ISSN : 1976-5304
https://kdfs.jams.or.kr

A 2018 Samsung Smart TV Data Acquisition Method Analysis

Terrence Nemayire, Alex Ogbole, Sungmi Park, Keecheol Kim, Yeonseok Jeong, Yunsik Jang
Legal Informatics and Forensic Science Institute, Hallym University

최신 스마트 TV 데이터 획득 기법 분석: 2018년 삼성 제품의 사례

Terrence Nemayire, Alex Ogbole, 박성미, 김기철, 정연석, 장윤식
한림대학교 정보법과학연구소

ABSTRACT

Internet of Things (IoT) has brought a fair share of challenges for Digital forensics and Law Enforcement Agencies in carrying out their investigative duties. The authors of this paper studied the current trends and noticed an increase in crimes that require digital evidence from Smart TVs. Smart TVs are not only a probable source for digital evidence, but have become an integral part in most digital investigations, since they have the ability to connect to the Internet, store digital materials and are able to be synced with various user cloud accounts. This paper marks out the changes in results when using past well-known acquisition methods on the recent Smart TV device and proposes a general investigation procedure model for data acquisition and probable digital evidence for Smart TVs using Chip-Off methods. Regarding the lack of generally applicable methods for Smart TV forensics, this work for a new model will contribute to collective efforts as a whole.

Key Words : IoT Forensics, Smart TV, Samsung TV, VDFS, Tizen

요 약

사물인터넷(IoT) 기기가 디지털 포렌식과 범죄수사기관의 조사업무에 도전을 던져주고 있다. 이 연구는 현장에서의 수요에 기반하여 최신 트렌트와 스마트 TV 디지털 증거의 요구가 증가하고 있음을 확인하였다. 스마트 TV는 단순한 디지털 증거의 출처가 아니라 인터넷에 연결, 저장, 유저 클라우드 계정과 연동되어 디지털 수사에서 비중이 커지고 있다. 이에 일반적으로 알려진 방식들을 종합적으로 최신 스마트 TV 모델에 적용하여 그 결과를 도출하고 특히 Chip-Off 기법을 통해 적지 않은 데이터를 성공적으로 추출할 수 있음을 확인하였고, 다양한 기법들을 종합적으로 적용하는데 효율적인 절차모델을 제시하였다. 다양한 스마트TV를 망라하는 기법이 제시되기 어려운 상황에서 최신 스마트 TV를 대상으로 한 새로운 수사 절차 접근 방안은 향후 수월한 수사에 기여 할 것이다.

주제어 : IoT포렌식, 스마트TV, 삼성TV, VDFS, 타이젠

Ⅰ. Introduction

An increasing number of electronic products are now becoming “Smart” with the ability to access the Internet and connect to other remote devices [1]. Having the functions of a Legacy Television and the complexity of a computer, a Smart TV provides features such as web browsers, facial recognition, motion control, voice control, online games, built-in camera, and use of wireless transmission screen. It also supports users’ downloaded contents and applications [2]. Furthermore, Smart TVs come with inbuilt disk storage media, random access memory (RAM), third-party software’s, and full networking capabilities [3] all these with the ability to be crucial data-sources

※ This research was supported by the MISP (Ministry of Science & ICT) Korea, under the National Program for Excellence in SW supervised by IITP(Institute for Information & Communications Technology Promotion). (2018-0-00216)
- Received 09 September 2019, Revised 16 September 2019, Accepted 26 September 2019
- 제1저자(First Author) : Terrence Nemayire (Email : terrynema@hallym.ac.kr)
- 교신저자(Corresponding Author) : Yunsik Jang (Email : jakejang@hallym.ac.kr)

during digital investigations. Apart from Smart TVs being a digital data sources, they can store a lot of user data such as account and credit card information, ability to integrate with other internet accounts, hence these features can be exploited by criminals looking for private information such as real-time audio and visual access amongst other criminal activities [4].

In June 2016, a warrant was issued for Samsung Smart TV like any other computer whose owner had been convicted for possession of child pornography, and Feldman, the owner, admitted that he watched adult and child pornography on the device [5]. This research paper contributes to the area of digital investigation by presenting potential vulnerabilities and methods of data acquisition for investigating Samsung Smart TV model. The primary goal for this research was to acquire user data and any data from the Smart TV that can potentially have help an investigation for Law Enforcement Agencies (LEA). The secondary goal was and to develop an USB based data acquisition system from the Smart Tv.

Ⅱ. Related Work

There are a number of works that focus on data acquisition methods for Smart TVs, however recent works have focused on LG [6] and Samsung [3]. Various Smart TVs operate on different Operating System (OS) and hence varying security configurations, vulnerabilities and exploitations [7]. Recent analysis on Operating Systems has mainly focused Samsung's Tizen OS (an open source, Linux based kernel) [8].

[1] managed to perform an online firmware upgrade by impersonating Samsung's update servers, after discovering that the browser's TLS/SSL implementation was vulnerable to man in the middle attack, and identified six potential vulnerabilities: firmware, browser, Samsung applications, remote help management, AllShare, and remote control.

On the other hand, [10] draws attention to Tizen OS and points out that Tizen applications require signing in and only on the bases of privileges granted by the Tizen environment, once can exploit privileges that required root access.

The most recent Smart Tv Digital forensics [3] lists three data acquisition methods carried out on a Samsung Smart TV, UE40F7000SLXXN model, the eMMC five-wire, Chip-off, and Software based method. The eMMC five-wire method was not successful due to the failure in resetting the processor, however, chip-off was successful and used in making an image file. Software based method, SamyGO widget installed in a flash drive was used to gain root access, and the images of the full flash memory was made [3].

A comprehensive overview of the previous works on Samsung Smart TV data acquisition is listed in Table 1.

표 1 . 기존 타이젠 OS 분석 방법

Table 1. Tizen OS (Samsung) analysis methods in literature

Analysis Approach	Past work	Model used	Potential Digital Artifact
Development Tools	-	-	Tizen SDK/Emulator (Tizen 2.0)
Root Access	Boztas et al., 2015 [3]	UE40F7000SL (Legacy OS)	*Rooting method developed by SamyGO Forum* 1. Install Skype app 2. Set Skype to AutoStart 3. Upload SamyGO widget to Smart TV via USB drive
Data Analysis	Kang et al., 2014 [9]	UN46ES8000 (Legacy OS)	Binary Diffing: Compare Pre-Image with Post-Image after function testing
File System	Kang et al., 2014[9]	UN46ES8000 (Legacy OS),	24 Partition SquashFS
Identified User Actions	▪ Boztas et al., 2015 [3], ▪ Kang et al., 2014 [9]	▪ UE40F7000SL (Legacy OS), ▪ UN46ES8000 (Legacy OS)	▪ Last TV on time ▪ Log policy configuration file ▪ App Install History ▪ Camera Usage ▪ Internet history ▪ Thumbnails of recently played video clips ▪ Recently executed service ▪ Saved TV channel list ▪ External storage usage info
Vulnerability	Sidiropoulos & Stefopoulos, 2013 [1]	UES5500	▪ Firmware Attack: firmware files can be customized using a tool developed by SamyGO and used for unauthorized privileges such as root access. ▪ Browser Attack: Man-in-the- Middle tools such as Burp Suite could be used to intercept traffic and modify requests and responses. ▪ Via Apps: using an app developed by SamyGO community to get root access

Ⅲ. Materials and Methods

1. Smart TV model selection

As one of our primary objectives was to test if the past data acquisition methods were still valid on recent Smart TV models, we have used Samsung UN43NU7150FXKR, a post 2017/2018 device. Samsung products make the first top 10 in popularity [11] and are readily available in most parts of world including South Korea [9] and Europe. The selected TV has the critical basic features of a smart TV and this model runs on Tizen 4.0 OS as of 31st August, 2018 [12].Table 2. depicts a detailed comparison between the model used in previous researches and our own.

표 2. 본 연구와 [3]에 사용된 스마트 TV 모델 비교
Table 2. Identification of device used for this research compared to [3]

Comparison Attributes	2014 Model	2018 Model
	UE40F7000SLXXN	UN43NU7400FXKR
Tv Release Year	2013-2014	2018
Operating Systems	Legacy Platform Orsay OS (LiMo)	Tizen 4.0
Storage Medium	4Gi Movi NAND flashchip	4Gig eNAND
File System Analysis	SquashFS 4.2	VDFS (Versatile Distributed File System)
Deployable Applications Extensions	*.wgt and *.tpk	*.wgt, *.rpm and *.net Png, txt, tx?, exe, tz, jpg, gz, sqlite, gif, ogg
Application Types	Native Applications Web Applications	Web Applications, HTML5, NET Core, Native Subsystems, .NET APIs
Application Rights Isolation - Privilege	Public, Partner and Platform	Developer
Network Protocols	HTTP/s, TCP, and UDP	: GIOP, HTTP/s, HTTP/XML, ICMP, IGMPv2, ISAKMP, MDNS, NBNS, PORTMAP, RPC, SIP, SNMP, SSDP, SSLv3, TCP, and UDP.
Encryption	TLS V1.2	TLS v1.2

2. Research Procedure

To our knowledge, there has not been a published or known standard Smart TV investigation procedure yet. In literature, investigators have suggested various methods to acquire data from the TV as suggested in Table 1 in the previous section.

Based on the past research results and our own analysis, we propose the formulation of a basic workflow standard towards Smart Tv investigation. Refer to Figure 1 below that was modeled on the work done in carrying out this research (Investigation).

The investigation procedure focused on network access (http/s traffic interception, and vulnerability scanning), hardware access (interfaces, vulnerability exploitation, chip-off) and further investigation and lastly at application level (development and deployment of test applications.

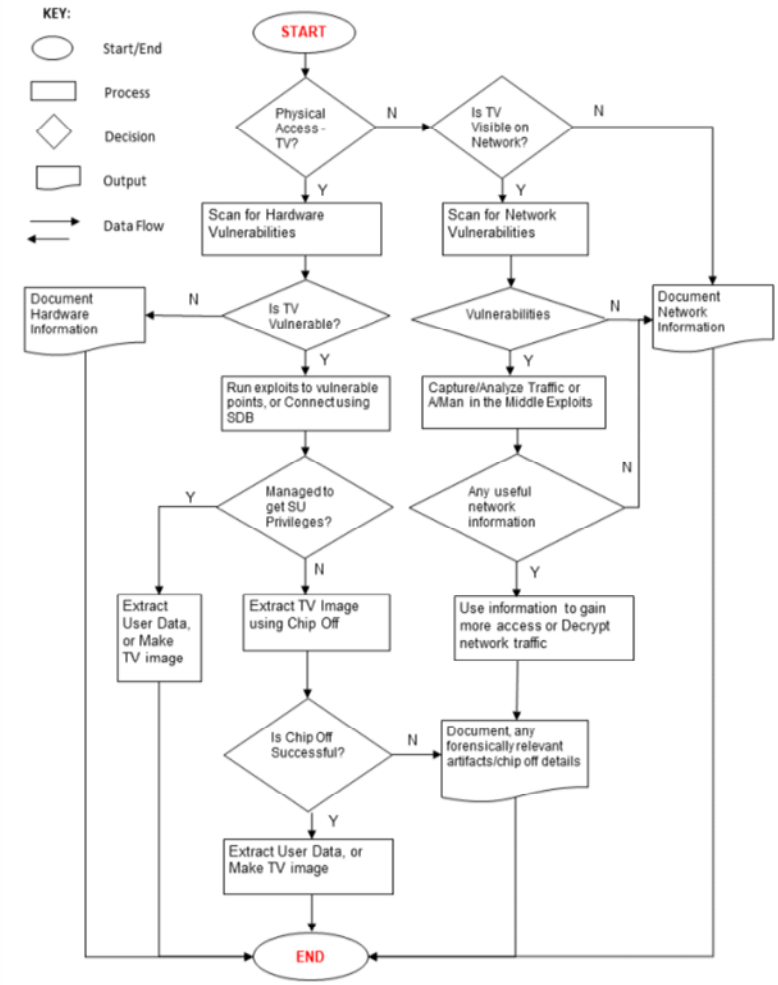


그림 1. 2018 삼성 스마트 TV 수사 절차 제안

Figure 1. 2018 Samsung Smart TV - Investigation Workflow (edited by authors)

Ⅳ. Analysis and Findings

1. Application Level

1.1. Root Access

The rooting method used by [3] in exploiting Skype application did not work as Skype was not available in Tizen app store, and the Tizen 4.0 had patched that vulnerability, Also using SDB, Tizen.40 has disabled the $root ON/OFF command and #./sdb shell command, hence restricting direct access to Tizen Kernel.

1.2. Tizen Application Deployment

This approach was previously used to obtain root access and search other ways to exploit Tizen OS using modified Tizen applications needing root privileges and exploit possible buffer overflows [9]. Although Tizen began supporting .NET development environment with .NET Core, Native Subsystems, .NET APIs, and Runtimes added, in case of TV product, using Native Application is blocked for security reason [8]. Thus, only the installation and execution of HTML5 web applications is possible on the Tizen 4.0 Smart TV model.

표 3. 핵심 타이젠 소프트웨어
Table 3. Tizen Core Software

Tizen Studio	A package of Tizen SDB that contains tools and managers under, also workspace for coding.
Device Manager	It provides connection and configuration between PC and Tizen devices including emulators.
Certificate Manager	It provides configurations on certificates to install both native and web application of Tizen.
SDB	It provides a software-based bridge to connect to the Tizen device.

With the new Tizen 2.5 and above versions, during application development and deployment on smart tv, Samsung developers (partners) are required to install "Samsung Certificate Extension" from Package manager, which means both TV and wearable device needs higher privilege of certificate than normal certificate, hence every application developer has to be authentically registered with Samsung in order to get smart tv certificates.

1.3. Application Installation

Developing a Tizen application requires a particular certificate from developing stages because Samsung does not want an illegal distribution of its applications. The certificate stores information about specific device data that can allow application installation. Installing an application on the emulator and SDB failed because the app did not have a proper certificate. Then, even after installing Samsung Certificate Extension and using Certificate Manager to issue and upload a proper certificate, the install command was rejected. As a result, installing a compiled package is done but it works only for the "Samsung TV Web Simulator". Executing app in the real device and VM-based emulator has failed. It seems it has but since there is two duplicated install paths on it.

1.4. Running Executable Files

A USB flash drive was connected to the Smart TV via USB port to run executable files from the flash drive. However, the Smart TV only showed media files such as .jpeg and .mp3 available for opening on its system. When we tried to download executable files from google browser, a pop-up window, 'This function is not supported,' came up and downloading process stopped. Tizen 4.0 may have disabled the download functionality for third party software.

Tizen 4.0, has been developed to allow files from the following family formats; png, txt, tx?, exe, tz, jpg, gz, sqlite, gif, ogg and other media file formats.

2. Network Level

2.1. Network Access

Wireless connection was established between hosts PC and the Smart TV by enabling Developer Mode and setting Host PC IP on the TV, and the host PC and Smart TV were connected via SDB (Smart Development Bridge), however connection could only be established if both Host PC and Smart TV were on the same network and Host IP having to be manually set and granted access to communicate with the TV.

2.2. Port Scanning

Port scanning software, Zenmap (version 7.70), was used to look for the listening ports and check their availability for exploitation. All range of ports of Smart TV's IP from 1 to 65535 was scanned, and 17 listening ports are found. Then, Telnet was used to check if those ports are open.

표 4. UN43NU7150 - 포트 번호와 기능
Table 4. UN43NU7150 TV - port numbers, functions

Port Number	Function	Remarks
1515	N/A	Accepts telnet request but rejects after 2 characters
26101	SDB connection port	Accepts telnet request but soon close connection
8080	Web server (lighttpd)	Shows '404-Not Found' page in browser
7678, 8187, 9110, 9197	UPnP 1.1 Ports	Only respond to UPnp-related packet - It runs 'Samsung Allshare unpnd 1.0,' and returned error describes Samsung's service
8001	vcom-tunnel	Shows nothing via web browser, but returns HTML-based page when connected with telnet
8002	teradataordbms	- accepts requests but no useful data returned - DB commands were given but soon rejected
9012	Websocket++ 0.5.1	- With web browser, page shows 'got HTTP request with 0 bytes of body data.'

3. Device Level

3.1. Chip-Off (Procedure)

As the final data acquisition method, chip-off was used on the eMMC chip (See Figure 2,3). In our research, this was the most successful method to gain access to user data. Therefore, in this section we will discuss the chip-off procedure for the UN43NU7400FXKR and summarize our finding directly after chip-off. The detailed result of analyzing the acquired data will be elaborated in the next section (V) separately.

The chip-off method uses heating guns to de-solder the eMMC chip from the motherboard (See Figure 4). After successfully detaching the chip from the motherboard, the chip is carefully cleaned placed on an eMMC reader and connected to the computer (See Figure 5). MD-Reader® and MD-NEXT® used in this analysis are registered trademarks of HancomGMD Corporation.

그림 2. 삼성 스마트 TV 메인보드
Figure 2. Samsung Smart TV Motherboard

그림 3. 삼성 스마트 TV eMMC 칩
Figure 3. Samsung Smart TV eMMC chip

그림 4. 스마트 TV 메인보드에서 칩을 분리하는 히팅머신
Figure 4. Heating machine desoldering chip from Smart TV motherboard

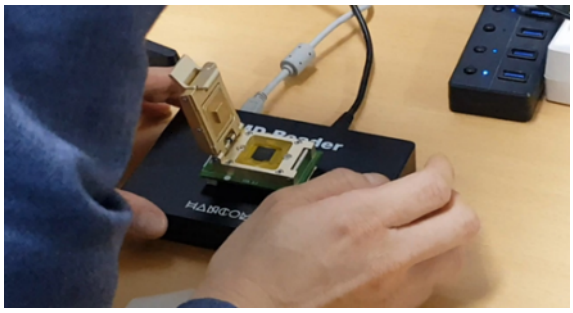


그림 5. eMMC 칩을 읽고 있는 MD-Reader
Figure 5. Reading the eMMC chip using MD-Reader

It should be noted that the chip-off process needs to be the last step of data acquisition. After the removal, the chip will most likely not be able to be re-attached to the motherboard to function to its full capacity.

Using MD-Reader(an eMMC reader hardware that supports several eMMC & eMCP sockets) and MD-NEXT (data extraction software), we were able to successfully read the disk image file, a 4G eNAND type with twenty-four (24) partitions. Analysis from the chip showed that Samsung has used of its own Vertically Deliberate improved performance File System (VDFS) since January 2017 [12]. VDFS is a verified high-performance file system that supports applications running high speed and performance databases eg. on web applications [14].

3.2. File System

Results from the chip-off method showed that there are 26 partitions as highlighted in Figure 6 below. With identical volume names following themselves; which is the primary and backup partitions. See Figure 7 highlighting the backup and primary entries of the unallocated partitions for vol1 and vol26 respectively. The partitions Platform.img, Systemrw.img, NONE contain data about the system and data.img contains most of the user-relevant data we have found in our research. Further analysis of the images was done using various commercial and open source-forensic softwares.

Name	ID	Starting Sector	Length in Sectors	Description	Flags
vol1 (Unallocated: 0-127)	1	0	128	Unallocated	Unallocated
vol4 (ddr.init: 128-1151)	4	128	1024	ddr.init	Allocated
vol5 (ddr.init: 1152-2175)	5	1152	1024	ddr.init	Allocated
vol6 (seret.bin: 2176-6271)	6	2176	4096	seret.bin	Allocated
vol7 (seret.bin: 6272-10367)	7	6272	4096	seret.bin	Allocated
vol8 (uImage: 10368-41087)	8	10368	30720	uImage	Allocated
vol9 (uImage: 41088-71807)	9	41088	30720	uImage	Allocated
vol10 (dtb.bin: 71808-73855)	10	71808	2048	dtb.bin	Allocated
vol11 (dtb.bin: 73856-75903)	11	73856	2048	dtb.bin	Allocated
vol12 (sign.bin: 75904-76031)	12	75904	128	sign.bin	Allocated
vol13 (sign.bin: 76032-76159)	13	76032	128	sign.bin	Allocated
vol14 (VD-HEADER: 76160-76287)	14	76160	128	VD-HEADER	Allocated
vol15 (secos.bin: 76288-80383)	15	76288	4096	secos.bin	Allocated
vol16 (secos.bin: 80384-84479)	16	80384	4096	secos.bin	Allocated
vol17 (secos_drv.bin: 84480-86527)	17	84480	2048	secos_drv.bin	Allocated
vol18 (secos_drv.bin: 86528-88575)	18	86528	2048	secos_drv.bin	Allocated
vol19 (NONE: 88576-92671)	19	88576	4096	NONE	Allocated
vol20 (NONE: 92672-117247)	20	92672	24576	NONE	Allocated
vol21 (platform.img: 117248-2984447)	21	117248	2867200	platform.img	Allocated
vol22 (platform.img: 2984448-5851647)	22	2984448	2867200	platform.img	Allocated
vol23 (systemrw.img: 5851648-5954047)	23	5851648	102400	systemrw.img	Allocated
vol24 (data.img: 5954048-7625583)	24	5954048	1671536	data.img	Allocated
vol25 (reserved: 7625584-7633775)	25	7625584	8192	reserved	Allocated
vol26 (Unallocated: 7633776-7634943)	26	7633776	1168	Unallocated	Unallocated

그림 6. 2018 스마트 TV 파티션
Figure 6. 2018 Smart TV Partitions

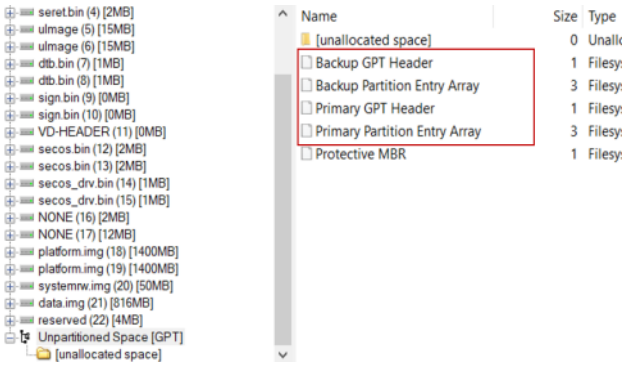


그림 7. 주 파티션과 백업 파티션
Figure 7. Primary and Back Partitions

As shown below, data.img from the 2018 Smart TV image file shows the name of the File System.

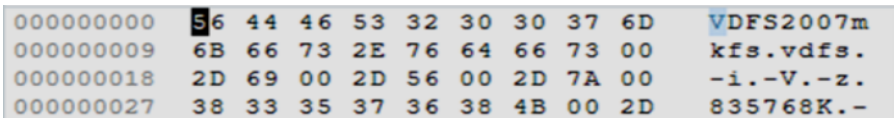


그림 8. Hex Viewer로 추출한 파티션 20 (data image)의 헤더 파일
Figure 8. Hex Viewer extract from Partion 20 (data image) header file

V. Chip-Off Image Analysis

The image files were analysed using Autopsy (version 4.8.0), Magnet Axiom Forensic Software and MD-Red (version 3.0, with UN43NU7150 specific module). Applications images, audio clips and application downloaded video samples were discovered in the Data image and most of these pre-loaded during application installation or deployment.

1. Recovered Media Files

Applications images, audio clips and application downloaded video samples were discovered in the data.img and most of these pre-loaded during application installation or deployment. Below are multi-media images, either accessed or loaded with applications by the user. Regardless of the user's intention, these images are automatically saved and provides a context to user activities. By analyzing the images and the three pieces of data indicated in each file's name (Unused, 9-digit value, 4-digit value), an investigator can better reconstruct the timeline of user actions (See Figure 9).

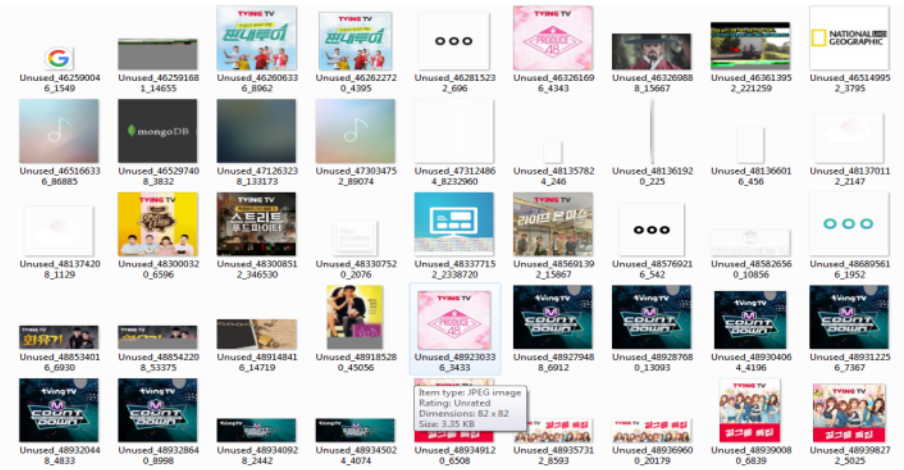


그림 9. MD-RED에서 복구한 이미지
Figure 9. Recovered Images in MD-RED

Active multimedia files such as audio (wav), pictures (png) and movie (mp4) files were recovered from the Smart TV images, as potential artifacts that can be used for digital investigations.

2. Browsing History

Web search and browsing history, was identified from the data image (Partition 24) that was analyzed, this is potential source for digital evidence from a Samsung Smart TV. Some activities had time stamps that is crucial for event reconstruction and timeline analysis.

http://opensource.samsung.com/opensource/18_DTV_K...	Potential Browser Activity	Web Related
http://opensource.samsung.com/opensource/18_DTV_K...	Potential Browser Activity	Web Related
http://pip-ssetvplus.cjenm.skcdn.com/CLIP/EA/B1201801...	Potential Browser Activity	Web Related
http://smart.hallym.ac.kr/dwr/util.js	Potential Browser Activity	Web Related
http://smart.hallym.ac.kr/lmsdata/js/common-hallym.js	Potential Browser Activity	Web Related
http://smart.hallym.ac.kr/lmsdata/js/common.js	Potential Browser Activity	Web Related
http://smart.hallym.ac.kr/lmsdata/js/common_button.js	Potential Browser Activity	Web Related
http://smart.hallym.ac.kr/lmsdata/js/common_conf.js	Potential Browser Activity	Web Related

그림 10. TV의 인터넷 사용 기록
Figure 10. Browsing history of the TV

3. System Information

Figure 11 shows system information of the Samsung Smart TV, showing , model, name, maker and the exact serial number. These values are crucial for particularizing to an individual model involved in a criminal event.

☑	1	Active	Maker	Samsung Electronics	Device Information
☑	2	Active	Model	UN43NU7150	Device Information
☑	3	Active	Name	[TV] Samsung 7 Series (43)	Device Information
☑	4	Active	Serial Number	05TX3NDK900237F	Device Information

그림 11. MD-RED에서 복구한 시스템 정보
Figure 11. System Information in MD-RED

4. Network Information

Figure 12 shows network information log carrying, last known device IP address, Wifi Names, SSID, network frequency and last modified time. Based on the network information, an investigator can predict the location of the suspect at a particular time, which is crucial for reconstruction of timeline and corresponding user activities.

☑	1	Active	Wifi	Last address : 10.50.228.154	Network Log
☑	2	Active	Wifi	Name : Hallym WiFi SSID : 48616c6c796d2057694669 frequency : 2462	Modified Time : 11/13/2018 07:13:59 Network Log

그림 12. MD-RED에서 복구한 네트워크 정보
Figure 12. Network Information in MD-RED

5.Application Installed and App ID

Web Figure 13 shows the installed applications and app ID. It shows pre-installed applications as well as applications that were installed by the user (e.g. "Flying Fish" in Figure 13).

1	Active	App Name : 핫쟈플레이	ZeGzXSgDov			AppInfo
2	Active	App Name : Melon	YgmIZRmiap			AppInfo
3	Active	App Name : Sotheby's	WiZj7McGNU			AppInfo
4	Active	App Name : e-Manual	UrrQtLiSUP			AppInfo
5	Active	App Name : Netflix	RN1MCdNq8t			AppInfo
6	Active	App Name : Google Play Movies & TV	QizQxC7CUf			AppInfo
7	Active	App Name : acm-service	org.tizen.acm-service			AppInfo
8	Active	App Name : Flying Fish	M4UT1lus05			AppInfo
9	Active	App Name : Plex	klciSQlYEM			AppInfo

그림 13. 설치된 애플리케이션과 앱 ID
Figure 13. Installed Applications and App ID

6. Active SQLite Databases

Multiple databases were found in the data.img partition (See Figure 14). The last modified time fits with the last usage time of the Smart TV (2018 Nov 13). SQLite is a valuable source of forensic evidence because when a user deletes data SQLite database declares the corresponding location as unallocated; then, until other records are over-written on that location the 'deleted' data can still be recover. Thus, an investigator can restore the data in 'unallocated' location.

Index	State	Type	File Path	File Name	Analyz...	Script App	Used Table	Time
1	Active	SQLite3	/dbspace	.pkgmgr_parser.db	○	AppInfo	package_info	Create Time : 12/12/2018 22 Modify Time : 11/13/2018 14:07:38
2	Active	SQLite3	/dbspace	.webappservice.db	○	AppInfo	widgetinfo	Create Time : 12/12/2018 22 Modify Time : 11/13/2018 19:28:35
3	Active	SQLite3	/usr/home/owner/.applications/dbspace	.media.db	○	Media Log	media	Create Time : 12/12/2018 22 Modify Time : 11/13/2018 19:24:38
4	Active	SQLite3	/usr/home/owner/apps_rw/org.tizen.browser/data/db	.browser-data.db	○	Browser	bookmark,history	Create Time : 12/12/2018 22 Modify Time : 11/13/2018 19:34:23
5	Active	SQLite3	/var/lib/buxton2	system.db	○	System Log	buxton	Create Time : 12/12/2018 22 Modify Time : 11/13/2018 16:58:40

그림 14. MD-RED에서 복구한 데이터베이스
Figure 14. Databases in MD-RED

7. System logs for Power ON and OFF activity

The log file shows when the Smart TV was turned on and off and time stamps of the actions. This set of logs can help an investigator reconstruct an attack by analyzing the relationship between the events and their time stamps. Furthermore, if there is an action with a suspicious time stamp, such anomaly may provide an insight for the reconstruction process as well [15].

	Index	State	Type	Item	Time	App
☑	1	Active	System Log	Power Off	11/13/2018 15:21:47	System Log
☑	2	Active	System Log	Power Off	10/15/2018 13:01:23	System Log
☑	3	Active	System Log	Power Off	10/16/2018 17:16:01	System Log
☑	4	Active	System Log	Power Off	10/16/2018 17:53:40	System Log
☑	5	Active	System Log	Power On	11/13/2018 13:51:22	System Log
☑	6	Active	System Log	Power On	10/16/2018 17:16:03	System Log

그림 15. MD-RED에서 복구한 시스템 on/off 로그
Figure 15. System on and off logs in MD-RED

VI. Conclusion

This Smart Tv research paper highlighted and examined the Smart TV device, from hardware, application and network level in order to determine possible sources of digital evidence that can be forensically acquired and is sound in a court of law. With the lack of a standard research procedure or investigation model, this work was carried out using the best possible means, taking into consideration all known past research methodologies and procedures.

In analysis, even though many of the previous data acquisition methods cannot be applied to the newer TV model, the Samsung 7 Series (UN43NU7150FXKR-2018) model still proved to be reliable source for potential digital forensic evidences, since it stores various user data ranging from media files (images, audio files, video files), browsing history, google searches. It is important to point out that this research work was made in the view that Smart device being investigated is available and the investigator has direct access to the device.

Acknowledgement

We thank HancomGMD for providing the necessary digital forensic tools and insight to this research, especially during chip-off analysis.

참 고 문 헌 (References)

[1] N. Sidiropoulos and P. Stefopoulos, SMART TV HACKING, University of Amsterdam, 2013.
Available: https://www.delaat.net/rp/2012-2013/p39/report.pdf

[2] H.Ma and Q. Guo, Design of functions in Smart TV (Unpublished master's thesis). University of Gävle, 2018.
Available: https://pdfs.semanticscholar.org/3c59/1b8073f23473262ebe8a3d920c0b9bb865b6.pdf

[3] A. Boztas, A.R.J. Riethoven, and M. Roeloffs, Smart TV forensics: Digital traces on televisions. Digit. Investig. 12, S72 - S80, 2015.

[4] I. Alam, S. Khusro, and M. Naeem, A review of smart TV: Past, present, and future, 2017 International Conference on Open Source Systems and Technologies (ICOSST), 2017.

[5] T. Brewster, That Time Cops Searched A Samsung Smart TV For Evidence Of Child Abuse. Forbes, Feb 7, 2017.
Available:
https://www.forbes.com/sites/thomasbrewster/2017/02/07/samsung-smart-tv-fed-search-child-pornography/#3fe381b317d7

[6] I. Sutherland, K. Xynos, H. Read, and A. Jones, T. Drange, K. Xynos, A forensic overview of the LG Smart TV, 2014.

[7] A.Abraham, Hacking Tizen: The OS of Everything, White Paper, 2015.
Available:
https://conference.hitb.org/hitbsecconf2015ams/wp-content/uploads/2015/02/WHITEPAPER-Hacking-Tizen-The-OS-of-Everything.pdf

[8] S. Suzuki, Tizen Security, Fourteenforty Res. Inst, 2014.

[9] H.S. Kang, M.S. Park, and S.J. Kim,Study on Smart TV Forensics. J. Korea Inst. Inf. Secur. Cryptol. 24, 851 - 860, 2014.

[10] I. Asrar, Attack Surface Analysis of The Tizen OS, Virus Bulletin Conference September,2014.

[11] 4K.com, The Best 4K HDR TVs For Every Budget - Reviews of 4k Smart, Curved, LED & Flat Screen TV - Sony, Samsung, LG, Vizio & More, 2018.
Available: http://4k.com/tv/

[12] Tizen Project, Tizen, n.d. Retrieved November 10, 2018,
Available: https://www.tizen.org/

[13] Tizen, Developer: Tizen SCM Tools Release - Version 17.01 [WWW Document], 2017.
Available: https://www.iotgadgets.com/2017/01/developer-tizen-scm-tools-release-version-17-01/

[14] A. V. Konradi, Performance Optimization of the VDFS Verified File System, MASSACHUSETTS INSTITUTE OF TECHNOLOGY, 2017.

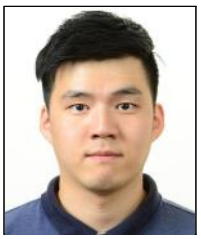
[15] H. Studiawan, F. Sohel, and C. Payne, A survey on forensic investigation of operating system logs, Digital Investigation, 29. 1-20, 2019.

저 자 소 개

Terrence Nemayire
정회원
2008년 11월: Midlands State University (Zimbabwe), Information Systems 졸업
2018년 3월~현재 : 한림대학교 대학원 정보법과학 석사과정
관심분야 : 디지털 포렌식, 암호학, 사이버 안보 등

Alex Ogbole
정회원
2017년 11월 : Benue State University (Nigeria), Computer Science 졸업
2018년 3월~현재 : 한림대학교 대학원 정보법과학 석사과정
관심분야 : 디지털 포렌식, 사이버 보안 등

박 성 미 (Sungmi Park)
정회원
2019년 2월 : 한림대학교 정보법과학과 졸업
2019년 3월 ~ 현재: 한림대학교 대학원 정보법과학 석사과정
관심분야 : 디지털 포렌식, 디지털 포렌식 자동화, IT 법 등



김 기 철 (Keecheol Kim)
정회원
2018년 3월~현재: 한림대학교 글로벌학부 정보법과학과전공 재학
관심분야: OSINT, 네트워크 포렌식 등

정 연 석 (Yeonseok Jeong)
정회원
2014년 3월~현재: 한림대학교 글로벌학부 정보법과학전공 재학
관심분야: 하드웨어 포렌식 등

장 윤 식 (Yunsik Jang)
정회원
1994년 3월~2005년 2월 : 경찰청(사이버테러대응센터 등) 근무
2005년 2월~2014년 2월 : 경찰대학(경찰학과 교수, 국제사이버범죄연구센터장)
2015년 3월~현재: 한림대학교 글로벌학부 교수
2017년 3월~현재: 한림대학교 글로벌융합대학 정보법과학연구소 소장
관심분야 : 사이버범죄, 디지털 포렌식, 범죄데이터분석