eMMC CHIPS. DATA RECOVERY BEYOND CONTROLLER

Rusolut
APPLICATIONS OF EMMC CHIPS

• SMARTPHONES
• TABLETS
• LAPTOPS
• VOICE RECORDERS
• CAMERAS
• MULTIMEDIA PLAYERS
• TV DECODERS
• INTERNET OF THINGS

...AND MUCH MORE...
DIFFERENT WAYS OF IMAGE EXTRACTION FROM DEVICES BASED ON EMMC CHIPS

LOGICAL EXTRACTION
- Image extracted from phone connected via cable

PHYSICAL EXTRACTION
- IN-SYSTEM PROGRAMMING (ISP)
- Image extracted from eMMC chip
- eMMC CHIP-OFF
- Image extracted from NAND memory of eMMC chip

eMMC-NAND ACCESS
- New standard
- Deepest depth of analysis
CLASSIC CHIP-OFF AND DATA EXTRACTION FROM eMMC CHIP

UNSOLDERING

CLEANING

PHYSICAL IMAGE EXTRACTION
EMMC vs RAW NAND CHIP-OFF DATA RECOVERY

NAND protocol

READ

eMMC protocol

READ
EMMC CHIP STRUCTURE

CONTROLLER

NAND MEMORY
WHY CARE ABOUT GETTING DATA VIA NAND FROM EMMC?

• DAMAGED EMMC CHIPS

• FACTORY RESET

• ERASED DATA RECOVERY
NAND MEMORY ADDRESSING AND R/W OPERATIONS

- Read Page
- Program (Write) Page
- Erase Block

Page is a smallest R/W unit
Block is a smallest Erase unit

Page size = 0.5 - 16 Kb
Block size = 128 Kb – 4 Mb
HOW DATA MODIFICATION PROCESS IS SUPPOSED TO WORK IN NAND MEMORY

1. READ PAGES
2. MODIFY DATA
3. ERASE BLOCK
4. PROGRAM (WRITE) PAGES
HOW DATA MODIFICATION PROCESS **ACTUALLY** WORKS IN NAND MEMORY

1. READ PAGES
2. MODIFY DATA
3. PROGRAM (WRITE) PAGES

OLD UNEARED BLOCK STAYS UNTOUCHED FOR SOME TIME UNTIL GARBAGE COLLECTION ALGORITHM ERASE IT. USUALLY IT’S NOT SO FAST PROCESS
LET’S TRY TO EXTRACT SOME **DELETED SMS** FROM THOSE “OVERWRITTEN” GARBAGE BLOCKS OF eMMC MEMORY VIA NAND INTERFACE.

TO MAKE THINGS WORSE LET’S **ERASE** EMMC CHIP!
THERE ARE SEVERAL STEPS...

• GAIN ACCESS TO NAND MEMORY OF eMMC CHIP

• EXTRACT PHYSICAL IMAGE OF NAND CHIP

• DECODE PHYSICAL IMAGE TO READABLE FORM

• CHECK IF THERE ARE STILL BLOCKS WITH “REMNANTS” IN THE DUMP (WE EXPECT TO SEE 0x00 IN THE WHOLE DUMP)

• SCAN DUMP USING SQLITE CARVING ALGORITHM TO FIND DELETED SMS

• ANALYSE RESULTS (WE EXPECT TO FIND NOTHING! USER’S DATA)
TECHNOLOGICAL PADS - NAND INTERFACE
NAND PINOUT ANALYSIS

- XRAY PCB LAYOUT ANALYSIS WITH FURTHER WIRE BONDING ANALYSIS OF NAND AND CONTROLLER

- NAND AND CONTROLLER PINOUT ANALYSIS THROUGH PCB LAYER REMOVAL

- CLASSIC “MAN IN THE MIDDLE ATTACK” USING LOGIC ANALYZER CONNECTED BETWEEN CONTROLLER AND NAND MEMORY
DELAYED EMMC CHIP
NAND PINOUT

DATA BUS

CONTROL SIGNALS
CONNECT CHIP TO ADAPTER
VISUAL NAND RECONSTRUCOR – THE NEW MODE FOR EMMC-NAND ACCESS
ADAPTER ASSEMBLY

eMMC chip level
Insert chip into reader by means of adapter

Model: NVMT0000L3
Vendor: Samsung
Capacity: 16 GB

Adapter assembly

PCI
Samsung BGA 180 #1 (PCB.3)

Frame
Samsung BGA 180 #1 (18.5x13)

Assembled adapter

Socket
Samsung BGA 180 #1
DATA SCRAMBLERS OF FLASH CONTROLLERS

DATA (FROM INTERFACE)\n\n$0x\text{BEEFBEF}$\n\n$\text{XOR}$\n\n$0xE417AE0C$\n\n$\text{SEED}$\n\n$0 1 1 0 0 0 0 1$\n\nLFSR-BASED GENERATOR\n\nRANDOMIZED DATA (TO NAND MEMORY)\n\n$0x5AF810E3$
LOGICAL IMAGE RECONSTRUCTION
REMEMBER WE ZEROED THIS DEVICE? WE EXPECT TO SEE 0x00 IN EVERY SECTOR/PAGE. BUT WHAT WE ACTUALLY SEE IS A BIT DIFFERENT:

- AFTER 1st ERASE CYCLE ~5% OF BLOCKS WEREN’T ERASED
- AFTER 2nd ERASE CYCLE ~1% OF BLOCKS WEREN’T ERASED
SMS CARVING

THE MOST INTERESTING PART. ARE THERE REALLY ANY MESSAGES?
RAW CARVING RESULTS
<table>
<thead>
<tr>
<th>№</th>
<th>Статус</th>
<th>Папка</th>
<th>Дата и время</th>
<th>Отправитель</th>
<th>Сообщение</th>
<th>Источник</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>SMS</td>
<td>Inbox</td>
<td>08/06/2013 11:17:42 PM</td>
<td>+7928937709</td>
<td>абонент +7928937709 свядал позвонил в сет 08/06/2013 в 17:17. Вы можете позвонить ему.</td>
<td>Сенер</td>
</tr>
<tr>
<td>2</td>
<td>SMS</td>
<td>Inbox</td>
<td>08/06/2013 9:36:15 AM</td>
<td>+79514982624</td>
<td>Эта абонент пытался вам позвонить</td>
<td>Сенер</td>
</tr>
<tr>
<td>3</td>
<td>SMS</td>
<td>Inbox</td>
<td>07/06/2013 18:35:29 PM</td>
<td>LiderRostov</td>
<td>Вас отнадят беляя нерас N S&amp;Podrobnya informacija ob uslovijah za polato - <a href="http://www.podpolato.ru">www.podpolato.ru</a></td>
<td>Сенер</td>
</tr>
<tr>
<td>4</td>
<td>SMS</td>
<td>Inbox</td>
<td>07/06/2013 18:35:29 PM</td>
<td>Tele2</td>
<td>Собака 10% в РП вил по вашему персональному коду 1812 т. 222,223.</td>
<td>Сенер</td>
</tr>
<tr>
<td>5</td>
<td>SMS</td>
<td>Inbox</td>
<td>07/06/2013 18:22:26 PM</td>
<td>RED Mail</td>
<td>Этот абонент пытался вам позвонить</td>
<td>Сенер</td>
</tr>
<tr>
<td>6</td>
<td>SMS</td>
<td>Inbox</td>
<td>07/06/2013 18:22:26 PM</td>
<td>+79514982624</td>
<td>пожалуйста не уходя все будет подумано</td>
<td>Сенер</td>
</tr>
<tr>
<td>7</td>
<td>SMS</td>
<td>Inbox</td>
<td>07/06/2013 18:22:26 PM</td>
<td>+79514982624</td>
<td>Люблю как обычно!</td>
<td>Сенер</td>
</tr>
<tr>
<td>8</td>
<td>SMS</td>
<td>Inbox</td>
<td>07/06/2013 18:11:00 AM</td>
<td>EGO</td>
<td>ЗАКАЗ — НОВОГО ОБЕЗДОПИСАНИЯ ОДНОЙ ВЕЩИ — 25% ДВОЙНОЙ В ПОДАРОК</td>
<td>Сенер</td>
</tr>
<tr>
<td>9</td>
<td>SMS</td>
<td>Inbox</td>
<td>07/06/2013 18:11:00 AM</td>
<td>Tele2</td>
<td>ЗАКАЗ — НОВОГО ОБЕЗДОПИСАНИЯ ОДНОЙ ВЕЩИ — 25% ДВОЙНОЙ В ПОДАРОК</td>
<td>Сенер</td>
</tr>
<tr>
<td>10</td>
<td>SMS</td>
<td>Inbox</td>
<td>07/06/2013 18:11:00 AM</td>
<td>+79514982624</td>
<td>Я тобу новой!</td>
<td>Сенер</td>
</tr>
<tr>
<td>11</td>
<td>SMS</td>
<td>Inbox</td>
<td>07/06/2013 18:11:00 AM</td>
<td>+79514982624</td>
<td>ты мне больше не милый..до крайней мере живешь...изи что этот день насталет</td>
<td>Сенер</td>
</tr>
<tr>
<td>12</td>
<td>SMS</td>
<td>Inbox</td>
<td>07/06/2013 18:11:00 AM</td>
<td>+79514982624</td>
<td>ОБЕЗДОПИСАНИЯ ОДНОЙ ВЕЩИ — 25% ДВОЙНОЙ В ПОДАРОК</td>
<td>Сенер</td>
</tr>
</tbody>
</table>
OUR THEORY IS PROVED. BUT NOBODY WANTS TO ERASE eMMC CHIP IN REAL LIFE.

WE CAN POSSIBLY GET MORE DATA FROM EVERY eMMC VIA NAND PROTOCOL?!
**SMS RECOVERY FROM 10 SMARTPHONES (SAME MODEL)**

<table>
<thead>
<tr>
<th></th>
<th>Source</th>
<th>SMS count</th>
<th>Comparison</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>NAND</td>
<td>116</td>
<td>283%</td>
</tr>
<tr>
<td></td>
<td>eMMC</td>
<td>41</td>
<td>100%</td>
</tr>
<tr>
<td>F</td>
<td>NAND</td>
<td>47</td>
<td>247%</td>
</tr>
<tr>
<td></td>
<td>eMMC</td>
<td>19</td>
<td>100%</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>Source</th>
<th>SMS count</th>
<th>Comparison</th>
</tr>
</thead>
<tbody>
<tr>
<td>B</td>
<td>NAND</td>
<td>2377</td>
<td>99.75%</td>
</tr>
<tr>
<td></td>
<td>eMMC</td>
<td>2383</td>
<td>100%</td>
</tr>
<tr>
<td>G</td>
<td>NAND</td>
<td>96</td>
<td>74%</td>
</tr>
<tr>
<td></td>
<td>eMMC</td>
<td>129</td>
<td>100%</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>Source</th>
<th>SMS count</th>
<th>Comparison</th>
</tr>
</thead>
<tbody>
<tr>
<td>C</td>
<td>NAND</td>
<td>4866</td>
<td>103%</td>
</tr>
<tr>
<td></td>
<td>eMMC</td>
<td>4723</td>
<td>100%</td>
</tr>
<tr>
<td>H</td>
<td>NAND</td>
<td>105</td>
<td>525%</td>
</tr>
<tr>
<td></td>
<td>eMMC</td>
<td>20</td>
<td>100%</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>Source</th>
<th>SMS count</th>
<th>Comparison</th>
</tr>
</thead>
<tbody>
<tr>
<td>D</td>
<td>NAND</td>
<td>118</td>
<td>144%</td>
</tr>
<tr>
<td></td>
<td>eMMC</td>
<td>82</td>
<td>100%</td>
</tr>
<tr>
<td>I</td>
<td>NAND</td>
<td>244</td>
<td>94%</td>
</tr>
<tr>
<td></td>
<td>eMMC</td>
<td>260</td>
<td>100%</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>Source</th>
<th>SMS count</th>
<th>Comparison</th>
</tr>
</thead>
<tbody>
<tr>
<td>E</td>
<td>NAND</td>
<td>6753</td>
<td>71%</td>
</tr>
<tr>
<td></td>
<td>eMMC</td>
<td>9464</td>
<td>100%</td>
</tr>
<tr>
<td>J</td>
<td>NAND</td>
<td>1540</td>
<td>131%</td>
</tr>
<tr>
<td></td>
<td>eMMC</td>
<td>1174</td>
<td>100%</td>
</tr>
</tbody>
</table>

Green blocks (A,C,D,F,H,J) – more SMS were found in NAND memory chip.

Red blocks (B,E,G,I) – less SMS were found in NAND memory chip due to uncorrectable bit errors caused by threshold voltage shifts (eMMC controller handles it) during read operation.
DATA RECOVERY FROM DAMAGED EMMC CHIPS

RETRIEVAL OF DELETED TEXT MESSAGES, CHATS, ETC. THROUGH NAND PROTOCOL INCLUDING GARBAGE BLOCKS ON DEEPER LEVEL THAT IS NOT ACCESSIBLE FOR CLASSIC MOBILE FORENSIC TOOLS

DATA RECOVERY AFTER FACTORY RESET OR OTHER OPERATIONS THAT ERASE DATA

Related links:
https://belkasoft.com/ssd-2016-part2