S. |
| O05E1A30 |  02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 | D..0..0...0.0...0 |
| O05E1A40 |  7C 61 97 98 03 04 FF FF 85 19 02 E0 44 00 00 00 | !a...-yy....A... |
| O05E1A50 |  1D FB FF 98 FB 04 00 00 54 00 00 00 ED 41 00 00 | .@...-...T...i... |
| O05E1A60 |  F4 01 01 00 00 00 00 00 B5 B1 27 47 B5 B1 27 47 | 0...-..u'Gu'G |
| O05E1A70 |  1C CF 05 53 00 00 00 00 00 00 00 00 00 00 00 00 | i..s..| |
| O05E1A80 |  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |  
| O05E1A90 |  44 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 | D...-..o'..o...S. |
| O05E1AAC |  ED 41 00 00 F4 01 01 00 00 00 00 00 00 00 00 00 | B5 B1 27 47 | |
| O05E1AB0 |  B5 B1 27 47 15 CF 05 53 00 00 00 00 00 00 00 00 00 00 | u'Gu'G.1.S. |
| O05E1AC0 |  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |  
| O05E1AD0 |  85 19 02 E0 CF 02 00 00 49 1E 2B A1 F1 02 00 00 | ...@...I...-... |
| O05E1AEO |  02 00 00 00 ED 81 00 00 00 00 00 00 00 00 00 00 00 | C8 02 00 00 | |
| O05E1AFO |  3A 00 00 00 3A 00 00 00 00 00 00 00 00 00 00 00 | ...@...I... |
| O05E1B00 |  BB 02 00 00 CB 02 00 00 00 00 00 00 00 00 00 00 00 | B8 12 12 D4 |
| O05E1B10 |  C5 EK 2D 1F 78 SE 32 68 68 62 6A 62 D4 64 B6 B6 |  |
| O05E1B20 |  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |  |
| O05E1B30 |  98 99 6A 6A 19 OC 54 OC 95 OC 0F 8F 8E 94 53 00 |  |
| O05E1B40 |  BD 05 97 7C 3F 80 D2 42 42 06 02 20 82 02 02 02 |  |
| O05E1B50 |  05 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |  |
| O05E1B60 |  38 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |  |
| O05E1B70 |  08 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |  |
| O05E1B80 |  08 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |  |
| O05E1B90 |  08 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |  |
| O05E1BA0 |  08 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |  |
| O05E1BB0 |  08 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |  |
| O05E1BC0 |  08 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |  |
| O05E1BD0 |  08 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |  |
| O05E1BE0 |  08 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |  |
| O05E1BF0 |  08 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |  |
| O05E1CG0 |  08 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |  |
```

68 © Copyright 2014 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice.
Mounting JFFS2 file system using a MTD

First, you need to create a MTD device:
  • Load related Linux kernel modules like mtdram, mtdblock and JFFS2. This creates a MTD device on the system.

After successful mounting, you can navigate and modify the file system on the fly.
Writing JFFS2 data

1. Dump mtdblock data to a file
   `dd if=/dev/mtdblock0 of=mtdblock0.dmp bs=512`

2. Program memory at JFFS2 location
   - `python DumpFlash.py -w -b 135 0xffffffff -O mtdblock0.dmp`
Demo: JFFS2 manipulation
After modifying the raw data and writing it back to the Flash memory, re-solder the chip:

• The re-soldering process is not very different from standard SMT soldering
• SMT was originally developed for the automatic soldering of PCB components
• The chips are usually small and the pitch of the pins is also relatively small
• Soldering these chips to the PCB manually is challenging, but not impossible
• There are many different methods, but I placed the chip on the pin location and heated the pins using the soldering iron
There are many pitfalls with SMT soldering and one of the big issues is bridging:

- The pitch for NAND flash TSOP48 model is 0.5 mm (which is extremely small). The solder can go over multiple pins and create shorts.

One of the big problems with re-soldering is possible damage to the board:

- Excessive heat is applied during de-soldering and it can damage the PCB board.
- Be extra careful when you re-solder the chips!
- Luckily, with Flash memory, many pins are not used. If the damaged patterns are not used, then the chips operate normally.
- Check with the chip datasheet to see if damaged patterns are used.
Demo: Re-soldering
Making a development board – TSOP48 socket
Making a development board – TSOP48 socket

Tough to solder manually on the board
Making a development board – the hack option
Flat flex cable to breakout board
Making a development board – the hack option
Making a development board - bidirectional
Tamper detection

FOR ORDERS, CONTACT:
EMAIL: 
ICQ: 

Full verifone kit, including full modified offline sof...

Advertisement from a modded POS device seller

Source: dailymotion
Tamper Detection
Tamper detection
Tamper detection
Tamper detection
Tamper detection
Tamper detection
Tamper detection
Does security by obscurity work?

The SDK is not publicly available
- To access the SDK, you need to have training (which is expensive)
- There is demand on the underground market for tampered devices

Does security by obscurity work here?
- Even without access to the SDK, it is possible to tamper with the device by directly accessing NAND flash memory
- The internal system is plain embedded Linux system, nothing special
- Do we really have a good way to detect tampered devices?
Conclusion

Interacting directly with Flash memory is useful when JTAG can’t be used:
• This is increasingly relevant as vendors obfuscate or remove JTAG interfaces to protect their intellectual property
• By directly interacting with the low level Flash memory interface, you can access data that sometimes can’t be retrieved otherwise
• USB stick low data investigations – do they clean up all remaining data when you format or erase the files?

The de-soldering method is referred to as destructive, but it is still possible to re-solder the chip to the system using SMT soldering methods:
• There is more chance of damaging the circuit board, but the chance of success is still high enough
Conclusion

There are many factors when extracting, modifying and reconstructing a bare metal image with your modification like ECC, bad blocks and JFFS2 erasemakers:

- You might try to modify code from many places like the boot loaders, the kernel or the JFFS2 root image

**Tamper detection can be sometimes security by obscurity:**

- Easily defeated by modifying software components
Credits

Original design of NAND reader/writer
   SpriteMod

NANDTool
   SpriteMod and Bjoern Kerlers