*Journal of The Korea Institute of Information Security & Cryptology* ISSN 1598-3986(Print)
VOL.24, NO.5, Oct. 2014 ISSN 2288-2715(Online)
http://dx.doi.org/10.13089/JKIISC.2014.24.5.851

# 스마트 TV 포렌식에 관한 연구*

강 희 수,† 박 민 수, 김 승 주‡
고려대학교 정보보호대학원

# Study on Smart TV Forensics*

Hee-soo Kang,† Min-su Park, Seung-joo Kim‡
Center for Information Security Technologies(CIST), Korea University

요 약

IT 기술의 발달과 사용자 편의를 증대시키는 전자제품에 대한 수요가 증가함에 따라 기존의 디지털 TV에 네트워크 기능을 추가하여 사용자에게 다양한 서비스를 제공하는 스마트 TV가 활발하게 개발되어 보급되고 있다. 이러한 TV 기능의 변화는 디지털 포렌식적으로 의미를 갖는다. 기존의 디지털 TV는 기기 안에 저장되는 데이터가 충분하지 않아 디지털 포렌식 조사의 대상으로 주목받지 못하였다. 하지만 스마트 TV는 사용자에게 다양한 기능과 편리한 사용을 제공하기 위해 사용자의 과거 행동을 파악할 수 있는 데이터를 기기 내부에 저장하기 때문에 디지털 포렌식 조사의 대상으로 가치가 있다. 본 논문은 디지털 포렌식의 한 분야로서 기존의 디지털 포렌식보다 폭넓은 연령대의 사용자 행동을 추적할 수 있는 스마트 TV 포렌식의 개념 및 방법을 제안한다.

ABSTRACT

With an increasing demand of powerful electronic goods, smart TV containing network module with digital TV gets more popular. These change are meaningful from a digital forensics perspective because smart TV store more user's data than digital TV. In this paper, we suggest smart TV forensics as a branch of digital forensics. With smart TV forensics, investigator can trace more wide age group's activities than existing digital forensics analysis.

**Keywords:** Smart TV Forensics, Smart TV, Digital Forensics

## I. 서 론

스마트 TV는 인터넷에 연결되어 기존의 TV기능뿐 아니라 게임, 인터넷 검색, VOD (Video on demand)와 같은 다양한 서비스로 사용자에게 편의를 제공하는 TV이다[1]. 스마트 TV는 다양한 응용서비스를 제공하기 위해 네트워크 모듈, 고사양의 CPU, Linux 위에서 동작하는 자체 운영체제와 소프트웨어 엔진을 가지고 있으며 이로 인해 사용자는 페이스북, Skype, 게임과 같이 컴퓨터 환경에서 동작하는 많은 앱들을 스마트 TV로 이용가능하다.

스마트 TV의 주요 생산업체로는 삼성, LG, 애플, 구글이 있으며 특히 삼성과 LG의 경우 스마트 TV를 주력상품으로 선정하여 새로운 모델의 스마트 TV를 지속적으로 출시하고 있다. 한국전자통신연구원(ETRI)은 국내 스마트 TV 이용가구 수가 2014년 약 360만 가구에서 2018년 890만 가구로 증가할 것이며 매출액은 약 1조 2000억원에서 1조 6000억원으로 증가할 것으로 예상하였다[2]. Fig. 1.은 이러

접수일(2014년 7월 17일), 수정일(1차: 2014년 8월 26일, 2차: 2014년 9월 16일), 게재확정일(2014년 10월 6일)
* 본 연구는 한국산업기술평가관리원의 IT R&D 프로그램 (10043959, 모바일단말의 비인가접근차단 및 운영환경 보장을 위한 EAL 4급 군사용 융합 보안 솔루션 개발) 사업의 연구결과로 수행하였습니다.
† 주저자, kukulux@korea.ac.kr
‡ 교신저자, skim71@korea.ac.kr(Corresponding author)

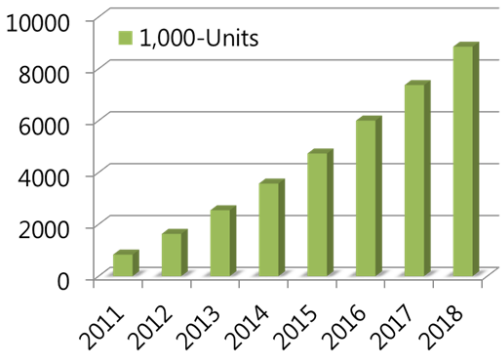


Fig. 1. Prospect of domestic smart TV usages

한 수치를 그래프 화 한 것이다. Fig. 1.에서 볼 수 있듯이 스마트 TV는 빠른 속도로 일반 가정에 보급되어 기존의 디지털 TV를 대체하고 있다.

스마트 TV는 사용자에게 편리한 서비스를 제공하기 위해 기기 내부에 다양한 데이터를 저장하며 이는 스마트 TV가 디지털 포렌식 조사의 대상이 될 수 있음을 의미한다. 하지만 디지털 포렌식의 주요 대상인 PC와 스마트폰과 다르게 스마트 TV는 여가 시간에, 사용자의 집 내부에서 사용되며 사용 연령층 또한 앞의 두 기기보다 폭넓기 때문에 수집된 데이터의 활용 방법이 기존의 디지털 포렌식과 다를 것으로 예상된다. 또한 앞서 언급한 것처럼 스마트 TV가 빠른 속도로 디지털 TV를 대체하고 있기 때문에 스마트 TV를 이용한 디지털 포렌식의 특징이 무엇이며 이를 이용하여 어떤 데이터를 분석 가능한지에 대한 연구가 필요하다. 본 논문은 스마트 TV에 남겨진 사용자 흔적데이터를 이용해 사용자의 과거 행동을 추적하는 스마트 TV 포렌식을 제안하며 시판된 제품을 선정하여 스마트 TV 포렌식 분석을 수행함으로써 실제로 어떤 데이터가 TV에 저장되는지 확인한다.

## II. 디지털 포렌식

디지털 포렌식은 법적 증거력이 있는 디지털 증거를 수집하여 분석하고 이를 보관하는 절차를 다루는 학문이다[3]. 디지털 증거는 컴퓨터와 같은 전자 기기에서 사용되는 데이터 중 법정에서 증거물로서 효력을 갖는 데이터를 뜻하며 조작 및 훼손이 용의하다는 특징이 있다. 따라서 최초 디지털 포렌식 조사 준비 과정에서부터 디지털 증거를 법원에 제출하기까지 모든 과정에 대해 디지털 증거의 무결성을 입증하는 것이 디지털 포렌식의 궁극적인 목표이다.

디지털 포렌식은 등장 초기 PC에서 삭제 된 데이터를 복구하는데 초점을 맞추었다[4]. 또한 개인 사용자가 PC를 소유하고 있는 경우가 많지 않았기 때문에 메인프레임과 같은 시분할 중앙집중형 컴퓨터 환경에서의 조사가 대부분이었다[5]. 하지만 일반인들의 PC사용량이 증가하고 인터넷, 워드, 이메일, 클라우드와 같은 다양한 서비스가 제공됨에 따라 디지털 포렌식 조사를 적용할 대상이 점차 확대되고 있다.

Table 1.은 디지털 포렌식의 주요 분야를 정리한 표이다. Table 1.에서 알 수 있듯이 현재 디지털 포렌식은 PC와 스마트폰을 주요 대상으로 하고 있으며 그 외 스마트 TV, 내비게이션, 의학용 전자기기와 같이 디지털 증거를 습득할 수 있는 기타 기기에 대한 디지털 포렌식 조사 절차와 해당 기기에서 발견 가능한 디지털 증거의 유형에 대한 연구가 부족하다.

Table 1. Branches of Digital Forensics

| Branches | Goal | Target Device |
|---|---|---|
| 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 /Smart phone |
| Document Forensics | Exploring the 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 /Smart phone |
| WEB Forensics | Tracing user's Internet usage history, such as Web history, favorites, and search words | PC /Smart phone |
| NETWORK Forensics | Acquiring network device's information, such as network configuration and packets | Network equipment |
| Cloud Forensics | Exploring cloud service usage history and files used | PC /Smart phone |
| Smart phone Forensics | Collecting and analyzing trace data existing on mobile devices | Smart phone |

## III. 스마트 TV 포렌식

### 3.1 스마트 TV 포렌식의 필요성

TV는 가정에서 가장 많이 사용되는 방송매체이다. 방통위에서 발표한 2013년 방송매체이용형태조사에 의하면 응답자 중 95.8%가 최근 3개월 동안 TV를 하루 이상 이용하였으며 스마트폰과 PC는 각각 69%, 58.1%의 응답자가 하루 이상 이용하였다[6]. 이처럼 TV가 일상생활에서 빈번하게 사용됨에도 불구하고 기존의 디지털 TV는 디지털 포렌식의 대상으로 큰 의미를 갖지 못하였다. 이는 디지털 TV가 단순히 방송국의 전파를 수신하는 기능만을 수행하고 기기 내부에 저장하는 데이터가 적었기 때문이다. 하지만 스마트 TV는 방송 수신 기능 외에 다양한 서비스와 편리한 사용을 제공하기 위해 기기 내부에 TV 사용 정보, 앱 설치 목록, 웹 히스토리 등 디지털 증거로서 가치 있는 데이터를 저장하기 때문에 디지털 포렌식 조사대상으로 가치가 있다. 본 논문에서는 스마트 TV에서 발견된 사용자 흔적데이터를 토대로 사용자의 과거 행동을 추적하는 디지털 포렌식의 분야를 스마트 TV 포렌식이라 정의한다.

디지털 포렌식 조사의 주요 대상인 PC와 스마트폰과 비교하였을 때 TV는 다소 한정적인 장소와 시간에 사용되며 사용 연령층이 다양하다는 특징이 있다. PC가 직장에서 업무시간에 주로 사용되며 스마트폰은 각종 장소에서 상시적으로 사용되는 것과 다르게 TV는 사용자의 집 안에서 여가시간에 주로 사용된다. 또한 TV는 PC와 스마트폰을 거의 사용하지 않는 60대 이상의 인구들도 다수 사용한다.

Table 2.는 연령대 별 TV, PC, 스마트폰 이용자 분포를 조사한 것이다[6]. Table 2에서 알 수 있듯이 PC와 스마트폰의 이용자는 10대에서 40대에 주로 분포하며 60대 이상 인구의 이용비율이 적다. 이에 반해 TV는 이용자의 연령 분포가 더 고르며 60대 이상의 이용자도 전체 응답자 중 18.7%로 높은 비중을 차지한다.

Table 2. Distribution of user's age groups

| Media / age | TV | PC | Smart phone |
|---|---|---|---|
| 10~19 | 11.2 | 15.8 | 14.0 |
| 20~29 | 15.2 | 22.9 | 21.9 |
| 30~39 | 18.9 | 25.9 | 25.9 |
| 40~49 | 19.8 | 22.0 | 23.4 |
| 50~59 | 16.2 | 10.3 | 11.8 |
| 60~ | 18.7 | 3.2 | 3.0 |

이처럼 TV와 PC, 스마트폰은 이용되는 장소와 시간대, 연령층이 각각 다르며 이는 과거 행동을 추적할 수 있는 범위와 사용자의 연령대에서 차이가 남을 의미한다. 특히 60대 이상의 인구는 PC와 스마트폰을 거의 이용하지 않으므로 기존의 디지털 포렌식 조사를 수행하기에 적합하지 않다. 스마트 TV 포렌식은 이와 같이 분석하려는 대상이 PC 및 스마트폰을 사용할 수 있어야 하는 기존의 디지털 포렌식의 한계를 보완할 수 있으며 사용자의 집 안에서 이루어지는 은밀한 행동을 복원할 수 있다는 장점이 있다. 또한 결혼률, 출산율 저하와 인구의 노령화로 인해 1인가구가 증가하고 있으며 페이스북, Skype와 같이 사용자 인증이 필요한 스마트 TV 서비스로 인해 스마트 TV 포렌식은 점차 개인의 행동을 추적하는 형태로 발전할 것이다. 따라서 스마트 TV 포렌식 분석 방법과 흔적데이터의 유형 및 흔적데이터의 활용 방안에 대한 연구가 필요하다.

### 3.2 스마트 TV 포렌식 조사 절차

Fig. 2.는 스마트 TV 포렌식의 절차를 나타낸 것이다. 스마트 TV 포렌식은 Root 권한 획득, 내부 구조 파악, 흔적데이터 수집, 흔적데이터 분석 4단계

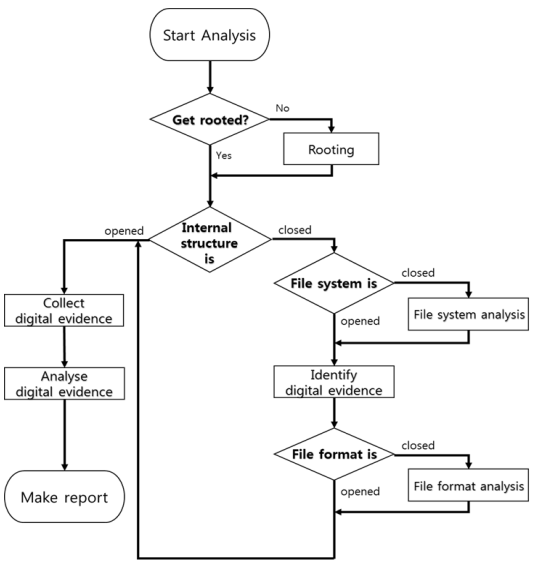


Fig. 2. Whole process of smart TV Forensics

로 이루어진다.

① Root 권한 획득

스마트폰 포렌식은 Root 권한 획득 후 수행 가능하다[7]. 이와 마찬가지로 스마트 TV 포렌식도 Root 권한을 획득하는 과정이 선행되어야 한다. Root 권한은 스마트 TV에 존재하는 파일을 탐색, 열람하고 dd와 같은 디스크 이미징 도구로 흔적데이터가 존재하는 파티션을 이미징 하여 데이터를 수집하기 위해 필요하다.

② 내부구조 파악

스마트 TV의 운영체제와 내부구조는 제조사별로 다르며 이에 대한 정보를 제공하지 않기 때문에 스마트 TV가 사용하는 파일시스템과 흔적데이터에 대한 데이터 저장방식을 파악하는 것이 중요하다. 만약 분석하고자 하는 스마트 TV가 독자적인 파일시스템을 사용할 경우 이에 대한 추가적인 분석이 필요하다.

③ 흔적데이터 수집

Root 권한 획득과 내부구조 파악 후 스마트 TV 내부에 존재하는 흔적데이터를 수집하는 단계이다. 본 단계에서는 내부구조 파악 후 스마트 TV의 데이터 영역을 이미징 하여 외부 저장장치에 저장하는 작업을 수행한다. 저장된 이미지 파일을 분석함으로써 데이터 영역 중 조사관이 관심 있어하는 흔적데이터를 찾아낼 수 있으며 분석 전 이미지 파일의 해시 값을 저장해 놓음으로써 분석 후 데이터의 무결성을 입증할 수 있다.

④ 흔적데이터 분석

수집된 흔적데이터를 분석하여 사용자의 행동을 추적한다. 조사관은 흔적데이터 수집단계에서 얻어진 데이터를 이용하여 사용자가 특정시간대 어떤 행동을 하였는지 추측하고 이를 토대로 보고서를 작성한다.

## IV. 실험

본 절에서는 시판된 스마트 TV모델을 선정하여 스마트 TV 포렌식 조사를 수행함으로써 TV에서 어떤 유형의 디지털 증거가 발견되는지 확인하고 수집된 데이터를 어떻게 사용할 수 있을지 활용방안에 대해 언급한다.

### 4.1 실험 환경

실험 대상으로 스마트 TV 시장에서 가장 큰 점유율을 차지하고 있는 국내 A사의 un46es8000모델을 선정하였으며 펌웨어 버전은 T-ECPAKUC-1041.1, BT-S/G이다. 또한 해당 스마트 TV는 2.6.x 버전 커널의 Linux 운영체제를 사용한다. 3.2절에서 언급한 것과 같이 TV 내부에 어떤 사용자 흔적이 남는지 알아보기 위해 TV의 내부구조를 파악하고 어떤 파일시스템을 사용하는지 분석하는 작업이 선행되어야 한다.

Table 3. un46es8000's major partitions

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

Table 3.은 un46es8000 모델의 19개 파티션 중 일부를 나타낸 것이다. 해당 스마트 TV는 총 19개의 파티션으로 구성되어 있으며 각 파티션 별로 용도가 다르다[8]. 이 중 사용자 데이터가 주로 존재하는 파티션은 이더넷 설정, 블루투스 설정과 같은 각종 설정파일을 저장하는 mmcblk0p12파티션과, 스마트 TV에서 지원하는 각종 서비스에 대한 유저 데이터를 저장하는 mmcblk0p19파티션이다. 두 파티션 모두 fat파일 시스템의 확장 형태인 vfat 파일 시스템을 사용하기 때문에 별도의 파일시스템 분석 없이 사용자 흔적데이터 탐색이 가능하다.

### 4.2 분석 방법

스마트 TV는 PC나 스마트폰과 달리 어떤 위치에 어떤 유형의 데이터가 남는지 알려진 정보가 없기 때문에 사용자 흔적데이터를 찾아내기 위해 별도의 분석 방법이 필요하다. 분석방법은 Root 권한 획득, 사전 이미징 작업, 테스트, 사후 이미징 작업, 바이너리 비교 단계로 구성된다.

본 절에서 제시하는 분석 방법을 사용함으로써 실험 대상 스마트 TV에 다양한 유형의 사용자 데이터가 존재함을 확인할 수 있다.

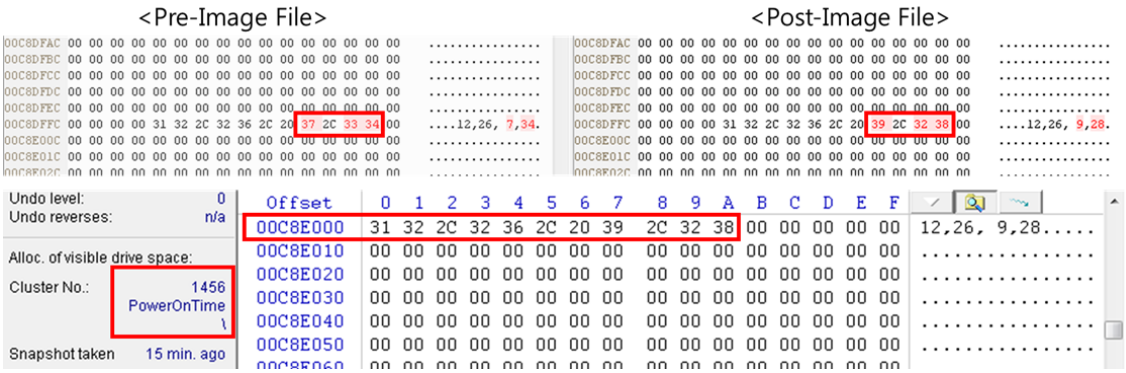


Fig. 3. Binary Diffing

① Root 권한 획득

스마트 TV의 데이터 분석을 위해 TV의 Root 권한을 획득하고 명령어 입력이 가능한 쉘을 실행시키는 작업이 선행되어야 한다. 이와 관련해 SeungJin Lee는 Blackhat 2013에서 스마트 TV의 모든 앱 및 API가 Root권한으로 실행되며 API에 존재하는 버그를 이용해 Buffer overflow 공격을 성공시킬 수 있음을 발표하였다 [9]. un46es8000모델 역시 이와 동일한 취약점을 가지고 있기 때문에 해당 취약점을 이용하여 Root 권한의 쉘을 실행시킬 수 있다.

본 실험에서의 Root 권한 획득은 Root권한 쉘을 실행하는 바이너리 파일을 제작하여 스마트 TV 부팅 시 자동으로 실행되는 바이너리 파일 폴더에 업로드 함으로써 이루어진다. 이 과정에서 바이너리 파일은 앞서 언급한 사용자 데이터 영역 파티션에 업로드 되지 않으며 사용자 데이터 영역을 침범하지 않으므로 Root권한 획득 전후 사용자 데이터의 무결성이 확보된다. 또한 이러한 방식의 Root 권한 획득은 특정 리눅스 커널의 버전에 의존하지 않고 스마트 TV의 모든 작업이 Root 권한으로 실행되며 Buffer overflow와 같은 공격을 방어하기 위한 메모리 영역 보호기법을 고려하지 않는 스마트 TV 설계상의 결함을 이용한 것이기 때문에 리눅스 커널 버전에 상관없이 동일한 방식으로 설계된 모든 스마트 TV에 적용 가능하다.

Root 권한 획득 단계는 최초 한 번만 수행된다.

② 사전 이미징 작업

사전 이미징 작업 단계에서는 테스트를 진행하기 전 TV에 존재하는 데이터를 백업하는 작업이 이루어진다. un46es8000은 제한된 개수의 명령어만을 제공하지만 다양한 시스템 유틸리티들을 통합해 놓은 Busybox를 내장하고 있기 때문에 dd와 같은 디스크 이미징 도구로 각 파티션을 이미징 할 수 있다.

③ 테스트

사전 이미징 작업 후 분석하기 원하는 작업을 수행하는 단계이다. 방송 시청, 앱 설치 및 실행, 인터넷 사용, 동영상 시청, 카메라 사용 등 TV가 제공하는 컨텐츠를 사용하는 것과 같은 작업이 테스트 단계에서 이루어진다.

④ 사후 이미징 작업

테스트 단계 후 변경된 TV의 데이터를 백업하는 단계이다. 사전 이미징 작업과 동일한 방법으로 수행한다.

⑤ 바이너리 비교(Binary Diffing)

사전 이미징 작업과 사후 이미지 작업에서 나온 이미지 파일을 비교하는 단계이다. 두 이미지 파일을 비교하고 변경된 부분을 찾음으로써 TV에서 특정 작업을 수행하였을 때 어떤 파일이 변경되었는지 찾아낼 수 있다. Fig. 3.은 mmcblk0p12 파티션을 2013년 12월 26일 16시 34분, 18시 28분 두 번에 걸쳐 이미징한 바이너리를 비교한 것이다. Fig. 4.에서 알 수 있듯이 바이너리 비교를 이용하여 mmcblk0p12 파티션의 00C8E007오프셋으로부터 4바이트의 데이터가 변경된 것을 확인 가능하며, 이 오프셋을 가지고 PowerOnTime이라는 파일이 변경되었음을 알 수 있다. 이러한 방식으로 인터넷 사용, TV 시청, 앱 사용 및 설치 등의 이벤트에 대해 ②~⑤ 단계를 반복함으로써 TV에 남는 흔적데이터의 종류와 위치를 파악할 수 있다.

### 4.3 사용자 흔적데이터

실험을 통해 un46es8000모델에서는 TV를 켠 시간, 앱 설치 및 이용 내역, 인터넷 히스토리와 같이 TV 이용에 대한 흔적데이터를 보관함을 알 수 있다. 이러한 흔적데이터들은 전체적으로 데이터 축적 기간에 제약이 없으나 마지막으로 TV를 켠 시간, 최근 재생 동영상 썸네일 이미지, 최근 서비스 실행 내역과 같은 일부 흔적데이터는 유지하는 데이터 개수를 제한하고 있어 새로운 데이터 생성 시 기존의 데이터가 삭제된다. 하지만 최신 정보만을 유지하는 일부 흔적데이터 외 나머지 흔적데이터는 기존의 데이터를 누적시키며 이러한 데이터를 변조하거나 삭제하기 위한 방법이 존재하지 않는다.

각 흔적데이터가 un46es8000모델에서 어떻게 저장되며 해당 데이터를 이용하여 얻을 수 있는 정보가 무엇인지에 대한 상세 설명은 다음과 같다.

#### 4.3.1 마지막으로 TV를 켠 시간

un46es8000모델에서는 사용자가 TV를 켤 때, 그 시간을 /mtd_rwarea/PowerOnTime이라는 파일에 기록한다. PowerOnTime은 11Byte의 hex값을 저장하고 있으며 그 값은 4개의 숫자와 3개의 구분자로 이루어진다. 예를 들어 2013년 12월 26일 18시 28분에 TV를 켠 경우 PowerOnTime 파일에는 31 32 2C 32 36 2C 20 39 2C 32 38 이라는 11Byte hex값이 기록되는데 이를 아스키 문자로 변환하면 12, 26, 9, 28과 같이 4개의 숫자로 해석된다. 이 숫자는 앞에서부터 각각 월, 일, 시간, 분을 나타내며 우리나라는 GMT+9시간대를 사용하기 때문에 실제 시간과 파일에 저장된 시간이 9시간 차이난다.

PowerOnTime의 값은 새롭게 TV를 켰을 때 기존의 데이터가 삭제되기 때문에 가장 마지막에 TV를 켠 시점만 알 수 있다. 또한 년도를 기록하지 않으므로 년도를 알아내기 위해서는 다른 흔적데이터를 이용하여야 한다.

#### 4.3.2 로깅정책 설정파일

TV의 방송기능, 앱, 서비스 등에 대한 로깅 정책은 /mtd_rwcommon/LogPolicyconfig.xml에 기록된다. Fig. 4.는 LogpolicyConfig.xml의 일부

```
<?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/
      queue_max="30" expiration="60" loglevel="10">
      <event name="WATCHTUTORIALVIDEO" loglevel="5" />
      <event name="PLAY" loglevel="5" />
      <event name="SAMSUNGLOGIN" loglevel="5" />
```

Fig. 4. LogPolicyConfig.xml

를 나타낸다. LogpolicyConfig.xml은 period val이라는 속성을 이용하여 로깅 정책의 만기일을 저장하는데 이 만기일이 마지막으로 TV를 켠 시점에서부터 2~3일 내외로 설정된다. 때문에 TV가 마지막으로 켜진 년도는 LogPolicyConfig.xml을 이용해 알 수 있다.

#### 4.3.3 앱 설치정보

TV에 앱이 설치될 때 해당 앱의 정보는 /mtd_rwcommon/common/widgetMgr/info.xml에 저장되며 info.xml의 내용은 설치된 앱의 이름, 앱 아이디, 설치 시간과 같은 정보를 포함한다. Fig. 5.는 info.xml의 내용을 나타낸 것이며 이를 이용해 info.xml이 어떤 형태로 데이터를 저장하고 있는지 알 수 있다.

info.xml의 앱 아이디는 설치된 앱에 자동으로 부여되는 식별자이며 앱의 리소스를 담고 있는 폴더명이 앱 아이디로 생성되기 때문에 특정 앱을 사용할 때 남는 사용자 데이터를 획득하려 할 시 info.xml에서 앱 아이디를 확인하여야 한다. info.xml에는 현재 TV에 설치된 모든 앱의 목록과 설치 시간이 저장되기 때문에 사용자가 어떤 앱을 사용하였는지 확인하려 할 때 사용할 수 있다.

```
<?xml version="1.0" encoding="UTF-8"?>
<list>
<widget id="111199000764" name="Camera" lock="false" removable="false"
installedDate="20120726110046164" runTitle="CameraApp" ispBound="false">
    <icon type="normal">icon/95.png</icon>
    <icon type="focus">icon/106.png</icon>
    <icon type="icon1080"></icon>
</widget>
<widget id="11111000010" name="YouTube" lock="false" removable="true"
installedDate="20130615155523788" ispBound="false">
    <icon type="normal">LIST_ON_20120106045029926.png</icon>
    <icon type="focus">THUM_LIST_OFF_20120106045029926.png</icon>
    <icon type="icon1080"></icon>
</widget>
<widget id="11091000000" name="Facebook" lock="false" removable="true"
```

Fig. 5. info.xml

#### 4.3.4 카메라 사용정보

사진 및 동영상 촬영 시 남는 카메라 사용 내역은 /mtd_rwcommon/common/111199000764/CameraAppFileInfo.xml에 저장된다. 경로 중 111199000764는 카메라 앱의 앱 아이디로 info.xml에서 확인 가능하다. Fig. 6.은 카메라 사용 시 관련 데이터가 CameraAppFileInfo.xml에 어떤 형태로 저장되는지 나타낸 것이다. Fig. 6.에서 알 수 있듯이 카메라 사용 시 사진/동영상 촬영 구분, 촬영일자, 해상도, 파일경로, 촬영 시간 등의 정보가 CameraAppFileInfo.xml에 포함된다.


Fig. 6. CameraAppFileInfo.xml

#### 4.3.5 인터넷 사용기록

스마트 TV는 웹브라우저를 내장하며 사용자가 인터넷을 이용할 경우 방문한 웹 페이지, 방문시간, 방문 횟수, 즐겨찾기 내역과 같은 정보가 저장된다. /mtd_rwcommon/webkit/database/file_0/0000000000000002.db는 Sqlite db 형태로 저장되기 때문에 뷰어를 사용하여 정보를 확인할 수 있다. Fig. 7.은 해당 파일을 Sqlite 뷰어로 내용을 확인한 것이다. Fig. 7.에서 알 수 있듯이 un46es8000은 접속한 URL과 마지막 방문 시간, 방문횟수를 저장한다. 특히 마지막 방문 시간은 Unix time 형태로 저장된다.

| ID | URL | LASTVISITDATE | FREQUENCY |
|---|---|---|---|
| 1 | http://bing.search.daum.net/ | 1381560274 | 4 |
| 2 | http://search.daum.net/bing?q=bing | 1381560285 | 2 |
| 3 | http://www.naver.com/ | 1395685502 | 1 |
| 4 | http://search.naver.com/search.naver?... | 1395685518 | 1 |
| 5 | http://comic.naver.com/webtoon/list.n... | 1395685530 | 1 |
| 6 | http://comic.naver.com/webtoon/detail... | 1395685547 | 1 |

Fig. 7. 0000000000002.db

#### 4.3.6 최근 재생 동영상 썸네일 이미지

TV에서 외부 저장소를 이용해 동영상을 시청할 때 해당 동영상의 썸네일 이미지는 xml형태의 mta 파일로 /mtd_common/RecentlyPlayed 폴더에 저장된다. RecentlyPlayed 폴더는 최대 8개의 mta 파일을 보관한다.

Fig. 8.은 하나의 mta파일의 내용과 해당 파일에서 얻을 수 있는 썸네일 이미지를 나타낸다. InlineMedia의 값은 썸네일 이미지를 Base64 인코딩 한 값으로서 해당 값에 대해 Base64 디코딩을 하여 원본 썸네일 이미지를 얻을 수 있다. 이러한 썸네일 이미지를 이용하여 사용자가 어떤 동영상을 시청하였는지 짐작 가능하다.


Fig. 8. mta file and restored thumbnail images

#### 4.3.7 최근 서비스 실행 내역

/mtd_rwarea/RecentlyServiceManager.dat은 TV 시청, 앱 사용, 인터넷 서핑, 동영상 재생과 같은 서비스에 대해 각각 최근 3건의 기록을 남긴다. 각 서비스별로 RecentlyServiceManager.dat이 남기는 정보는 다음과 같다.

① TV 시청: 시청 채널
② 앱 사용: 사용한 앱 아이디
③ 인터넷 서핑: 방문 URL
④ 동영상 재생: 동영상 파일이름, 썸네일 이미지

RecentlyServiceManager.dat에는 각 서비스 이용내역에 대한 시간정보가 남지 않지만 서비스 종류와 상관없이 사용한 시간 순서대로 이용내역이 저장된다. 따라서 RecentlyServiceManager.dat에 쌓인

이용내역의 순서를 고려하면 사용자의 특정 행위가 어떤 시점에서 이루어졌는지 유추할 수 있다.

#### 4.3.8 저장된 TV 채널 목록

TV는 시청하기 전 방송국의 신호를 수신하여 시청 가능한 채널을 등록하는 과정을 수행한다. 이때 채널 목록은 /mtd_rwarea/map-AirD에 저장된다. 저장되는 항목은 채널 번호와 방송국에 대한 식별자이다. 이 정보를 이용하여 TV가 어떤 지역에서 주로 사용되었는지 판단할 수 있다. Fig. 9.에서 알 수 있듯이 map-AirD는 112Byte단위로 채널을 구분하며 0번 offset에 채널 번호, 29번 offset부터 방송국 식별자가 저장된다.

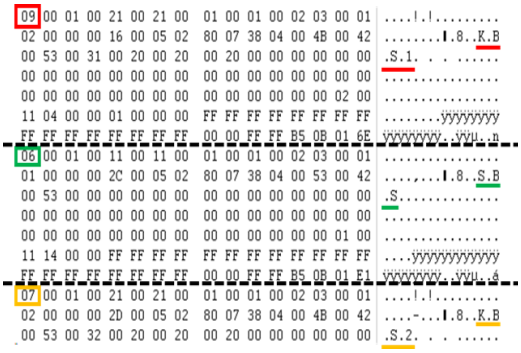


Fig. 9. map-AirD

#### 4.3.9 외부저장소 이용 정보

외부저장소는 USB, 외장 하드디스크와 같은 별도의 저장장치이다. 외부저장소는 TV를 이용해 외부저장소에 저장된 컨텐츠를 시청하려 할 때 주로 사용된다. 이 때 TV에서 사용된 외부저장소에 대한 내역은 /mtd_contents/device0012.db에 기록된다. device0012.db 역시 Sqlite db 형태로 저장되기 때문에 뷰어로 내용을 확인할 수 있다.

Fig. 10에서 알 수 있듯이 device0012.db의 MODELNAME필드에 외부저장소의 모델명이 저장되어 사용자가 어떤 형태의 외부저장소를 TV에 연결하였는지 파악할 수 있다. 하지만 일반적인 OS의 로그형태와 다르게 un46es8000모델에서는 외부저장소의 시리얼 넘버를 저장하지 않고 모델명만 기록하고 있으므로 정확히 어떤 장비가 TV에 연결되었는지 식별할 수 없다.

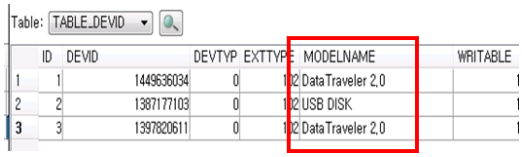
Table: TABLE_DEVID

| | ID | DEVID | DEVTYP | EXTTYPE | MODELNAME | WRITABLE |
|---|---|---|---|---|---|---|
| 1 | 1 | 1449636034 | 0 | 1 | 2 DataTraveler 2.0 | 1 |
| 2 | 2 | 1387177103 | 0 | 1 | 2 USB DISK | 1 |
| 3 | 3 | 1397820611 | 0 | 1 | 2 DataTraveler 2.0 | 1 |

Fig. 10. device0012.db

### 4.4 사용자 흔적데이터 활용 방안

#### 4.4.1 TV를 마지막으로 사용한 시간 획득

PowerOnTime과 LogPolicyConfig.xml을 함께 봄으로써 마지막으로 TV의 전원을 킨 시간(년/월/일/시/분)을 알 수 있다. 이 데이터는 용의자의 알리바이를 검증하기 위한 수단으로 이용할 수 있다. 예를 들어 용의자가 범죄가 일어난 시간에 TV를 시청하였다고 주장할 경우 TV를 마지막으로 켠 시간이 해당 시간과 동떨어져 있을 경우 용의자의 알리바이가 거짓이라 추정할 수 있다.

#### 4.4.2 사용자의 TV 사용 내역 추적

TV에 남는 대부분의 사용자 흔적에는 시간정보가 기록되지 않아 타임라인을 구성하는데 적절하지 않다. 하지만 RecentlyServiceManager.dat과 다른 서비스 사용기록을 함께 봄으로써 사용자 행동에 대한 제한적인 타임라인을 구성할 수 있다. 이는 사용자가 TV의 서비스를 이용할 때 관련 데이터가 RecentlyServiceManager.dat에 순차적으로 저장됨을 이용한 것이다. 특히 웹페이지 방문내역은 시간정보를 포함하므로 웹페이지 방문기록 사이에 있는 서비스 기록들에 대해서는 해당 서비스가 어느 시간대 사용되었는지 추정 가능하다. 또한 카메라 사용정보와 같이 사용 시간을 남기는 다른 흔적데이터의 이용함으로써 과거 사용자의 행동을 부분적으로 파악할 수 있다.

#### 4.4.3 악성 앱 감염여부 확인

info.xml은 TV에 설치된 앱의 목록을 저장하고 있기 때문에 현재 TV에 악성 앱이 존재하는지 확인할 수 있다. 또한 동작 방식이 알려진 악성 앱의 경우 다른 사용자 흔적데이터를 활용하여 이를 탐지할 수 있다. 예를 들어 TV에 내장된 카메라를 이용해 사용자를 도촬하는 악성 앱[9][10]에 감염되었는지

확인하려면 CameraAppInfo.xml에서 카메라 사용 내역을 뽑아 악성 앱이 이용한 것으로 의심되는 내역이 존재하는지 검사해 볼 수 있다.

## V. 결론 및 향후 연구

본 논문은 현재 빠른 속도로 가정에 보급되고 있는 스마트 TV에 대한 디지털 포렌식 조사 방법인 스마트 TV 포렌식을 제안하며 스마트 TV 포렌식이 특정 연령대의 사용자와, 특정 공간 및 시간에 일어난 행동을 추적하기 적절하지 않던 기존의 디지털 포렌식을 보완할 수 있음을 보였다. 또한 본 논문에서는 스마트 TV 포렌식 조사 절차를 수립하고 상용화된 스마트 TV를 대상으로 분석함으로써 실제 스마트 TV 포렌식을 이용하여 어떤 정보를 얻을 수 있을지 보였다. 그 결과 기존의 디지털 포렌식에서 얻을 수 있었던 전원 시간, 인터넷 사용기록, 외부저장소 이용 정보와 같은 흔적 데이터 뿐 아니라 카메라 사용정보, 앱 설치 내역 및 사용 정보, 재생 동영상 썸네일 이미지와 같이 스마트 TV에서 제공하는 컨텐츠와 관련된 흔적데이터도 함께 얻을 수 있었다. 마지막으로 본 논문에서는 이러한 흔적데이터에 대한 활용방안을 제시함으로써 스마트 TV 포렌식이 어떤 목적으로 사용될 수 있을지 보였다.

향후에는 스마트 TV 뿐 아니라 에어컨, 냉장고와 같이 앞으로 보급될 다양한 스마트 가전으로 대상을 넓혀 스마트 가전에서의 포렌식 조사 절차 및 흔적데이터 분석 방법을 일반화 시키는 연구를 진행할 예정이다.

## References


[1] KISA, "Smart TV Market Trend Analysis," Jan. 2013.

[2] ETRI, "Market outlook and the results of Smart TV receptor Servey," Jan. 2013.

[3] B.D. Carrier and E.H. Spafford, "An event-based digital forensic investigation framework," Proceedings of the 2004 digital forensic research workshop (DFRWS), pp. 11-13, Jul. 2004.

[4] C.C. Wood, W.W. Banks, S.B. Guarro, A.A. Garcia, V.E. Hampel and H.P. Satorio, "Computer security: a comprehensive controls checklist," Wiley-Interscience, 1987.

[5] S.L. Garfinkel, "Digital forensics research: The next 10 years," Digital Investigation 7, vol. 7, pp. S64-S73, Aug. 2010.

[6] KCC, "The use of survey form broadcast medium in 2013 years," Dec. 2013.

[7] Jeong-hyun Lim, Chang-woo Song, Kyung-young Chung, Ki-wook Rim and Jung-hyun Lee, "Forensic evidence collection procedures of smartphone in crime scene," IT Convergence and Security 2012, vol. 215, pp. 35-41, Dec. 2012.

[8] A. Grattafiori and J. Yavor, "The outer limits: Hacking the samsung Smart TV," Black Hat Briefings (2013), Jul. 2013.

[9] Seung-jin (beist) Lee and Seung-joo Kim, "Hacking, Surveilling, and Deceiving the Audience with Smart TV," Black Hat Briefings (2013), Jul. 2013.

[10] B. Michéle and A. Karpow, "Watch and be Watched: Compromising All Smart TV Generations," Proceedings of the 11th Consumer Communications Networking Conference (to appear), CCNC. IEEE, Jan. 2014.

## 〈저 자 소 개〉

강 희 수 (Hee-soo Kang) 학생회원
2013년 2월: 중앙대학교 컴퓨터공학부 졸업
2013년 3월~현재: 고려대학교 정보보호대학원 금융보안학과 석사과정
〈관심분야〉 정보보증, 정보보호관리체계, 모바일 보안

박 민 수 (Min-su Park) 학생회원
2010년 2월: 신라대학교 컴퓨터네트워크학과 졸업
2013년 2월: 고려대학교 정보보호대학원 정보보호학과 석사
2013년 3월~현재: 고려대학교 정보보호대학원 정보보호학과 박사과정
〈관심분야〉 정보보증, 정보보호제품 보안성 평가, 디지털 포렌식, Usable Security

김 승 주 (Seung-joo Kim) 종신회원
1994년~1999년: 성균관대학교 정보공학과 (학사, 석사, 박사)
1998년 12월~2004년 2월: KISA(舊한국정보보호진흥원) 팀장
2002년~현재: 한국정보통신기술협회(TTA) IT 국제표준화전문가
2004년 3월~2011년 2월: 성균관대학교 정보통신공학부 조교수, 부교수
2011년 3월~현재: 고려대학교 사이버국방학과/정보보호대학원 정교수
2004년~현재: 한국정보보호학회 이사
2005년~2006년: 교육인적자원부 유해정보 차단 자문위원
2007년: 국가정보원장 국가사이버안전업무 유공자 표창
2007년~2009년: 전자 정부 서비스 보안 위원회 사이버 침해사고대응 실무위원회 위원
2010년: 방송통신위원회 정보통신망 침해사고 민관합동조사단 위원
2012년 3월~2012년 6월: 선관위 디도스 특별검사팀 자문위원
2013년 4월~2013년 12월: IT보안인증사무국 자문위원
2013년 9월~현재: 중앙선거관리위원회 자문위원
2014년 3월~현재: 헌법재판소 자문위원
〈관심분야〉 보안공학, 암호이론, 정보보증, 정보보호제품 보안성 평가, Usable Security