Smart TV Forensics

A. Boztas
M. Roeloffs

A. Boztas@holmes.nl
M. Roeloffs@holmes.nl

25 March 2015
Agenda

• The NFI
• Introduction
• Material and methods
• Data acquisition
• Data analysis
• Future
• Conclusion
Introduction
Introduction

Research questions:

• *Can a Smart TV be a key component in a digital forensic investigation?*

• *Is it possible to acquire data from a Smart TV?*

• *Can a Smart TV contain relevant data?*
Material and Methods

- Literature study
- Selection Smart TV
- Data acquisition
- Data analysis
  - System information and settings
  - Apps
  - Web browsing
  - Photo and multimedia files
  - External media
  - Cloud services
  - Channel information

Click Distribution by LCD-TV Manufacturer (Q4 2011-Q4 2012)

Source: Idealo
Data Acquisition: NFI Memory Toolkit

- Chip-off
- De-soldering of eMMC chip
- Read out with
- NFI Memory Toolkit II
- This method works on almost all embedded devices, the problem after chip-off is crypto.
Data Acquisition: the Five-Wire Method

- More and more embedded systems use eMMC chips
- eMMC is roughly the same as an MMC card
- Only three signals + Power Supply required to read
- Controller, a disk image is created, no rough copy of NAND
Data Acquisition: the Five-Wire Method
Data Acquisition: the Five-Wire Method

Does not work yet.
Probably because there are also other chips which start-up and draw current.
Can do it with many other devices
Data Acquisition: App

- Smart TVs are ordinary computers
- Often work with Linux operating system
- Rooting
Data Acquisition: App

• SamyGO forum on the Internet
• Many opportunities for "rooting"
• Possible to use Smart TV as a BitTorrent client, etc.
Data Acquisition

The Five-Wire Method
   Quick Method, more research is needed, repeatable
Chip-off
   Takes longer time, repeatability is getting better
App
   Fast method, but does not work on all firmware
Removable Soldered Memory

Test device now equipped with removable media by using a BGA adapter.
FILE SYSTEM ANALYSIS
File System Analysis

Squashfs
  • Read-only
  • Software of Samsung Open Source Release Center
  • Adjustment image authentication and compression

Samsung eMMC
  • Samsung chip oriented file system
  • Like a BTRFS variant, journaling, snapshotting
    • Magic `1eMMCFS`

Partition redundancy
  • Some partitions have the same size
  • Used to reset software
## File System Analysis

<table>
<thead>
<tr>
<th>flash_device_name</th>
<th>flash_device_size</th>
<th>flash_image_name</th>
<th>flash_upgrade_type</th>
<th>flash_partition_map</th>
<th>flash_mount_path</th>
</tr>
</thead>
<tbody>
<tr>
<td>/dev/mmcblk0p0</td>
<td>524288</td>
<td>onboot.bin</td>
<td>OTHER</td>
<td>BOOTLOADER0</td>
<td>NONE</td>
</tr>
<tr>
<td>/dev/mmcblk0p1</td>
<td>524288</td>
<td>u-boot.bin</td>
<td>NONE</td>
<td>BOOTLOADER1</td>
<td>NONE</td>
</tr>
<tr>
<td>/dev/mmcblk0p2</td>
<td>524288</td>
<td>secos.bin</td>
<td>USER</td>
<td>SECOS0</td>
<td>NONE</td>
</tr>
<tr>
<td>/dev/mmcblk0p3</td>
<td>524288</td>
<td>secos.bin</td>
<td>USER</td>
<td>SECOS1</td>
<td>NONE</td>
</tr>
<tr>
<td>/dev/mmcblk0p4</td>
<td>0</td>
<td>ex_partition</td>
<td>NONE</td>
<td>NONE</td>
<td>NONE</td>
</tr>
<tr>
<td>/dev/mmcblk0p5</td>
<td>524288</td>
<td>seret.bin</td>
<td>USER</td>
<td>SERETO</td>
<td>NONE</td>
</tr>
<tr>
<td>/dev/mmcblk0p6</td>
<td>524288</td>
<td>seret.bin</td>
<td>USER</td>
<td>SERET1</td>
<td>NONE</td>
</tr>
<tr>
<td>/dev/mmcblk0p7</td>
<td>7340032</td>
<td>ulimage</td>
<td>USER</td>
<td>KERNEL0</td>
<td>NONE</td>
</tr>
<tr>
<td>/dev/mmcblk0p8</td>
<td>5767168</td>
<td>rootfs.img</td>
<td>USER</td>
<td>RFS0</td>
<td>NONE</td>
</tr>
<tr>
<td>/dev/mmcblk0p9</td>
<td>7340032</td>
<td>ulimage</td>
<td>USER</td>
<td>KERNEL1</td>
<td>NONE</td>
</tr>
<tr>
<td>/dev/mmcblk0p10</td>
<td>5767168</td>
<td>rootfs.img</td>
<td>USER</td>
<td>RFS1</td>
<td>NONE</td>
</tr>
<tr>
<td>/dev/mmcblk0p11</td>
<td>8192</td>
<td>sign0.bin</td>
<td>NONE</td>
<td>SECUREMAC0</td>
<td>NONE</td>
</tr>
<tr>
<td>/dev/mmcblk0p12</td>
<td>8192</td>
<td>sign1.bin</td>
<td>NONE</td>
<td>SECUREMAC1</td>
<td>NONE</td>
</tr>
<tr>
<td>/dev/mmcblk0p13</td>
<td>8192</td>
<td>VD-HEADER</td>
<td>NONE</td>
<td>NONE</td>
<td>NONE</td>
</tr>
<tr>
<td>/dev/mmcblk0p14</td>
<td>3145728</td>
<td>NONE</td>
<td>NONE</td>
<td>mtd_drmregion_a</td>
<td>mtd_exu</td>
</tr>
<tr>
<td>/dev/mmcblk0p15</td>
<td>3145728</td>
<td>NONE</td>
<td>NONE</td>
<td>mtd_drmregion_b</td>
<td>mtd_exu</td>
</tr>
<tr>
<td>/dev/mmcblk0p16</td>
<td>157286400</td>
<td>NONE</td>
<td>NONE</td>
<td>mtd_rwarea</td>
<td>mtd_exu</td>
</tr>
<tr>
<td>/dev/mmcblk0p17</td>
<td>367001600</td>
<td>exe.img</td>
<td>USER</td>
<td>EXE0</td>
<td>mtd_exu</td>
</tr>
<tr>
<td>/dev/mmcblk0p18</td>
<td>367001600</td>
<td>exe.img</td>
<td>USER</td>
<td>EXE1</td>
<td>mtd_exu</td>
</tr>
<tr>
<td>/dev/mmcblk0p19</td>
<td>419430400</td>
<td>rocommon.img</td>
<td>USER</td>
<td>CONTENT0</td>
<td>mtd_rocommon</td>
</tr>
<tr>
<td>/dev/mmcblk0p20</td>
<td>419430400</td>
<td>rocommon.img</td>
<td>USER</td>
<td>CONTENT1</td>
<td>mtd_rocommon</td>
</tr>
<tr>
<td>/dev/mmcblk0p21</td>
<td>104857600</td>
<td>emanual.img</td>
<td>OTHER</td>
<td>NONE</td>
<td>mtd_emanual</td>
</tr>
<tr>
<td>/dev/mmcblk0p22</td>
<td>157286400</td>
<td>NONE</td>
<td>NONE</td>
<td>NONE</td>
<td>mtd_contents</td>
</tr>
<tr>
<td>/dev/mmcblk0p23</td>
<td>104857600</td>
<td>NONE</td>
<td>NONE</td>
<td>NONE</td>
<td>mtd_swu</td>
</tr>
<tr>
<td>/dev/mmcblk0p24</td>
<td>1870979072</td>
<td>rwcommon.img</td>
<td>OTHER</td>
<td>NONE</td>
<td>mtd_rwcommon</td>
</tr>
</tbody>
</table>
Data Analysis: System and Network Information

- Device name
- Connected devices
- Network information
- Smart functionalities
Data Analysis: System and Network Information

• System information:
  • Serial number
  • Model
  • Brand
  • Unique ID
  • etc.

• Network information:
  • Information about network name
  • IP-addresses
  • Bluetooth devices
  • MAC-address
Data Analysis: Apps

- Facebook
- Twitter
- YouTube, etc.
Data Analysis: Apps

• Name
• Date
• Screenshots
• User related information
## Data Analysis: Apps

<table>
<thead>
<tr>
<th>Name</th>
<th>Date Modified</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>FB</td>
<td>24-09-2014 16:02</td>
<td>File folder</td>
</tr>
<tr>
<td>TW</td>
<td>24-09-2014 16:02</td>
<td>File folder</td>
</tr>
<tr>
<td>Y2B</td>
<td>24-09-2014 16:02</td>
<td>File folder</td>
</tr>
</tbody>
</table>

- 100001756376377_637236553011551
- 100001756376377_637236553011551 Dieter Baar
- 100002591493138_591328540963524 Å–Jan Peter
- 100007871257058_1405149866424042
Data Analysis: Apps

```
"widgetname": "Facebook", "vendor": "Samsung",
"install_date": "Wed, 19 May 2010 15:57:57+0900",
account_id": null, "login_token": null, "external_cp_app"
": true, "sso_id": "test@hotmail.com",
"is_logged_in": false, "is_installed": true, "is_activated": true
,"is_init_state": true, "is_latest_version": true,
"installed_version": "1.18128", "widget_type": null,
name": "Twitter", "widgetname": "Twitter",
"vendor": "Samsung", "install_date": "Sat, 13 Mar 2010 11:31:03
+0900",
```
Data Analysis: Web Browsing

• Visited websites
• Web history
• Information about search machines
• Bookmarks
• Cookies
• etc.
Data Analysis: Web Browsing

settings.db located in p24/webkit/WebBrowser.

- SQLite database
- Contains 14 tables

Relevant tables:
- FullBrowserHistory:
- fullBrowser_HiddenHistory:
- fullBrowser_Bookmark:
- fullBrowser_Search:
# Data Analysis: Web Browsing

<table>
<thead>
<tr>
<th>URL</th>
<th>Title</th>
<th>EnterTime</th>
<th>DeviceName</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="http://nl.msn.com/?pc=SMTV">http://nl.msn.com/?pc=SMTV</a></td>
<td>Hotmail, Messenger</td>
<td>1970-01-01</td>
<td>Local</td>
</tr>
<tr>
<td><a href="http://www.google.nl/">http://www.google.nl/</a></td>
<td>Google</td>
<td>1970-01-01</td>
<td>Local</td>
</tr>
<tr>
<td><a href="http://www.google.com/">http://www.google.com/</a></td>
<td>Google</td>
<td>1970-01-01</td>
<td>Local</td>
</tr>
<tr>
<td><a href="http://www.facebook.com/">http://www.facebook.com/</a></td>
<td>Facebook</td>
<td>1970-01-01</td>
<td>Local</td>
</tr>
<tr>
<td><a href="http://www.youtube.com/">http://www.youtube.com/</a></td>
<td>YouTube</td>
<td>1970-01-01</td>
<td>Local</td>
</tr>
<tr>
<td><a href="http://www.youtube.com/watch?v=CU4NFfR7sRg">http://www.youtube.com/watch?v=CU4NFfR7sRg</a></td>
<td>Kampilen - Soufiane</td>
<td>1970-01-01</td>
<td>Local</td>
</tr>
<tr>
<td><a href="http://www.amazon.com/">http://www.amazon.com/</a></td>
<td>Amazon.com: Online</td>
<td>1970-01-01</td>
<td>Local</td>
</tr>
</tbody>
</table>
Data Analysis: Picture and Multimedia Files

- The file .CM.db located in p22
- SQLite database
- Contains 20 tables
- Information about audio, pictures and video files
- When files are opened, played etc.

Relevant tables:
- PhotoTable
- MusicTable
- VideoTable
- FileTable
- p22/RecentlyPlayed contains files with .mta extension.
Data Analysis: Picture and Multimedia Files

<table>
<thead>
<tr>
<th>TITLE</th>
<th>DATE</th>
<th>HEIGHT</th>
<th>MAKER</th>
</tr>
</thead>
<tbody>
<tr>
<td>IMG_0376</td>
<td>1404734357</td>
<td>2448</td>
<td>iPhone 5s</td>
</tr>
<tr>
<td>IMG_0371</td>
<td>1404734281</td>
<td>2448</td>
<td>iPhone 5s</td>
</tr>
<tr>
<td>IMG_0380</td>
<td>1404734417</td>
<td>2448</td>
<td>iPhone 5s</td>
</tr>
<tr>
<td>IMG_0378</td>
<td>1404734390</td>
<td>2448</td>
<td>iPhone 5s</td>
</tr>
<tr>
<td>IMG_0374</td>
<td>1404734292</td>
<td>2448</td>
<td>iPhone 5s</td>
</tr>
<tr>
<td>IMG_0369</td>
<td>1404734269</td>
<td>2448</td>
<td>iPhone 5s</td>
</tr>
<tr>
<td>IMG_0373</td>
<td>1404734288</td>
<td>2448</td>
<td>iPhone 5s</td>
</tr>
<tr>
<td>IMG_0375</td>
<td>1404734356</td>
<td>2448</td>
<td>iPhone 5s</td>
</tr>
<tr>
<td>IMG_0368</td>
<td>1404734256</td>
<td>2448</td>
<td>iPhone 5s</td>
</tr>
<tr>
<td>IMG_0372</td>
<td>1404734390</td>
<td>2448</td>
<td>iPhone 5s</td>
</tr>
<tr>
<td>IMG_0377</td>
<td>1404734379</td>
<td>2448</td>
<td>iPhone 5s</td>
</tr>
<tr>
<td>IMG_0370</td>
<td>1404734277</td>
<td>2448</td>
<td>iPhone 5s</td>
</tr>
</tbody>
</table>
Data Analysis: External Media Artifacts

- Device0013.db located in p22
- SQLite database
- Contains one table TABLE_DEVID
- Information about USB flash drives
Data Analysis: TV Channels

- p16/map-AirA, map-AirD, map-CableA, map-CableD, map-SateD
- p22/.EPG.db; SQLite database and contain Electronic Program Guide
- Due to time constraints not further investigated
Data Analysis: Cloud services

- URL
- Pictures
- Videos
- Username
- etc.,

![Data Analysis Table]

<table>
<thead>
<tr>
<th>url</th>
<th>stamp</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="https://www.dropbox.com/ajax_captcha_login">https://www.dropbox.com/ajax_captcha_login</a></td>
<td>1357005907</td>
</tr>
<tr>
<td><a href="http://noticefile.samsungcloudsolution.com/Front/NoticeAll?co">http://noticefile.samsungcloudsolution.com/Front/NoticeAll?co</a></td>
<td>1404998892</td>
</tr>
<tr>
<td><a href="https://www.dropbox.com/1/oauth/authorize?oauth_token=">https://www.dropbox.com/1/oauth/authorize?oauth_token=</a></td>
<td>1405000446</td>
</tr>
<tr>
<td><a href="https://www.dropbox.com/home">https://www.dropbox.com/home</a></td>
<td>1405001971</td>
</tr>
<tr>
<td><a href="https://www.dropbox.com/1/oauth/authorize?oauth_token=">https://www.dropbox.com/1/oauth/authorize?oauth_token=</a></td>
<td>1405002037</td>
</tr>
<tr>
<td><a href="https://www.dropbox.com/1/oauth/authorize?oauth_token=">https://www.dropbox.com/1/oauth/authorize?oauth_token=</a></td>
<td>1357005770</td>
</tr>
</tbody>
</table>
Conclusion

• A Smart TV is actually a computer and can be investigated with the same forensic toolset
• Acquiring data is possible
• A Smart TV can contain relevant data
• Relevant information is usually saved in SQLite databases
• Malicious users can abuse a Smart TV for viewing child pornography, communication, botnet, etc.
Future

• Further investigation of the five-wire method
• Investigate other makes and models Smart TV
• Extensive data analysis research
• Develop an app for acquiring data
• Make memory dump
• Analyse network activity
Questions