Further Analysis on Smart TV Forensics

Minsu Park, Heesoo Kang, Seungsoo Baek, Seungjoo Kim

Center for Information Security Technologies (CIST), Korea University, Republic of Korea
{minsoon2, kukulux, offident79, skim71}@korea.ac.kr

Abstract

Smart devices have become an important part of our life due to improvements in IT technology and corresponding increase in demand for smart devices. In particular, smart TVs represent a convergence of computers and TV and have become popular. Therefore, many researchers conduct smart TV forensics to accurately and seamlessly investigate a suspect's actions. However, previous works have focused not on critical information, such as viewing history, but on minor information such as web surfing history and system configuration information in smart TVs. To make matters worse, minor information is irrelevant to time or order. Therefore, it is inadequate to use previous methods to investigate and rearrange the order of a suspect's action. We therefore propose a novel method to obtain time relevant information in smart TVs. We find additional information, such as the list of TV channels that are watched, the last viewing time, recent service history, information on recently played video and recent camera usage information.

Keywords: Digital forensic Investigation, Smart CE forensics, Smart TV

1 Introduction

Technological convergence between computers and appliances has produced smart TVs that have become an important part of our life. The number of smart TV users is increasing, and according to Parks Associate's report [1], the distribution rate of smart TVs in North America and Eastern Europe is expected to increase from the current 38% and 32% in 2015 to 62% and 54% in 2016, respectively. A smart TV not only provides traditional television functions, but also allows viewers to search content through the Web, install games, watch videos or photos, etc. Recently, smart TVs have begun to record when and what channels the viewer is watching. Moreover, it recommends an optimal TV program by analyzing user behavior. In order words, a smart TV may be aware of the user's behavioral patterns.

The Korea Communication Commission (KCC) is a branch of Korean government, and it announced the results of a survey of the daily usage rate of media, including TV, PCs and smartphones, according to ages [2]. The results indicate that young people in their 20's to 40's have a much higher usage rate for smartphones and PCs than people over 60. However, the result showed that most respondents watched TV regardless of age. In order words, people of all ages consistently spend time watching TV. This fact has a significant meaning for digital forensics. Before smart TV forensics, digital forensics mainly depended on the analysis of a suspect's PC or smart phone to obtain evidence. However, it was not sufficient for an investigator to trace evidence because a suspect may not use only a PC or smartphone all day long. Moreover, if the suspect is older, the probability that the inspector could obtain any information from a PC or smart phone might be low. Considering the results of the KCC survey [2], smart TV forensics can be very helpful because these strengthen the time gap defect of computer or smart phone forensics. In addition, since a smart TV is generally located in a fixed place, such as an office or suspect's home, an investigator can easily conclude the flow of the suspect's actions.

Smart TVs were first released in 2010, and many researchers have studied smart TVs. Sutherland et al. [3-4] addressed the importance of smart TV forensics and conceptually explained that some information could be obtained through the system information and network configuration. However, he used an outdated version of the firmware and the amount of information was too small to reconstruct a suspect's actions as legal evidence. Boztas et al. [5] presented additional information that could be obtained from smart TVs in DFRWS 2014. He also analyzed the user's web access history and media files stored in a smart TV. However, his study mainly focused on functions other than viewing TV. He focused on minor functions in smart TVs such as, Internet usage or the analysis of media files. As mentioned above, people purchase smart TVs for the main purpose of watching TV. In other words, the analysis in [5] could be insufficient to investigate and rearrange the order of the suspect's actions because the data are not largely associated with time or order.

*Corresponding Author: Seungjoo Kim; E-mail: skim71@korea.ac.kr
DOI: 10.3966/160792642018081904009

Therefore, we propose a novel method to obtain information relevant to time or order from a smart TV. We find that the additional time or order based information, such as the TV channel list that has been watched, the last viewing time, the recent service history, recent video playback information and recent camera usage information. This paper consists of the following sections. Section 2 introduces an overview of digital forensics and related works. Section 3 explains the smart TV forensics method and analyzes the user's actions from time or order related information and static information. Section 4 shows a comparison with previous work with our experimental result. Section 5 concludes our paper.

2 Preliminaries

2.1 Overview of Digital Forensic

Digital forensics is a kind of forensic science that encompasses the recovery and investigation of materials found in digital devices [6-7]. Since digital materials are easily manipulated or damaged, an investigator must prove their integrity and should ensure these have legal force in court. Therefore, an investigator follows procedures to collect media, examining data, analyzing information and report these as evidence. Figure 1 shows the general procedure for digital forensics.

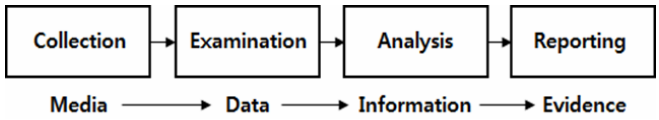


Figure 1. Digital forensic analysis process

Traditional digital forensics has mainly focused on computers, such as PCs or mainframe computers. However, the growth in Internet usage and the development of network connected devices has expanded the domain of digital forensics. Nowadays, digital forensics mostly deals with not only computers but also smart devices, such as smart phones. Table 1 presents the branches of digital forensics [8]. With the advent of the Internet of Things (IoT), smart appliances, such as smart TVs, have also been rapidly developed. On the other hand, there are few digital forensics methods for smart appliance because the platforms of the appliances vary by vendor. In this sense, our work can contribute to the forensics of smart appliances.

Table 1. Branches of digital forensics

Area	Content	Target Equipment
Disk Forensics	Analyzing files on a hard disk and recovering deleted data	PC
Memory Forensics	Acquiring data, encoded keys, and passwords that exist in RAM	PC, Smartphone
Document Forensics	Exploring remaining data when using electronic documents such as Word, Excel, and PowerPoint files	PC
Email Forensics	Analyzing sent/received emails and investigating altered emails	PC, Smartphone
Web Forensics	Tracing user's Internet usage history, such as Web history, favorites, and search words	PC, Smartphone
Network Forensics	Acquiring network information, such as network configuration and packets	Network equipment
Cloud Forensics	Exploring cloud service usage history and files used	PC, Smartphone
Mobile Forensics	Collecting and analyzing trace data existing on mobile devices	Smartphone

2.2 Related Works and Limitations

Early studies on smart TVs mainly focused on hacking methods to find security vulnerabilities. Grattafiori and Yavor [9] and Lee and Kim [10] initially addressed the security vulnerabilities of smart TV and the probable risks in the case where a smart TV is attacked. On the basis of [9-10], Falayleh [11], Sutherland et al. [4] and Boztas et al. [5] mentioned the necessity to conduct smart TV forensics and the study of its conceptual procedure. Then, Sutherland et al. [4] presented an experimental study on smart TVs by using the LG smart TV and mentioned the kinds of basic information that were obtainable. However, it was so simple that the investigator could not recognize and reconstruct the suspect's past actions only with information related to system and network configuration. Boztas et al. [5] stated that additional information, such as website access logs, lists of installed applications, stored media files and camera activity history could be obtained using a disk dump. In general, most people spend much time watching TV even though smart TVs have many functions. Therefore, the main component of smart TV forensics should be to analyze the TV viewing history. However, [5] focused on secondary functions rather than on the main functions. In addition, the results of [5] are not associated with time, so it is not enough in order for the investigator to rearrange the suspect's actions as digital evidence. Thus, it is necessary to investigate and obtain data that focuses on TV viewing.

3 Our Experimental Forensics on Smart TV

3.1 Material Environment

In this section, we describe the material environment for our experiment. We used a Samsung smart TV with model number un46es8000. The reason we chose a Samsung smart TV was that it was the most popular smart TV in 2014 [12]. The internal composition of un46es8000 is very similar to that of any computer. In addition to a TV tuner, it has an ARM based CPU, DDR3 main memory, a WiFi module and an Ethernet port for network communication. The firmware version is TECPAKUC 1041.1, BT-S/G, which is modified from Linux.

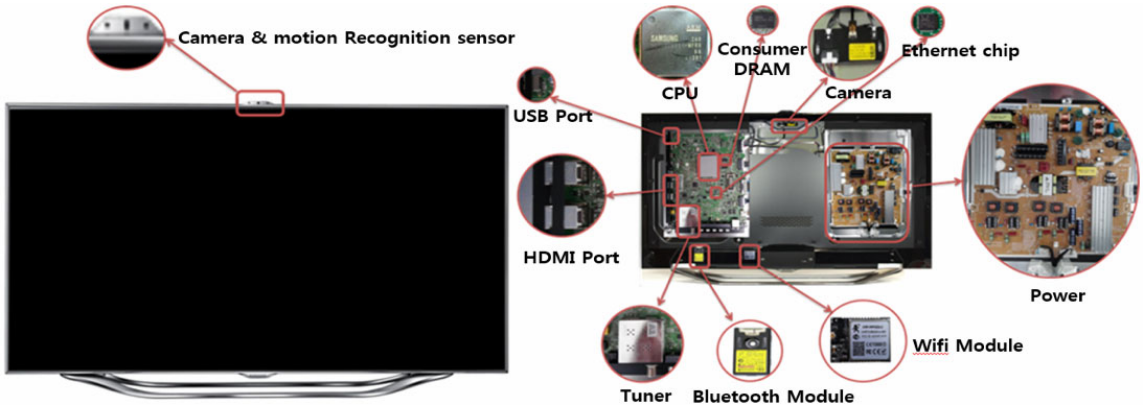


Figure 2. Samsung Smart TV (un46es8000)

3.2 Methods

In this section, we address the methods for smart TV forensics. In order to trace a suspect's actions, we should first understand the internal structure of the target smart TV and its file system. As with the digital forensics procedure in Section 2, we used the following method for Smart TV forensics: (1) acquiring root privilege (2) understanding the internal structure (3) collecting and examining data (4) analyzing information and producing a report.

Acquiring root privileges. An investigator has to acquire system root privileges to image the data in order to analyze the system and file structure of a smart TV. In general, a disk dump method is available for the root authorization conditions. We have used the system vulnerability of the Linux system mentioned in Ref. [10] to obtain root privileges. Then, we imaged the entire data on the target by using the 'dd' program in the firmware. In order to acquire root privileges on the smart TV, an application is required to installed, which exploits vulnerabilities. It, however, does not overwrite any data on the smart TV due to the fact that the application is installed in a portion of the unallocated memory. The collection and survey of the data, accordingly, do not affected. Although this method does not guarantee the integrity of a disk, it is currently the best method. Boztas used Samygo root tools and the same problem occurs [6]. In the case of smart phones, digital forensic analysis also goes through a rooting process. Depending on the types of smartphone, the same problems occur [14]. Therefore, it is necessary to study the rooting method, which does not write data in a data area, to solve the integrity issue.

Understanding internal structure: An investigator should understand the internal structure to analyze the files that are needed. However, a file system in smart TV varies according to vendors. Samsung usually uses a RFS (Robust File System). But through empirical analysis, VFAT (Virtual File Allocation Table) file system was identified. Figure 3 shows its mount information for current flash memory and VFAT file system.

```
/dev/mmcblk0p12 on /mtd_rwarea type rfs (rw,relatime,vfat,llw,iocharset=utf8)
/dev/mmcblk0p10 on /mtd_drmregion_a type rfs (rw,relatime,vfat,llw,iocharset=
/dev/mmcblk0p11 on /mtd_drmregion_b type rfs (rw,relatime,vfat,llw,iocharset=
/dev/mmcblk0p15 on /mtd_rocommon type squashfs (ro,relatime)
/dev/mmcblk0p17 on /mtd_contents type rfs (rw,relatime,vfat,llw,iocharset=utf
/dev/mmcblk0p19 on /mtd_rwcommon type rfs (rw,relatime,vfat,llw,iocharset=utf
none on /proc/bus/usb type usbfs (rw,relatime)
```

Figure 3. Mount information

Thus, we have referred to the VFAT file system that is openly provided on the Internet to understand the structure. Referring to [13], we can more easily be aware of the system and file structure in a smart TV. Table 2 shows the major parts of the partitions for un46es8000.

Table 2. Major parts of the functions on un46es8000.

Device Boot	Path	File System
/dev/mmcblk0p10	/mtd_drmregion_a	RFS (VFAT)
/dev/mmcblk0p11	/mtd_drmregion_b	RFS (VFAT)
/dev/mmcblk0p12	/mtd_rwarea	RFS (VFAT)
/dev/mmcblk0p14	/mtd_exe	-
/dev/mmcblk0p15	/mtd_rcommon	-
/dev/mmcblk0p16	/mtd_emanual	RFS (VFAT)
/dev/mmcblk0p17	/mtd_contents	RFS (VFAT)
/dev/mmcblk0p18	/mtd_swu	RFS (VFAT)
/dev/mmcblk0p19	/mtd_rwcommon	RFS (VFAT)

Data collection and examination. The purpose to collect and examine data is to understand the connectivity and dependency between the files and functions in a smart TV. For example, if we first turn on a smart TV, some data files can be used and may affect other related files. First, to collect and examine data, we have enumerated the smart TV functions, such as turning on the TV, selecting the channels, installing and playing applications, storing media files and so on. Next, to determine which files are involved in those functions, it is necessary to check the binary changes in the files before and after operating the functions. Thus, we followed these steps: (1) pre imaging (2) testing (3) post imaging and (4) binary diffing. First, in the pre imaging step, we imaged the entire disk volume before operating the functions. Next, during the testing step, we executed the list of functions on the smart TV. Then, during post imaging, as with pre imaging, we reimaged the entire disk volume after operating the functions. Finally, during the binary diffing step, we compared the changes in the binary between the pre image and post image disk volume. We finally, determined the parts of the disk that are linked to the smart TV functions. For example, the disk partition mmcblk0p12 was imaged at 16:34 26th Dec. Then, we turned on the TV. Next we reimaged the disk at 18:28 26th Dec. Finally, we found that the 4 byte change in 00C8E007 offset in the mmcblk0p12 partition and recognized the likability between the part around 00C8E007 offset and the PowerOnTime.dat file. Figure 4 presents the binary diffing example.

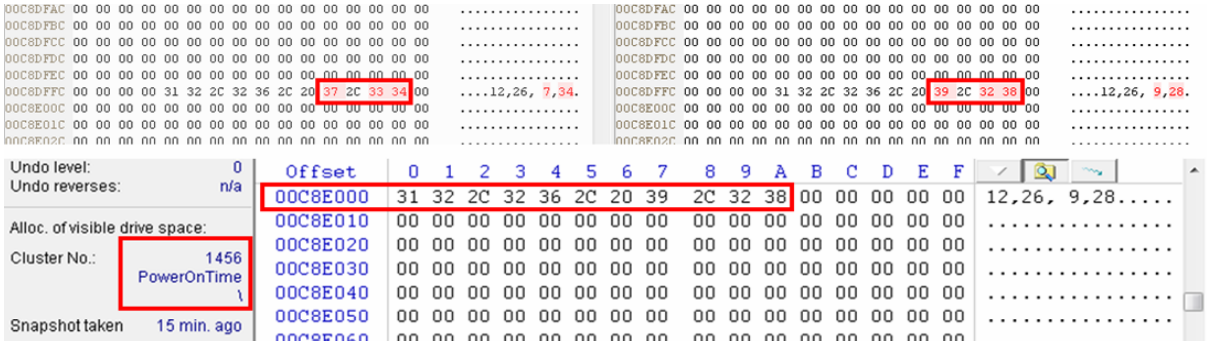


Figure 4. Binary diffing

Information analysis and report. For the information analysis and report, the investigator analyzes the data to provide meaning and to link it to the suspect's actions. The investigator then produces evidence from the result of the analysis and generates a report. In this paper, we will not deal with the reporting step because this is the responsibility of an investigator. Instead, we will focus on describing our results in detail in Chapter 3.3.

3.3 Information Analysis for a Smart TV

In this chapter, we explain the results of our experimental analysis on a smart TV. We could determine the user's actions as follows: (1) Last time the TV was turned on; (2) History of web access; (3) Recently operated service list; (4) Thumbnails of video files that were recently played; (5) Application information; (6) Camera Usage Information; (7) Selected TV channel list; (8) Selected TV channel list.

Last time the TV was turned on. We determined the last time the user turned on the TV from the /mtd_rwarea/PowerOnTime file. The PowerOn-Time file is 11 bytes in size and consists of four numbers and three identifiers. Given that the TV is turned on at 09:28 GMT on December 26, 2013, the PowerOn-Time would record the month, day, hour and minute information into ASCII characters and hex values according to the identifier. Therefore, we could see the hex values as 0x31(1), 0x32(2), 0x2C(identifier), 0x32(2), 0x36(6), 0x2C(identifier), 0x20(space), 0x39(9), 0x2C(id-entifier), 0x32(2) and 0x38(8). PowerOnTime can only write the information when the TV is turned on. Thus, we can only know the last date and time when the TV was turned on. This time information is automatically synchronized with a predetermined time through samsung smart TV server or manually set up by a user. Default time setting is automatically set through samsung server. Figure 5 shows the system menu. If a user modifies the time information for a malicious purpose, it will not be possible to trust the time information of the system. Such a time information manipulation is a typical anti-forensic technique and it decreases the reliability of the collected log data. This occurs to a majority of digital devices such as the PC and the smart phone in addition to the smart TV. Generally, in order to resolve this issue, the information of all log files are confirmed and the time consistency is assured [15-16]. If one wants to alter time with malicious intention without being caught, the person shall modify time with considering time information in all log files. This is the latter requires much effort because the person must consider the time consistency of a large number of log files that contain time information. However, the smart TV does have less log file types compared to the PC and the smart phone. Therefore, it does not have enough information to confirm the time consistency. Therefore, it requires much more time-related information to

analyze the time manipulation of the smart TV. Furthermore, additional studies are required regarding the time information manipulation. In addition to the date and time information, we could see yearly information using /mtd_rwcommon/LogPolicycon-fig.xml, LogPolicyconfig.xml stores the logging policy for applications. Its tag "period val" has the expiration information in terms of the date and time, including year, as shown in Figure 6. When the TV is turned on, the logging policy updates in 2 or 3 days. Thus, we could know the yearly information linking LogPolicy-config.xml with PowerOnTime.

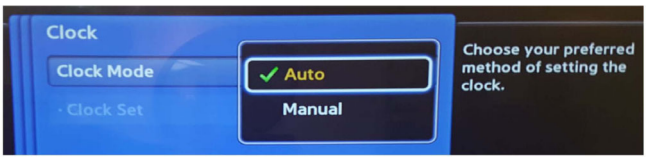


Figure 5. System menu (Clock)

```
<?xml version="1.0" encoding="UTF-8" ?>
<rsp stat="ok" xmlns="http://openapi.samsung.com/api/1.0">
  <period val="2014-04-19T07:24:05" />
  <server type="operating" />
- <list>
  - <service name="kids" url="https://lcprd1.samsungcloudsolution.net/openapi/log/kids"
      queue_max="30" expiration="60" loglevel="10">
      <event name="WATCHTUTORIALVIDEO" loglevel="5" />
      <event name="PLAY" loglevel="5" />
      <event name="SAMSUNGLOGIN" loglevel="5" />
      <event name="SAMSUNGLOGOUT" loglevel="5" />
      <event name="CHANGECHARACTER" loglevel="5" />
      <event name="TOOLS" loglevel="5" />
      <event name="RETURN" loglevel="5" />
```

Figure 6. LogPolicyConfig.xml

Recently operated service list. We found that the most important file storing information for TV viewing was in the /mtd_rwarea/ Re-centlyServiceManager.dat file. The file has three recent records regardless of services. The types of service stored include TV channels that have been watched, information on applications that are used, URL that has been visited, and the name of video files that are played. Recent-lyServiceManager.dat does not record the time infor-mation of the services, but the information is recorded in the time order. Therefore, we could arrange a user's actions related to the services in the time order. In particular, when the file has a URL that has been visited, we could easily infer the user's actions because the user's web page visit history includes time information. Table 3 shows the information that can be obtained through a combination of the RecentlyServiceManager.dat with other files.

	ID	URL	TITLE	LASTVISITDATE	FREQUENCY
1	1	http://bing.search.daum.net/	http://bing.searc	1381560274	3
2	2	http://search.daum.net/bing?q=bing	http://search.dau	1381560285	1

Figure 7. Web access history

Table 3. Combination and analysis with other files

File Name	Contents
RecentlyServiceManager.dat	The last three TV channels the user watched
RecentlyServiceManager.dat + RecentlyPlayed.dat	Thumbnail images of the last three videos the user watched
RecentlyServiceManager.dat + Info.xml	Names of the last three applications the user ran
RecentlyServiceManager.dat + 0000000000000002.db	List of the last three Websites the user visited

Thumbnails of recently played video files. When we watch a video file from external storage, the thumbnail images from the video are created and stored into mta files with the XML format. The directory location is /mtd_common/RecentlyPlayed, and the directory limits the number of files as 8 mta files, and each mta file has 5 thumbnails of recently played video files. Figure 8 shows an example of the thumbnail images in the mta file.

Figure 8. An example of thumbnail images in an mta file

Camera usage information. We could determine the trace of the camera usage in a smart TV in the /mtd_rwcommon/common/111199000-764/CameraAppFileInfo.xml file. The file records information whenever the camera is used and stores information for a picture that was taken including the date and time, name, stored file location, stored thumbnail image location, resolution, size and playing time. When the camera is powered, the usage time information is written in PowerOnTime and in 0000000002.db simultaneously.

Additional information. Our study results also showed the web access history, application information, saved TV channel list and external usage storage information described in Boztas [5]. The information was confirmed to be the same as the study results of Boztas [5]. Figure 9 shows this information.

Figure 9. Application information

4 Comparison

Table 4 presents a comparison of the previous works with the results of our experiment on smart TV forensics. We obtained additional information related to time or order that the previous works were not able to obtain. Therefore, we could conduct a chronological analysis of the user's actions on the smart TV. In addition, our experiment focus on major TV functions, such as the last time the TV was turned on and the list of channels that were recently watched. Thus, it would be helpful for an investigator to provide more accurate and diverse behavior of the suspect than previous studies.

Table 4. Comparison the previous works with our result of experiment

Info Type	User's action	[4]	[5]	Ours
Time	Last time TV turned on	X	X	O
	History of the web access	X	O	O
Order	Recent operated function list	X	X	O
	Recent watched channels	X	X	O
	Recent used applications	X	O	O
	Recent accessed URL	X	O	O
	Recent played video files	X	O	O
	Thumbnails of recent played video files	X	X	O
Non time or order relevant	Saved TV Channel List.	X	O	O
	Application information	X	O	O
	Camera Usage Information	X	X	O
	External Storage Usage Information	X	O	O
	System and Network Configuration	O	O	O

5 Conclusion

We have examined a novel method to conduct forensics on a smart TV. We deter-mined the time or order related information in a smart TV, including the last time the TV was turned on, the list of recently operated functions, the list of recently watched channels, recent video file playback and camera usage information. The previous works in [4] and [5] have a weaknesses in that they do not focus on major functions and analyze non-time relevant information. Therefore, such information is insufficient to allow the investigator to rearrange a suspect's actions due to the lack obtainable information and non-time relevant information. Therefore, the result of our experiment overcomes the weaknesses of previous works and enables an investigator to more easily produce evidence. For future research, we will expand this subject to various smart appliances, such as robot vacuums and refrigerators. Also, we will study live forensic methods for smart devices by using a memory dump. Additional analysis on various models will be needed because the results may differ depending on the types of smart TV.

Acknowledgements

This research was supported by the MSIP (Ministry of Science, ICT and Future Planning), Korea, under the ITRC (Information Technology Research Center) support program (IITP-2016-R0992-16-1006) supervised by the IITP (Institute for Information & communications Technology Promotion) and Institute for Information & communications Technology Promotion (IITP) grant funded by the Korea government (MSIP) (R0101-16-0195, Development of EAL 4 level military fusion security solution for protecting against unauthorized

accesses and ensuring a trusted execution environment in mobile devices).

References

[1] Parks Associates, www.parksassociates.com.

[2] Korea Communications Commission, *Broadcast Media Use/ Behavior Research*, December, 2013.

[3] I. Sutherland, H. Read, K. Xynos, Forensic Analysis of Smart TV: A Current Issue and Call to Arms, *Digital Investigation*, Vol. 11, No. 3, pp. 175-178, September, 2014.

[4] I. Sutherland, K. Xynos, H. Read, A. Jones, T. Drange, A Forensic Overview of the LG Smart TV, *12th Australian Digital Forensics Conference*, Perth, Western Australia, 2014, pp. 1-8.

[5] A. Boztas, A. R. J. Riethoven, M. Roeloffs, Smart TV Forensics: Digital Traces on Televisions, *Digital Investigation*, Vol. 12, pp. S72-S80, March, 2015.

[6] J.-H. Lim, C.-W. Song, K.-Y. Chung, K.-W. Rim, J.-H. Lee, Forensic Evidence Collection Procedures of Smartphone in Crime Scene, in: K. J. Kim, K. Y. Chung (Eds.), *IT Convergence and Security 2012, Lecture Notes in Electrical Engineering, Vol. 215*, Springer, Dordrecht, 2013, pp. 35-41.

[7] S. L. Garfinkel, Digital Forensics Research: The Next 10 Years, *Digital Investigation*, Vol. 7, pp. S64-S73, August, 2010.

[8] H.-S. Kang, M.-S. Park, S.-J. Kim, Study on Smart TV Forensics, *Journal of The Korea Institute of Information Security & Cryptology*, Vol. 24, No. 5, pp. 851-860, October, 2014.

[9] A. Grattafiori, J. Yavor, *The Outer Limits: Hacking the Samsung Smart TV*, http://www.blackhat.com/us-13/briefings.html#Grattafiori.

[10] S. Lee, S. Kim, Hacking, Surveilling, and Deceiving Victims on Smart TV, http://media.blackhat.com/us-13/Us-13-Lee-Hacking-Surveilling-and-Deceiving-Victims-on-Smart-TV-Slides.pdf.

[11] M. A. Falayleh, A Review of Smart TV Forensics: Present State & Future Challenges, *The International Conference on Digital Information Processing, E-Business and Cloud Computing (DIPECC2013)*, Dubai, UAE, 2013, pp. 50-55.

[12] BI Intelligence, https://intelligence.businessinsider.c-om.

[13] A. E. Brouwer, http://www.win.tue.nl/~aeb.

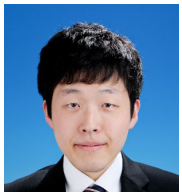
[14] K. Barmpatsalou, D. Damopoulos, G. Kambourakis, V. Katos, A Critical Review of 7 Years of Mobile Device Forensics, *Digital Investigation,* Vol. 10, No. 4, pp. 323-349, December, 2013.

[15] X. Ding, Z. Hengming, Time Based Data Forensic and Cross-reference Analysis, *Proceedings of the 2011 ACM Symposium on Applied Computing*, Taichung, Taiwan, 2011, pp. 185-190.

[16] S. Willassen, Hypothesis-based Investigation of Digital Timestamps, *IFIP International Conference on Digital Forensics*, Kyoto, Japan, 2008, pp 75-86.

Biographies

Minsu Park received his B.S degree in Computer Network from Silla University of Korea, in 2010 and also received his M.S degree in Information Security from Korea University of Korea, in 2013. He is currently working toward the Ph.D. degree in Information Security, Korea University, Korea. His research interests include Information Assurance, IoT Security, Digital Forensic and Usable Security.



Heesoo Kang received his B.S. in computer science from Chung Ang University in Korea, in 2013 and also received his M.S degree in Information Security from Korea University of Korea, in 2015. He is currently working toward the Ph.D. degree in Information Security, Korea University, Korea. His research interests include smart device security, security evaluation, and mobile security.

Seungsoo Baek received his BS degree in Computer Science in Korea Military Academy in 2002 and MS degree in Computer Science from Naval Postgraduate School, the US in 2007 respectively. He is currently a doctoral candidate majoring in information security in Korea University from 2012. Also, he is working for Korea Military Academy as an assistant professor in department of Computer Science. His main research interests include Cyberwar, Network security, C4I system and Digital Forensics of IoT devices.

Seungjoo Kim received his B.S., M.S. and Ph.D. from Sungkyunkwan University (SKKU) of Korea, in 1994, 1996 and 1999, respectively. Prior to joining the faculty at Korea University (KU) in 2011, He served as Assistant & Associate Professor at SKKU for 7 years. Before that, He served as Director of the Cryptographic Technology Team and the (CC-based) IT Security Evaluation Team of the Korea Internet & Security Agency (KISA) for 5 years. He is currently a Professor in the Graduate School of Information Security Technologies (CIST). Also, He is a Founder and Advisory director of a hacker group, HARU and an international security & hacking conference, SECUINSIDE. Prof. Seungjoo Kim's research interests are mainly on cryptography, Cyber Physical Security, IoT Security, and HCI Security. He is a corresponding author.