



Netherlands Forensic Institute
Ministry of Security and Justice

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:

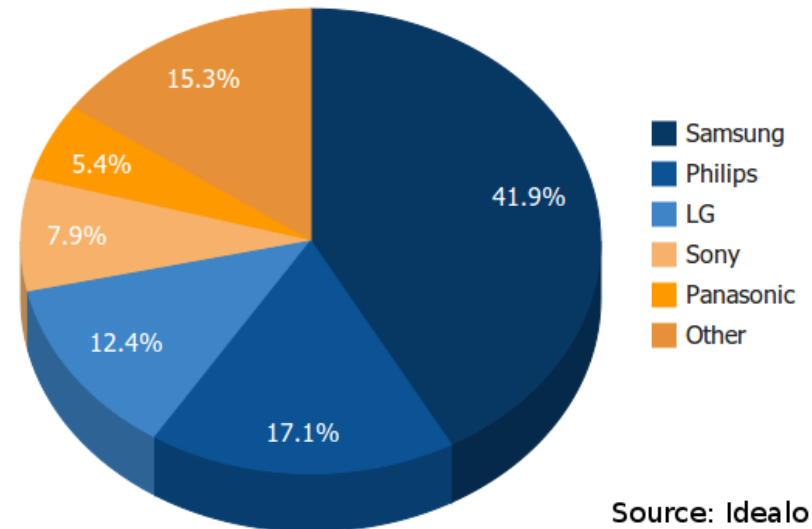
- *Can a Smart TV be a key component in a digital forensic investigation?*
- *Is it possible to acquire data from a Smart TV?*
- *Can a Smart TV contain relevant data?*



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

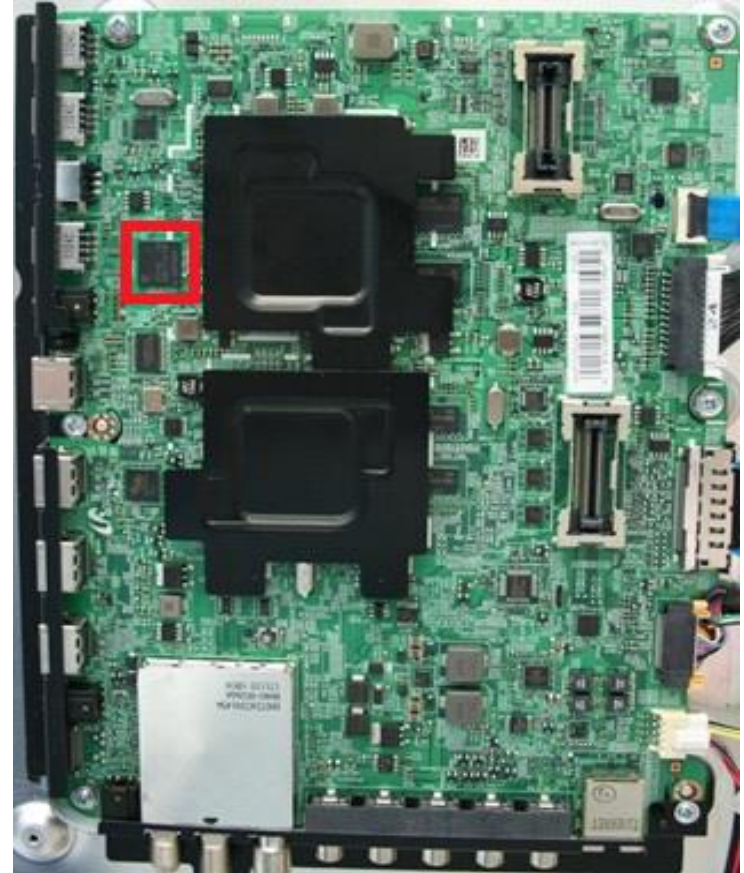
Click Distribution by LCD-TV Manufacturer (Q4 2011-Q4 2012)





Data Acquisition: NFI Memory Toolkit

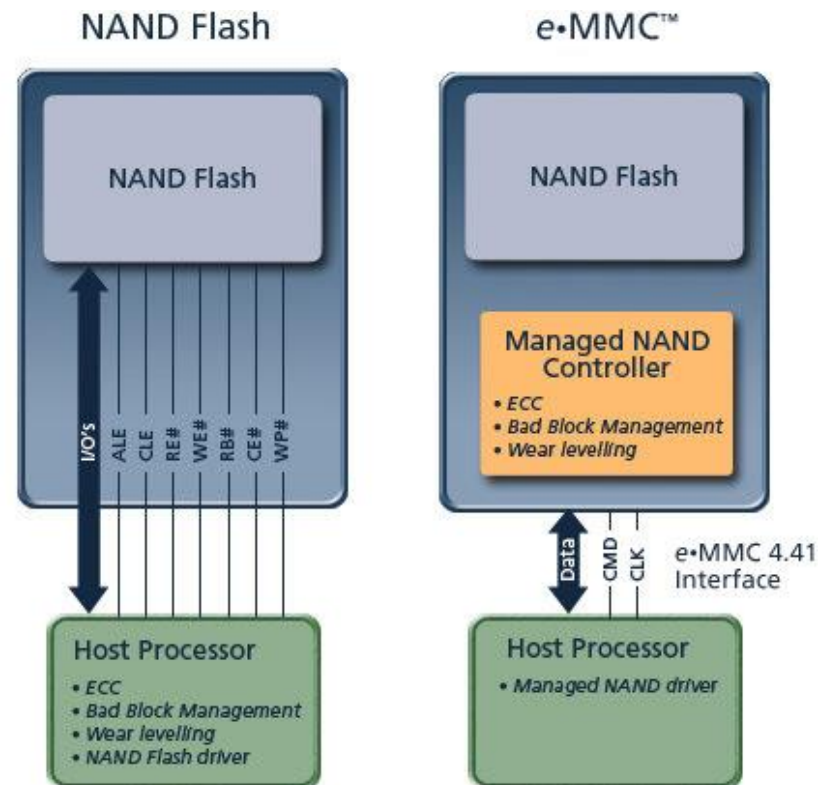
- Chip-off
- De-soldering of eMMC chip
- Read out with
- NFI Memory Toolkit II
- This method works on almost all embedded devices, the problem after chip-off is crypto.





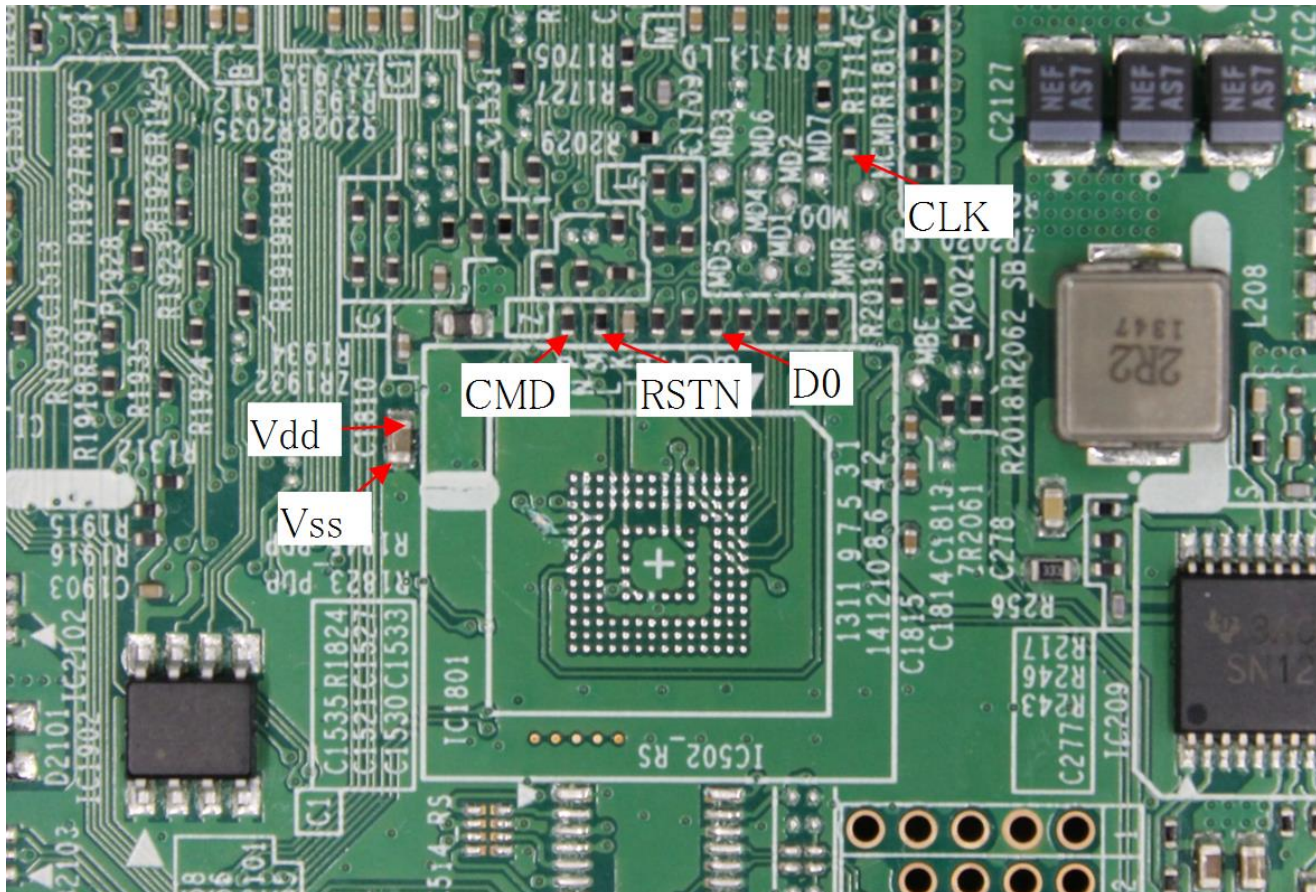
Data Acquisition: the Five-Wire Method

- 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

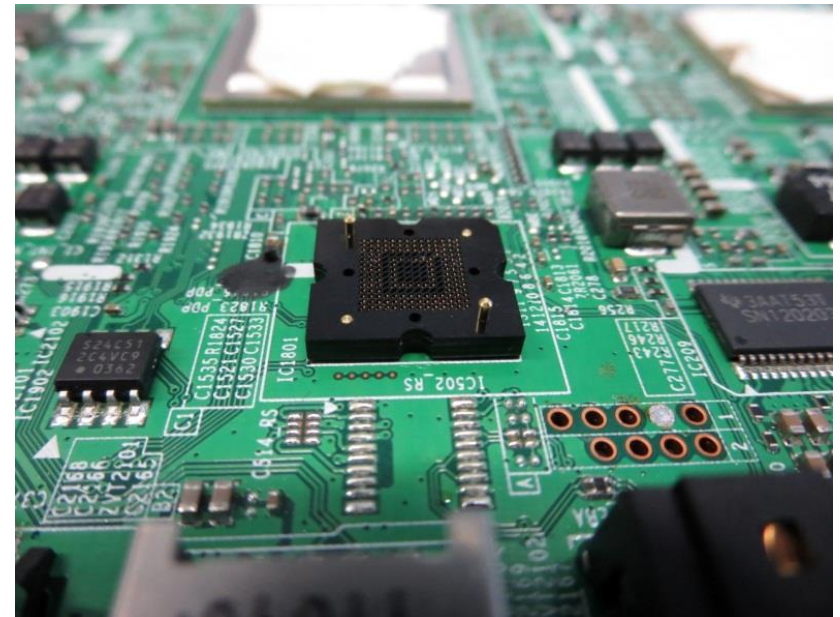
App

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

| flash_device_name | flash_device_size | flash_image_name | flash_upgrade_type | flash_partition_map | flash_mount_path |
|-------------------|-------------------|------------------|--------------------|---------------------|------------------|
| /dev/mmcblkOp0 | 524288 | onboot.bin | OTHER | BOOTLOADER0 | NONE |
| /dev/mmcblkOp1 | 524288 | u-boot.bin | NONE | BOOTLOADER1 | NONE |
| /dev/mmcblkOp2 | 524288 | secos.bin | USER | SECOSO | NONE |
| /dev/mmcblkOp3 | 524288 | secos.bin | USER | SECOS1 | NONE |
| /dev/mmcblkOp4 | 0 | ex_partition | NONE | NONE | NONE |
| /dev/mmcblkOp5 | 524288 | seret.bin | USER | SERETO | NONE |
| /dev/mmcblkOp6 | 524288 | seret.bin | USER | SERET1 | NONE |
| /dev/mmcblkOp7 | 7340032 | ulmage | USER | KERNELO | NONE |
| /dev/mmcblkOp8 | 5767168 | rootfs.img | USER | RFS0 | NONE |
| /dev/mmcblkOp9 | 7340032 | ulmage | USER | KERNEL1 | NONE |
| /dev/mmcblkOp10 | 5767168 | rootfs.img | USER | RFS1 | NONE |
| /dev/mmcblkOp11 | 8192 | sign0.bin | NONE | SECUREMAC0 | NONE |
| /dev/mmcblkOp12 | 8192 | sign1.bin | NONE | SECUREMAC1 | NONE |
| /dev/mmcblkOp13 | 8192 | VD-HEADER | NONE | NONE | NONE |
| /dev/mmcblkOp14 | 3145728 | NONE | NONE | NONE | mtd_drmregion_a |
| /dev/mmcblkOp15 | 3145728 | NONE | NONE | NONE | mtd_drmregion_b |
| /dev/mmcblkOp16 | 157286400 | NONE | NONE | NONE | mtd_rwarea |
| /dev/mmcblkOp17 | 367001600 | exe.img | USER | EXE0 | mtd_exe |
| /dev/mmcblkOp18 | 367001600 | exe.img | USER | EXE1 | mtd_exe |
| /dev/mmcblkOp19 | 419430400 | rocommon.img | USER | CONTENT0 | mtd_rocommon |
| /dev/mmcblkOp20 | 419430400 | rocommon.img | USER | CONTENT1 | mtd_rocommon |
| /dev/mmcblkOp21 | 104857600 | emanual.img | OTHER | NONE | mtd_emanual |
| /dev/mmcblkOp22 | 157286400 | NONE | NONE | NONE | mtd_contents |
| /dev/mmcblkOp23 | 10485760 | NONE | NONE | NONE | mtd_swu |
| /dev/mmcblkOp24 | 1870979072 | rwcommon.img | OTHER | NONE | mtd_rwcommon |



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

| Name | Date modified | Type |
|---|------------------|-------------|
|  FB | 24-09-2014 16:02 | File folder |
|  TW | 24-09-2014 16:02 | File folder |
|  Y2B | 24-09-2014 16:02 | File folder |

 100001756376377_637236553011551
 100001756376377_637236553011551Dieter Baar
 100002591493138_591328540963524Ä–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_verion":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: fullBrowser_Bookm:  New Record

| | URL | Title | EnterTime | DeviceName | E |
|---|---|---------------------|------------|------------|---|
| 1 | http://nl.msn.com/?pc=SMTV | Hotmail, Messenger, | 1970-01-01 | Local | |
| 2 | http://www.google.nl/ | Google | 1970-01-01 | Local | |
| 3 | http://www.google.com/ | Google | 1970-01-01 | Local | |
| 4 | http://www.facebook.com/ | Facebook | 1970-01-01 | Local | |
| 5 | http://www.youtube.com/ | YouTube | 1970-01-01 | Local | |
| 6 | http://www.youtube.com/watch?v=CU4NFfR7sRg | Kampioen - Soufiane | 1970-01-01 | Local | |
| 7 | http://www.amazon.com/ | Amazon.com: Online | 1970-01-01 | Local | |



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: PhotoTable_14048: ▼



| | TITLE | DATE | HEIGHT | MAKER |
|----|------------|------------|--------|-----------|
| 1 | 3 IMG_0376 | 1404734357 | 2448 | iPhone 5s |
| 2 | 1 IMG_0371 | 1404734281 | 2448 | iPhone 5s |
| 3 | 3 IMG_0380 | 1404734417 | 2448 | iPhone 5s |
| 4 | 5 IMG_0378 | 1404734390 | 2448 | iPhone 5s |
| 5 | 4 IMG_0374 | 1404734292 | 2448 | iPhone 5s |
| 6 | 0 IMG_0369 | 1404734269 | 2448 | iPhone 5s |
| 7 | 2 IMG_0373 | 1404734288 | 2448 | iPhone 5s |
| 8 | 1 IMG_0375 | 1404734356 | 2448 | iPhone 5s |
| 9 | 7 IMG_0368 | 1404734256 | 2448 | iPhone 5s |
| 10 | 1 IMG_0372 | 1404734390 | 2448 | iPhone 5s |
| 11 | 4 IMG_0377 | 1404734379 | 2448 | iPhone 5s |
| 12 | 3 IMG_0370 | 1404734277 | 2448 | iPhone 5s |



Data Analysis: External Media Artifacts

- Device0013.db located in p22
- SQLite database
- Contains one table TABLE_DEVID
- Information about USB flash drives

Database Structure | Browse Data | Execute SQL

Table: TABLE_DEVID

| ID | DEVID | DEVTYPE | EXTTYPE | MODELNAME | WRITABLE | PARTITIONINDEX | PARTITIONKEY | USERID | REGISTER |
|----|-------|------------|---------|----------------------|----------|----------------|--------------|--------|----------|
| 1 | 1 | 1404825533 | 0 | 102 DataTraveler 3.0 | 1 | 0 | 1 | | 1 |



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

The screenshot shows a database management interface with three tabs: 'Database Structure', 'Browse Data', and 'Execute SQL'. The 'Database Structure' tab is active. Below the tabs, there is a 'Table:' label followed by a dropdown menu showing 'ProgramTable' and a magnifying glass icon. Below this, a table structure is displayed with the following columns: ID, PROGRAM ID, CHANNEL ID, START TIME, CHANNEL NUMBER, CHANNEL NAME, LANGUAGE, TITLE, GENRE ID, and DURATION.

| ID | PROGRAM ID | CHANNEL ID | START TIME | CHANNEL NUMBER | CHANNEL NAME | LANGUAGE | TITLE | GENRE ID | DURATION |
|----|------------|------------|------------|----------------|--------------|----------|-------|----------|----------|
|----|------------|------------|------------|----------------|--------------|----------|-------|----------|----------|



Data Analysis : Cloud services

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

Table:

| | url | stamp |
|---|---|------------|
| 1 | https://www.dropbox.com/ajax_captcha_login | 1357005907 |
| 2 | http://noticefile.samsungcloudsolution.com/Front/NoticeAll?cc | 1404998892 |
| 3 | https://www.dropbox.com/1/oauth/authorize?oauth_token= | 1405000446 |
| 4 | https://www.dropbox.com/home | 1405001971 |
| 5 | https://www.dropbox.com/1/oauth/authorize?oauth_token= | 1405002037 |
| 6 | https://www.dropbox.com/1/oauth/authorize?oauth_token= | 1357005770 |



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

