



Smart TV Forensics - Digital Traces On Televisions

By

Abdul Boztas, Remko Riethoven and Mark Roeloffs

From the proceedings of

The Digital Forensic Research Conference

DFRWS 2015 EU

Dublin, Ireland (Mar 23rd- 26th)

DFRWS is dedicated to the sharing of knowledge and ideas about digital forensics research. Ever since it organized the first open workshop devoted to digital forensics in 2001, DFRWS continues to bring academics and practitioners together in an informal environment.

As a non-profit, volunteer organization, DFRWS sponsors technical working groups, annual conferences and challenges to help drive the direction of research and development.

<http://dfrws.org>



Contents lists available at ScienceDirect

Digital Investigation

journal homepage: www.elsevier.com/locate/diin

Smart TV forensics: Digital traces on televisions



A. Boztas*, A.R.J. Riethoven, M. Roeloffs

Netherlands Forensic Institute, Laan van Ypenburg 6, The Hague, The Netherlands

A B S T R A C T

Keywords:

Digital forensics
Smart TV
Smart TV forensics
Cyber crime
Digital crime

The Smart TV is becoming increasingly popular amongst consumers. Many consumers use a Smart TV to gain quick access to the Internet including video on demand, social networking and instant messaging. Most Smart TVs also provide capabilities to connect with external devices such as a USB flash drive, a mobile phone etc. All of these features make a Smart TV a potentially rich source of information for forensic purposes. With increasing utilisation, it is also easier for malicious users to abuse a Smart TV. Therefore a digital forensics study on the field of Smart TV is imperative. This paper proposes new procedures for acquiring, analysing and investigating a Smart TV.

© 2015 The Authors. Published by Elsevier Ltd. This is an open access article under the CC BY-NC-ND license (<http://creativecommons.org/licenses/by-nc-nd/4.0/>).

Introduction

Electronic technology continues to develop. Each day new electronic devices that influence human daily life are entering the market. These devices may store digital data which may be interesting from a digital investigation perspective. A Smart TV (Wikipedia, 2014) is one of these devices. A Smart TV, sometimes referred to as connected TV or hybrid TV, describes a trend of integration of the Internet into television sets and set-top boxes, as well as the technological convergence between computers, television sets and set-top boxes. Smart TVs are available as stand-alone products, but regular televisions can also be made “smart” through set-top boxes that enable advanced functions; for example, Google TV, Apple TV. These devices are mostly IP devices, which enable streaming content over Internet without the need for cable or satellite. Most of the Smart TVs provide access to external hard drives, digital cameras, mobile phones or Internet applications. A Smart TV allows the viewers to connect to the Internet and

browse the web as on a computer without the need for additional peripherals. Smart TVs include a wide range of applications which can be used for different means. Viewers can use applications to search and find videos, music, photos and other content on the web, a local cable TV channel, a satellite TV channel or a local storage device.

In the digital forensic area, questions arise as to whether a Smart TV should be an important component of a digital investigation. In the article (Sutherland et al., 2014) a number of questions are posed concerning the relevance of the Smart TV in a digital forensic investigation: do Smart TVs retain and contain relevant information? How easily is this data accessed? In Mutawa et al. (2012) it is stated that the increased use of social networking applications on smartphones makes these devices a “goldmine” for forensic investigators. Is the use of, for example, social networking applications on Smart TVs doing the same for forensic investigators?

This paper presents research on extracting and analysing digital data from a Smart TV in a forensically sound manner. It will give a complete guide to acquiring and investigating data on a Smart TV. This paper does not present an in-depth study of the inner workings of a Smart TV. The scope of this research focuses only on the methods of extracting data from a Smart TV and the global analysis

* Corresponding author.

E-mail addresses: a.boztas@holmes.nl (A. Boztas), r.riethoven@holmes.nl (A.R.J. Riethoven), m.roeloffs@holmes.nl (M. Roeloffs).

of the said acquired data. Our goal is to show that a Smart TV may indeed contain different kinds of digital traces which can be relevant for investigations, such as, pictures, connected devices, visited websites, etc. If forensic examiners are not knowledgeable regarding the different types of Smart TV based systems and what artifacts each may leave behind, they could miss critical information during an investigation.

Related work

Earlier work on Smart TVs focuses mainly on gaining access to the Smart TV in order to get user data remotely (Grattafiori and Yavor, 2013) and (Lee and Kim, 2013). The latter authors also go further into making a surveillance device from the Smart TV, by recording audio and video from the built-in microphone and camera respectively. The main point made in the previous research is that it is not that hard to find ways to gain access to the Smart TV on a low-level. With these methods it should be possible to gain access to a Smart TV. There is no forensic research available for any brand or model of Smart TV.

From a hardware perspective, the Smart TV is just an embedded system with a large (for example 40-inch) screen. The Smart TV can be handled like any embedded system. An embedded system which has been investigated thoroughly is a mobile phone. Willassen (2005) and van der Knijff (2010) show methods which can be used during the investigation of a Smart TV.

Materials and methods

In this section we will explain how we carried out this research. Initially, a literature and market share survey was conducted. The Smart TV market continues to grow (Tarr, 2013) and expand rapidly in major countries (Hong, 2013). We determined which models and brands of Smart TV are popular (Top10, 2014) or more common under users and which functionality of these Smart TVs are commonly used. On the basis of this literature study, the model and type of the Smart TV for our research was selected. Secondly, we set up an experimental environment to generate different types of digital traces when using the Smart TV. Finally methods were developed to acquire and analyse the digital traces of this Smart TV.

Selecting a smart TV

As previously stated, there exists a great deal of variety of types and models of Smart TVs on the market. The features available on a Smart TV vary depending on the brand and model of TV. Most Smart TVs will allow access to popular social networking sites and communication programs such as Skype. The most popular brands of Smart TV are Samsung, LG, Panasonic and Sony. This research was conducted on a Samsung television model UE40F7000SLXXN, based on popularity, the fact that it contains a camera and microphone, and the fact that Samsung has an open source platform for their Smart TVs. The Samsung Smart TVs are very popular amongst

customers and offer a great deal of functionality which therefore may leave relevant digital traces for a digital investigation. This type of television allows the viewer to install applications, visit websites, peruse pictures, communicate by voice and video, connect external devices, etc. User data was generated by performing different usage scenarios which covered most of the available functionality of the Samsung Smart TV.

Data acquisition methods

The selected Smart TV uses flash memory as storage. The flash memory on the investigated Smart TV is an eMMC chip (Wikipedia MultiMediaCard, 2015). Depending on the hardware, there are several options to acquire data. The following methods for acquiring the data were utilised:

- eMMC five-wire method: an eMMC chip, like the one used in our reference Smart TV only needs five signals to be connected: Vss, Vdd, Clock, Command & Data0. These signals were detected on the main board. It is then possible to read the eMMC chip using a standard USB SD-cardreader attached to a writeblocker.
- NFI Memory Toolkit II (MTK II): (NFI, 2011) this is a universal forensic solution that enables investigators to read memory chips and potentially extract user data – such as text messages, phone numbers, pictures and browser history – from a wide variety of devices. The MTK II is a combination of hardware and software. The hardware makes a physical connection, generates signals and supplies power to a memory chip, while the software runs the necessary command-sets to access data in the various types of memory chips.
- Application: a software approach for acquiring data is the use of a custom application with a small footprint which was installed on the Smart TV and writes the data out to an external storage device. This might be possible as Samsung distributes a Software Development Kit to develop applications for this particular model of Smart TV.

Analysis of digital traces

The fundamental goal of this research is to determine which digital traces are left behind on a Smart TV for investigation purposes. This means that this paper is not a complete description of the inner workings of this particular Smart TV and instead is focused on acquiring traces of user interaction. Different tools and forensic programs like EnCase were used to search through the data of the Smart TV. Our research was focused on the following types of traces which may well be relevant for a digital forensic study:

- System information and settings: device name, connected devices, network information and smart functions.
- Apps: Facebook, Twitter, YouTube, etc.
- Web browsing: visited websites, traces of search engines, etc.
- Photo and multimedia files

- External media: connected external devices such as USB flash drive, harddisks, etc.
- E-mails and appointments
- Cloud services: Dropbox and OneDrive
- Channel information: which channels are viewed.

Data acquisition

eMMC five-wire method

On the main board of the Samsung Smart TV, the five necessary signals were detected in order to use the five-wire method and extract data from the eMMC chip. It was not possible to make a copy of the eMMC memory. This is probably due to the fact that the processor is also trying to access the memory. It was not possible to reset or halt the processor, because reset points were not found. It was also not possible to put the Smart TV into a specific mode, in order to prevent the processor from accessing the memory. For this specific brand and model Smart TV the five-wire method did not work.

NFI memory toolkit

The next option was to desolder the flash memory and read it with the MTK II.

Fig. 1 depicts the main board of the Samsung Smart TV. The white square emphasises the location of the memory chip of the Smart TV.

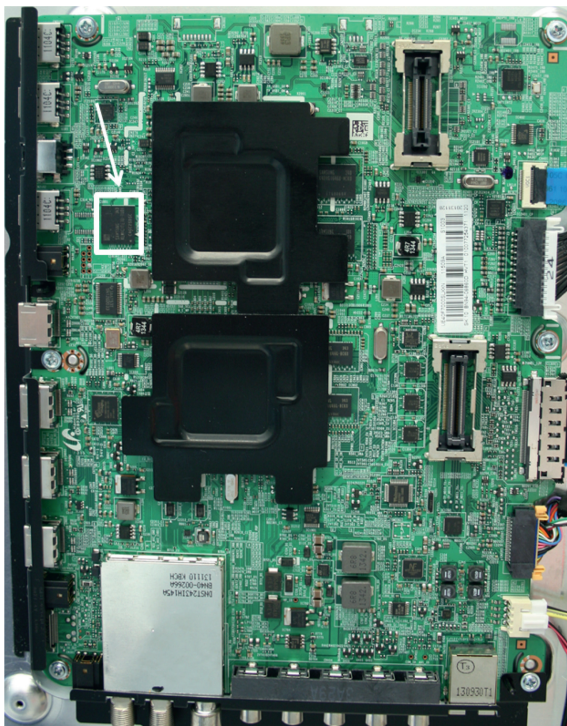


Fig. 1. Main board.

The memory chip of the Samsung model UE40F7000SLXXN is a Samsung KLM4G1FE3B-B00, which is a 4GiB MoviNAND flash chip. MoviNAND is the trademarked name for Samsung's eMMC chips. By utilising a (hot air) rework station, the memory chip was removed from the main board (Breeuwsma et al., 2007). The MTK II was then used to make an image of the memory chip.

Application

Due to the fact that data acquisition by chip extraction is very specialised and destructive, a software method was investigated. A hacking community (SamyGo, 2014) has already made progress in this area. The SamyGO Forum describes a method to 'root' a Samsung Smart TV (SamyGo Forum, 2013b). Rooting is needed to obtain elevated privileges for an application that runs on Linux for ARM operating system installed on this Smart TV. Without elevated privileges, it is not possible to extract data from the user space memory or have full access to the file system. The rooting procedure is as follows:

1. Install the Skype App from the Samsung App store.
2. Start the Skype app and ensure Skype is set to autostart, before closing it.
3. Install the SamyGO widget.
 - (a) Download the SamyGO_usb widget.
 - (b) Place the SamyGO folder on a USB flash drive.
 - (c) Navigate to "more apps" and insert the USB flash drive.
 - (d) Start the SamyGO widget.

By examining the code in the *Main.js* file of the SamyGO widget, it is derived that a file patch was unzipped in the Skype folder. The patch file is a zip file with the contents:

- AutoStart
- libSkype.so
- remoteSamyGO.zip
- runSamyGO.sh

The file *libSkype.so* overwrites the current file, and is started by Skype at the startup of the Smart TV. This *libSkype.so* in turn starts the script *runSamyGO.sh*, which installs busybox and initiates an ftp server. With the added functionality of an ftp-server on the rooted Smart TV it is possible to transfer data.

With changes to the SamyGO shell script, it is possible to make images of the complete flash memory from the Smart TV. The script *runSamyGO.sh* was modified, so that it would start another script (*run1.sh*), which installs a busybox instance into the */tmp/bin* directory and uses the *dd* command from the busybox to create an image. During this imaging process the data is written to a USB flash drive which is inserted into the Smart TV.

This software method is vulnerable to updates of the firmware of the Smart TV. As (Grattafiori and Yavor, 2013) show, security researchers are also targetting the Smart TV operating systems. During our research the firmware was automatically updated to a newer version. The root method

of the Smart TV ceased to work and therefore the application was rendered useless. For other models of Samsung Smart TVs this method might still be working and the SamyGO userbase might overcome this problem in the future by releasing an updated version or method. As (Lee and Kim, 2013) shows there will be more methods of getting software access to the Smart TV, but it will take work for each brand and model of TV. It will always be an arms race between the makers of exploits and the Smart TV manufacturers who will repair these exploits. Therefore, the hardware methods for getting access to Smart TVs will be more lasting and forensically more sound than the software methods.

File system analysis

As described in the previous section, data can be successfully acquired from the Smart TV using two different methods. Each of these methods results in an image which can be analysed with both standard tools and specific forensic tools. In this section the results of the image analyse are presented.

The image from the 4 GiB flash memory contains in total 24 partitions. It uses a standard DOS partition scheme (Carrier, 2005, p. 81–84) with four primary partitions. One of the primary partitions is an extended partition containing 20 logical partitions. All partitions, except the placeholder extended partition, have a hex byte 83 standard Linux identifier (Carrier, 2005, p. 90). Based upon a signature identification of the content within the partition, at least two different file system images were discovered. Table 1 lists the partitions containing a Squash File System image (SquashFS) and Table 2 lists the partitions with the proprietary Samsung eMMC chip oriented File System (eMMCfs). In Table 3 u-boot images are listed that were discovered.

The acquired *dd* image and the MTK II eMMC storage area image are both equal in size. However, besides the standard eMMC storage area, the MTK II also acquired the Boot area and Replay Protected Memory Block (RPMB) area from the chip in separate image files.

SquashFS

The SquashFS, which is intended to be a read-only file system, is not viewable with the standard *squashfs-tools* (Lougher, 2014). Samsung made its own changes to *squashfs-tools* version 4.2. This version (*squashfs4.2.tar.gz*) can be downloaded from Samsungs Open Source Release Center (Samsung, 2014), in the TV/DTV/ETC section. With

Table 1
SquashFS file system, little endian, version 4.0.

Label	Start sector	Size in bytes
p8	19,536	5,767,168
p10	45,168	5,767,168
p17	376,080	367,001,600
p18	1,092,896	367,001,600
p19	1,809,712	419,430,400
p20	2,628,928	419,430,400

Table 2
Samsung eMMC chip oriented File System.

Label	Start sector	Size in bytes
p14	56,544	3,145,728
p15	62,704	3,145,728
p16	68,864	157,286,400
p21	3,448,144	104,857,600
p22	3,652,960	157,286,400
p23	3,960,176	10,485,760
p24	3,980,672	1,870,979,072

this program it is possible to unsquash the file system thereby exporting all content. Loopback mounting a Samsung SquashFS image is possible when applying the modification Samsung made to SquashFS for a given Linux kernel.

In the unsquashed partition *p17* we found a text file *partitions.txt* (see Fig. 2) which lists more information about the used partition schema. This figure however lists 25 partitions instead of the previous found 24. One partition with the size of 524,288 bytes is missing in our 4GiB images. Because partition *p1* is zero-filled in the *dd* image, we assume that this is the RPMB and *p0* is the Boot area. Further research on the Boot area and RPMB acquired with the MTK II should be conducted to support this assumption.

Samsung eMMC chip oriented file system

The eMMCfs is a proprietary file system made by Samsung. In order to investigate the contents of the partitions with this type of file system, specifications were needed. On most of their Smart TVs, Samsung uses VD GNU/Linux, which is an open source Linux distribution by the VD Project (2014). Our particular Smart TV uses this distribution of Linux on its ARM processors. In the source code of this operating system, found in Samsung (2014) in the TV/DTV/LED section with the name *13_UNxxF7200.zip*, the Linux file system drivers for eMMCfs were found. These sources can be compiled for any Linux-based operating system. Depending on the version of the Linux kernel, a user wanting to include native support for eMMCfs can do so. On the SamyGO forums (SamyGo Forum, 2013a) users have already made some patches for different kernel versions which can be used, or an expert user can use the sources from Samsung and incorporate them into their Linux distribution.

U-boot legacy ulmage

U-Boot is a universal bootloader that is used to boot devices. This particular bootloader has comprehensive support for loading and managing boot images. The boot

Table 3
u-boot legacy ulmage (Linux 3.0.33, Linux/ARM OS Kernel Image).

Label	Start sector	Size in bytes
p7	5184	7,340,032
p9	30,816	7,340,032

flash_device _name	flash_device _size	flash_image _name	flash_upgrade _type	flash_partition _map	flash_mount _path
/dev/mmcblk0p0	524288	onboot.bin	OTHER	BOOTLOADER0	NONE
/dev/mmcblk0p1	524288	u-boot.bin	NONE	BOOTLOADER1	NONE
/dev/mmcblk0p2	524288	secos.bin	USER	SECOS0	NONE
/dev/mmcblk0p3	524288	secos.bin	USER	SECOS1	NONE
/dev/mmcblk0p4	0	ex_partition	NONE	NONE	NONE
/dev/mmcblk0p5	524288	seret.bin	USER	SERETO	NONE
/dev/mmcblk0p6	524288	seret.bin	USER	SERET1	NONE
/dev/mmcblk0p7	7340032	ulmage	USER	KERNELO	NONE
/dev/mmcblk0p8	5767168	rootfs.img	USER	RFS0	NONE
/dev/mmcblk0p9	7340032	ulmage	USER	KERNEL1	NONE
/dev/mmcblk0p10	5767168	rootfs.img	USER	RFS1	NONE
/dev/mmcblk0p11	8192	sign0.bin	NONE	SECUREMAC0	NONE
/dev/mmcblk0p12	8192	sign1.bin	NONE	SECUREMAC1	NONE
/dev/mmcblk0p13	8192	VD-HEADER	NONE	NONE	NONE
/dev/mmcblk0p14	3145728	NONE	NONE	NONE	mtddrmregion_a
/dev/mmcblk0p15	3145728	NONE	NONE	NONE	mtddrmregion_b
/dev/mmcblk0p16	157286400	NONE	NONE	NONE	mtd_rwarea
/dev/mmcblk0p17	367001600	exe.img	USER	EXEO	mtdd_exe
/dev/mmcblk0p18	367001600	exe.img	USER	EXE1	mtdd_exe
/dev/mmcblk0p19	419430400	rocommon.img	USER	CONTENT0	mtdd_rocommon
/dev/mmcblk0p20	419430400	rocommon.img	USER	CONTENT1	mtdd_rocommon
/dev/mmcblk0p21	104857600	emanual.img	OTHER	NONE	mtdd_emanual
/dev/mmcblk0p22	157286400	NONE	NONE	NONE	mtdd_contents
/dev/mmcblk0p23	10485760	NONE	NONE	NONE	mtdd_swu
/dev/mmcblk0p24	1870979072	rwcommon.img	OTHER	NONE	mtdd_rwcommon

Fig. 2. File partitions.txt.

images in Table 3 are so called secure boot images which are signed by Samsung. This is used to prevent the Smart TV from booting other type of images, unless the security is broken.

Partition redundancy

As seen in Fig. 2, a number of partitions have the same size, some of which have the same bitwise content. Reference *p2* is short for */dev/mmcblk0p2*, henceforth the partitions that have the same content are *p2 + p3*, *p5 + p6*, *p7 + p9* and *p8 + p10*. This is most likely to enable the resetting of the Smart TV to factory settings or in the event of an unsuccessful software or firmware upgrade, it may be reverted to a previous version.

Analysis of digital traces

In this section, digital traces contained in the file system of the Smart TV will be analysed. For clarity partition references in this section are also based on the partition schema depicted in Fig. 2 shortened to *p<number>*.

System and network information

The Samsung Smart TV provides functionality to display information about the Smart TV itself. Fig. 3 shows an example of information that is displayed by the Smart TV. First this functionality was used to display information about the Smart TV and then files were searched that



Fig. 3. System information.

contained this information. Experiments show that information is redundantly stored in multiple files on the Smart TV. The following files contain information about serial number, model name, device ID of Smart TV.

- *p16/dlna_web_root/dmr/SamsungMRDesc.xml*
- *p16/dlna_web_root/rcr/RemoteControlReceiver.xml*
- *p16/dlna_web_root/MainTVServer2/MainTVServer2Desc.xml*
- *p16/dlna_web_root/rcr/dialreceiver.xml*

For example; a part of the file *SamsungMRDesc.xml* file contains the following information:

```

<manufacturerURL>
http://www.samsung.com/sec
</manufacturerURL>
<modelDescription>
SamsungTVDMR
</modelDescription>
<modelName>
UE40F7000
</modelName>
<modelNumber>
AllShare1.0
</modelNumber>
<modelURL>http://www.samsung.com/sec
</modelURL>
<serialNumber>REMOVED by Authors</serialNumber>
<UDN>REMOVED by Authors</UDN>
<sec:deviceID>REMOVED by Authors</sec:deviceID>

```

The following files contain information about the firmware version:

- *p17/infolink/manager/versionfile*
- *p24/common/WidgetMgr/mgrinfo.dat*

Network information

The Samsung Smart TV provides functionality to display network information, as seen in Fig. 4. Network related information was found to be stored in the following files:

- *p16/network/network_tv_name*: information about TV name on network
- *p16/network/network_wfd_config*: information about port numbers
- *p16/wfd_rtspsource*: information about IP-address
- *p16/Bluetooth_Dev_info*: information about paired bluetooth devices
- *p24/common/WidgetMgr/network.info*: the MAC-address of the ethernet port

Apps activity

Experiments show that information about installed apps is saved in the subdirectory *widgets* which is located on the root of *p24*. The subdirectory *widgets* contains two subdirectories, which are named *User* and *Normal*. The subdirectory *User* contains information about apps which have been manually installed by the user. The subdirectory

Normal contains information about apps which were installed from the Samsung App Store. The following files and subdirectories contain relevant information about the applications:

- *p24/common/WidgetMgr/info.xml*: information about installed apps on Smart TV
- *p24/common/11111000001/_sfdata.json*: information about the installation date of apps
- *p24/common/WidgetMgr/history.xml*: historic information about paths in which pictograms from the last used apps were saved.
- *p24/history/capture*: a folder containing low resolution screenshots from the last used apps, which are named with the identifier number of the app. The corresponding identifier number is also saved in a file which is called *history.xml* located in the root folder *history*. This means that the Samsung TV takes a screenshot from the running app with content. The number of screenshots, when a screenshot is being made and their longevity has not yet been determined.
- *p16/SOCIAL*: a directory about social media related apps, containing for each social media related app, one subdirectory with an abbreviation of the app name. For example: *SOCIAL/FB* contains information about Facebook app or *SOCIAL/TW* contains information about Twitter

In order to illustrate the type of information gain from these files, a part of the file *_sfdata.json* is included:

```

"widgetname":"Facebook","vendor":"Samsung",
"install_date":"Wed, 19 May2010 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",

```

Web browsing activity

While conducting our research, it was discovered that all relevant Internet traces were kept in SQLite databases. This database is the file *settings.db* in partition *p24* in the sub-directory *webkit/WebBrowser*. This database contains 14 tables. Below the tables which contain relevant information are listed:

- *FullBrowserHistory*: contains information about the URL, title, count and visited date. During this investigation it was determined that VisitDay was always 1970 and was not updated to the actual date and time.
- *fullBrowser_HiddenHistory*: contains only the name of visited websites without additional information
- *fullBrowser_Bookmark*: contains information about websites which are bookmarked

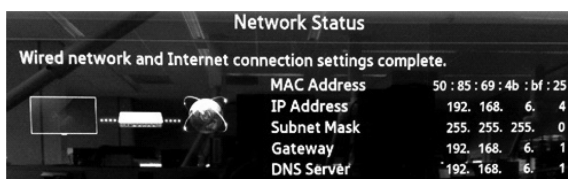


Fig. 4. Network information.

- fullBrowser_Search: contains the name of search engines. For example google, bing

Fig. 5 depicts an example of a table as found in *settings.db*.

Pictures, audio and video files

The file *.CM.db* which is located on the root of partition *p22*, contains information about audio, picture and video files as well as other specific information such as when these files were opened, played etc. This file is also an SQLite database and contains 20 tables. Below are the relevant tables:

- PhotoTable: name and EXIF information of the picture
- MusicTable: name of the file, media information such as artist, genre etc.
- VideoTable: name of the file, title, container type etc.
- FileTable: media files which were opened. The sub-directory *p22/Recently Played* contains files with the *.mta* extension. According to information on (File Extensions, 2014) these files are Samsungs AllShare files and they can contain thumbnails. During this research it was not possible to view these files.

Fig. 6 shows an example of a table as found in the database *.CM.db*.

External media artifacts

The file *device0013.db* which is located in the root of *p22* contains information about USB flash drives that have been connected to the Smart TV. This file is an SQLite database and contains one table *TABLE_DEVID*. Fig. 7 shows the fields of this table. During this research it was not possible to determine with experiments why the database file is called *device0013.db*. There are no files numbered 0 through 12 or higher found (for example *device0015.db*).

TV channels

The following files contain information about television channels.

- *p16/map-AirA*, *map-AirD*, *map-CableA*, *map-CableD*, *map-SateD*; These files contain the names of channels for analogue and digital terrestrial, cable or satellite connections.
- *p22/.EPG.db*; This is an SQLite database and contains the Electronic Program Guide. The tables contains TV program broadcast information. Fig. 8 shows as an example of the schema of a table in this file.

Cloud artifacts

During this research of cloud services, databases that log http and https requests were found. The following databases relate traces to cloud services:

- *p24/webkit/database/snapshot/WebpageSnapshots.db*. Fig. 9 shows an example of a table in this file.
- *p24/webkit/localstorage/StorageTracker.db*
- *p24/webkit/WebBrowser/settings.db*
- *p16/UDBCOMMON*.

Conclusion

This paper presents the possibilities to perform a digital forensic investigation on a Smart TV. The results of this research will be of importance to forensic investigators, as well as in criminal investigations and civil litigation matters.


It is important to understand that malicious users can abuse a Smart TV for criminal purposes such as viewing child pornography, communication with other criminals, botnet, etc. The Smart TV can be a member of a home network and can contain traces and information about other digital equipment or computers at a crimescene. Therefore forensic investigators have to realise that a Smart TV may contain relevant information. In the future we expect that the Smart TV will also be a major component in the field of digital forensics.

This research has shown that it is possible to make a copy of data from a Smart TV for forensic investigation purposes. Section Data acquisition contains two methods for data collection from a Smart TV, an application and the NFI Memory Toolkit II. We expect the chip-off method, in combination with the MTK II, to continue to work for Smart

Table: FullBrowserHistory  New Record


	URL	Title	Count	VisitDay
1	http://www.bing.com/	Bing	1	1970-01-01
2	http://nl.msn.com/?pc=SMTV	MSN NL: Hotmail, Outlook, Skype, het	89	1970-01-01
3	http://nieuws.nl.msn.com/afbeeldingen/heb-je-	Roemeense bedelaar heeft drie luxe e	1	1970-01-01
4	http://www.telegraaf.nl/	Nieuws Altijd op de hoogte van het l	3	1970-01-01
5	http://tmgonlinemedia.nl/consent/consent/?reb	Nieuws Altijd op de hoogte van het l	1	1970-01-01
6	http://www.telegraaf.nl/prive/22152971/_Ma	Man sterft na winnen prijs in show Elle	1	1970-01-01
7	http://www.dumpert.nl/	dumpert.nl	3	1970-01-01
8	http://www.dumpert.nl/mediabase/6577295/e:	dumpert.nl - KOMT DIE GOLF!!!	1	1970-01-01
9	http://www.dumpert.nl/mediabase/6577257/7f	dumpert.nl - Helikoptercrew redt kraa	1	1970-01-01

Fig. 5. Example table from *settings.db*.

Table: **FileTable_PLAYLIST** 

	ID	PL ID	PATH ID	NAME	ADDED DATE	MOD DATE	CREATE DATE
1	2	1	2	ibocukklip.wmv	1404995459	1244675184	1404742872
2	9	1	1	IMG_0375.JPG	1404995481	1404734356	1404742842
3	10	1	1	IMG_0376.JPG	1404995482	1404734357	1404742838
4	11	1	1	IMG_0377.JPG	1404995483	1404734379	1404742839
5	12	1	1	IMG_0378.JPG	1404995484	1404734390	1404742839
6	13	1	1	IMG_0379.JPG	1404995485	1404734393	1404742840
7	14	1	1	IMG_0380.JPG	1404995486	1404734417	1404742840
8	15	1	1	IMG_0381.JPG	1404995487	1404734419	1404742840
9	16	1	1	IMG_0368.JPG	1404995488	1404734256	1404742840
10	17	1	3	dontlea.mp3	1404995502	1176202936	1404742859

Fig. 6. Example table from .CM.db.

Table: **TABLE_DEVID**  New Record

	ID	DEVID	DEVTYPE	EXTTYPE	MODELNAME	WRITABLE	PARTITIONINDE	PARTITIONKKE	USERID
1	1	1404825533	0	102	DataTraveler 3.0	1	0	1	

Fig. 7. Example table from device0013.db.

Table: **ProgramTable** 


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

Fig. 8. Example table from .EPG.db.

TVs containing flash based storage. Until now it was not possible to find other ways which will always work. The desoldering is also the best forensically sound method to make a copy of a device. With this method, no data is changed during the acquisition process.

The use of this method has also some disadvantages. The desoldering process needs to be done with specific equipment and there is also a risk that the process will

damage the Smart TV. This method cannot be performed on-site. This research also explored the collection of data via these methods and determined that file contents were not altered by the use of the NFI Memory Toolkit. An application can only be used in cases where it is not possible to extract the chip from the TV. Due to the installation of this application on a Smart TV, the original state of data will be changed. The change of data is in some

Table: **PageInfo** 

	url	stamp
1	http://noticefile.samsungcloudsolution.com/Front/NoticeAll?c	1404998892
2	https://www.dropbox.com/1/oauth/authorize?oauth_token=	1405000446
3	https://www.dropbox.com/home	1405001971
4	https://www.dropbox.com/1/oauth/authorize?oauth_token=	1405002037
5	https://www.dropbox.com/1/oauth/authorize?oauth_token=	1357005770
6	https://www.dropbox.com/1/oauth/authorize?oauth_token=	1357005907
7	https://www.dropbox.com/ajax_captcha_login	1357005895

Fig. 9. Example table from WebpageSnapshots.db.

cases predictable, for example it is possible to determine the directory where the application files are stored during installation. But the problem with an embedded system which runs an operating system is that the operating system will always change data in the memory/file system when an embedded system is running such as log files. So it is not always feasible to determine all the conditions for an embedded operating system that cause changes in data.

Forensic examiners know that every type of digital equipment can contain artifacts of digital data that may be interesting for their case. In practice a great deal of digital equipment is still being overlooked. The analysis of acquired data from the Smart TV shows that a Smart TV also contains relevant digital artifacts for digital forensic purposes, and that this data is easily acquired and interpreted. Section Analysis of digital traces describes the found digital artifacts on Smart TV during this research, including traces of social networking applications like Facebook and Twitter. The screenshots the Smart TV makes from content within a running application are valuable for a forensic investigator to get a first quick impression of user activity.

The forensic investigator can use the result of this paper as a guide for performing a digital forensic investigation on a Smart TV. This research shows that a Smart TV can contain relevant digital data for forensic investigations and therefore it should be a part of digital investigations. It also describes multiple methods which are usable for acquiring data on other embedded systems.

Future work

In this paper only one brand and model of Smart TV was analysed. There are many different types and brands of Smart TVs on the market. In order to get a better understanding of Smart TVs, other types also need to be examined. Only certain types of digital traces and mostly traces that were easy to interpret were analysed. A deeper analysis of the Smart TV would reveal even more interesting traces, for example the frequency of the creation of application content screenshots and the longevity of said screenshot files. It is also expected that there are a lot more digital traces in the various types of Smart TV, as each brand or model can contain different types of apps or have different functionality which can leave behind different digital traces.

The SamyGO rooting method will most probably only work for a specific model and firmware. An alternative method could be a triage type of application which copies only important files from a Smart TV or makes a copy of the Smart TV without altering the content.

Another important research point is internal volatile memory of the Smart TV. The internal volatile memory should also be acquired and analysed. Internal volatile memory can contain very relevant information such as passwords, last activity on the Smart TV, etc. More research should be done in the field of obtaining a memory dump of a Smart TV.

The five-wire method shouldn't be excluded in future research, it may still be a viable method for other brands and models Smart TV.

There is also research to be done on the network activity of a Smart TV, be it by ethernet, wifi or bluetooth. This is interesting for cases where data interception is part of the investigation.

Acknowledgements

The authors wish to thank S. Laraghy for her valuable support in producing this paper.

References

- Breeuwsma MF, de Jongh M, Klaver C, van der Knijff R, Roeloffs M. Forensics data recovery from flash memory. *Small Scale Device Forensics J* 2007;1(1).
- Carrier B. *File system forensic analysis*. Addison-Wesley Professional; 2005.
- File Extensions, <http://www.fileinfo.com/extension/mta>; 2014.
- SamyGo Forum. emmc – samsung chip oriented filesystem. 2013. <http://forum.samygo.tv/viewtopic.php?f=63&t=5993> [accessed 18.09.14].
- SamyGo Forum. [How to] get root access on F series. 2013. <http://forum.samygo.tv/viewtopic.php?f=64&t=6239> [accessed 18.09.14].
- Grattafiori A, Yavor J. The outer limits: hacking the samsung smart tv. *Blackhat Briefing* 2013; 2013.
- Hong K. Out of nowhere, chinas smart tv market explodes into the mainstream. 2013. <http://thenextweb.com/asia/2013/10/16/out-of-nowhere-chinas-smart-tv-market-explodes-into-the-mainstream> [accessed 19.09.14].
- Lee S, Kim S. Hacking, surveilling and deceiving victims on smart tv. *Blackhat Briefing* 2013; 2013 (updated 2013, cited 16.06.2014).
- Lougher P. Squashfs. 2014. <http://squashfs.sourceforge.net> [accessed 19.09.14].
- Wikipedia MultiMediaCard. Multimediacard. 2015. <http://en.wikipedia.org/wiki/MultiMediaCard> [accessed 07.01.15].
- Mutawa NA, Baggili I, Marrington A. Forensic analysis of social networking applications on mobile devices. *Digit Invest* 2012;9(0): S24–33. The Proceedings of the twelfth annual {DFRWS} conference 12th annual Digital Forensics Research conference.
- NFI. A universal forensic solution to read memory chips. 2011. http://www.forensicinstitute.nl/products_and_services/forensic_products/memory_toolkit/index.aspx [accessed 18.09.14].
- VD Project. Vd project is a group to release a linux distribution – vd gnu/linux. vd gnu/linux is based on slackware, BSD like system, i18n/m17n, ipv6, secure, free, and so on. 2014 <http://vdlinux.sourceforge.net/> [accessed 04.02.15].
- Samsung. Opensource release center. 2014. <http://opensource.samsung.com> [accessed 19.09.14].
- SamyGo. Samsung tv firmware hacking. 2014. <http://samygo.tv/> [accessed 19.09.14].
- Sutherland I, Read H, Xynos K. Forensic analysis of smart TV: a current issue and call to arms. *Digit Invest* September 2014;11(3):175–8. <http://dx.doi.org/10.1016/j.diin.2014.05.019>. ISSN: 1742-2876.
- Tarr G. IHS: smart TVs rise to 27% of TV shipments. 2013. <http://www.twice.com/news/tv/ihs-smart-tvs-rise-27-tv-shipments/3471>.
- Top10. Top 10 best tv manufacturing brands. 2014. <http://top-10-list.org/2014/04/30/top-10-best-tv-manufacturing-brands>.
- van der Knijff R. Chapter 8-embedded systems analysis. In: From ECc, Altheide C, Daywalt C, Donno Ad, Forte D, Holley JO, et al., editors. *Handbook of digital forensics and investigation*. San Diego: Academic Press; 2010. p. 383–435. ISBN 13: 978-0-12-374267-4.
- Wikipedia. Smart_tv. 2014. http://en.wikipedia.org/Smart_TV [accessed 18.09.14].
- Willassen S. Forensic analysis of mobile phone internal memory. *Adv Digit Forensics* 2005;191–204. Springer US 2005.