

스마트홈 가전 및 IoT 기기 포렌식을 통한 범죄 수사에 사용될 수 있는 아티팩트 획득

이 진 오*, 손 태 식**
아주대학교 AI융합네트워크학과 (대학원생)*
아주대학교 사이버보안학과(교수)**

Acquisition of artifacts used for criminal investigations through smart home appliances and IoT devices forensics

Jino Lee*, Taeshik Shon**
Dept. of AI Convergence Network, Ajou University (Graduate Student)*
Dept. of Cyber Security, Ajou University (Professor)**

요 약

기술의 발전으로 IoT 기기들의 가정 및 개인 보급률이 증가하고 있으며, 스마트홈 IoT라는 단어가 생성될 정도로 일상생활에 많은 IoT 기기가 사용되고 있다. 이에 따라 IoT 기기를 통한 보안 및 다양한 범죄가 발생하고 있으며, 사건 발생 시 IoT 기기에 저장된 데이터를 획득하여 수사를 진행할 수 있다. 그러나 IoT 기기의 분석 및 보안과 관련된 연구가 매우 적어 대부분의 IoT 기기 데이터 획득에 대한 연구가 필요하다. 따라서 본 논문에서는 스마트홈 가전 및 IoT 기기를 선정하고 기기를 분석해 적용 가능한 데이터 획득 기법을 확인하였다. 기기 자체에서 데이터를 획득할 수 없는 IoT 기기는 연동된 스마트폰을 통해 데이터를 획득하고, 대상 기기별로 획득한 아티팩트를 정리하였다. 기기 내부의 데이터를 추출할 수 있는 스마트 tv는 적용 가능한 포렌식 기법을 설명하고, 탑재된 파일시스템인 VDFS의 메타데이터를 분석 및 획득한 아티팩트를 정리하였다. 추가로 스마트 TV의 파일시스템 VDFS를 분석 및 데이터를 보다 쉽게 획득할 수 있는 도구를 개발하였으며, 이를 통해 획득할 수 있는 크리덴셜 및 아티팩트를 설명한다.

주제어 : 디지털 포렌식, 스마트 tv, VDFS, iot

ABSTRACT

With the development of technology, the home and personal penetration rate of IoT devices is increasing, and many IoT devices are being used in daily life to the extent that the word smart home IoT is created. Accordingly, security and various crimes through IoT devices are occurring, and when an incident occurs, data stored in the IoT device can be obtained and investigated. However, research on the analysis and security of IoT devices is very small, so research on most IoT device data acquisition is needed. Therefore, in this paper, smart home appliances and IoT devices were selected and the devices were analyzed to confirm applicable data acquisition techniques. IoT devices that cannot obtain data from the device itself acquire data through the linked smartphone, and organize the acquired artifacts for each target device. Smart TV, which can extract data inside the device, describes applicable forensic techniques, analyzes and organizes metadata of VDFS, which is a mounted file system, and develops a tool to analyze and obtain data more easily, and explains credentials and artifacts that can be acquired.

Keyword : Digital Forensics, Smart tv, VDFS, iot

1. 서 론

현재 IoT 기기가 발전함에 따라 개인 및 가정에 보급되고 있는 스마트홈 가전 및 IoT 기기 수가 그림 1과 같이 증가하고 있으며, 일상생활의 많은 부분을 차지하게 되었다.

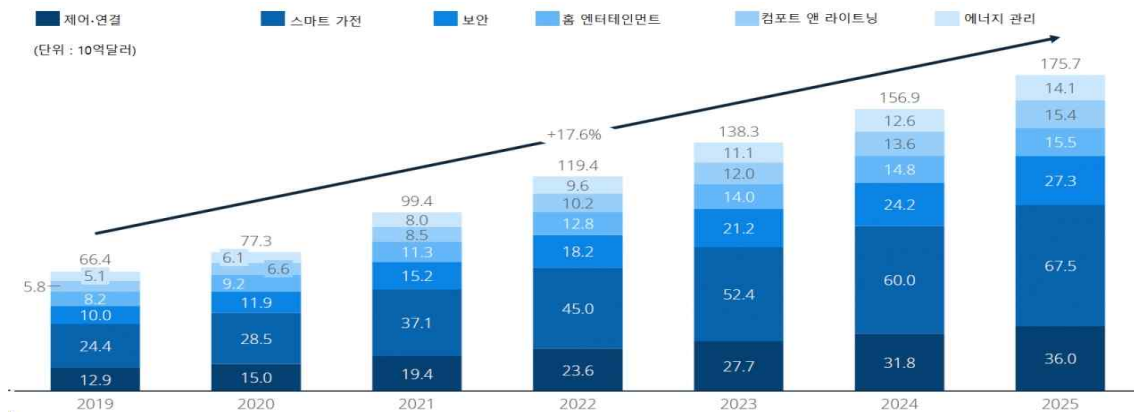
※ 본 연구는 한국전력공사의 2021년 착수 사회공모 기초연구 사업에 의해 지원되었음 (과제번호:R21X001-45)

• Received 28 January 2022, Revised 03 February 2022, Accepted 27 June 2022

• 제1저자(First Author) : Jino Lee (Email : dlwlsdh95@ajou.ac.kr)

• 교신저자(Corresponding Author) : Taeshik Shon (Email : tsshon@ajou.ac.kr)

그러나 IoT 기기들의 발전 및 보급률이 급속도로 증가하고 있는 반면에, IoT 기기들의 보안 기술은 그 속도를 따라가지 못하고 있다. 현재 가정에 보급된 IoT 기기들의 보안 기능이 대부분 없거나 매우 낮은 수준으로 보안이 취약한 상황이다[1]. 이로 인해 최근 IoT 기기들을 통한 개인 카메라 해킹, 개인정보 유출 등의 보안 공격 및 침해 사고가 발생하고 있으며, 이와 같은 범죄 수사를 위한 디지털 포렌식 기술의 수요는 지속적으로 증가하고 있다. 그러나 보안사고의 사례는 계속해서 증가하고 있으나, 사고에 대응 혹은 대처할 수 있는 기술 및 연구가 부족한 상황이다[2]. IoT 기기 내부 또는 연동된 클라우드 서버에는 사건 발생 시, 사용 기록, 사용자 정보, 시간 기록 등 알리바이 또는 증거가 될 수 있는 다양한 데이터가 저장되어 있다[3]. 그러나 현재 저장된 데이터를 획득할 수 있는 방안에 대한 연구가 활발히 진행되어있지 않아, 사건에 대한 증거 및 알리바이의 획득에 난항을 겪고 있다.



<Figure 1> IoT device growth rate(4)

따라서 본 논문에서는 가정에 보급될 수 있는 IoT 기기들의 분석을 진행 및 적용 가능한 포렌식 기법을 판별하여 적용하였다. 가정에 보급되는 IoT 기기들 중 내부에 내부 저장공간이 존재하지 않아 데이터가 저장되지 않는 소형 IoT 기기들의 데이터의 경우 해당 클라우드 서버와 연동된 스마트폰에서 획득 하였으며, Nand Flash Memory가 존재하는 스마트 TV의 경우 데이터 이미지를 획득하여 데이터 분석을 진행하였다. 추가로, VDFS(Vertically Deliberate FileSystem) 아티팩트를 획득할 수 있는 도구를 개발한다. 포렌식 기법의 적용을 통해 기존에 분석이 어려웠던 가전 및 스마트홈 IoT 기기의 데이터를 획득하였으며, 삼성 스마트 TV의 아티팩트를 추출해주는 도구를 통해 기존에 잘 알려지지 않았던 VDFS에서의 아티팩트 획득이 보다 쉽게 가능하도록 하였다. 이를 통해 시각, 장소, 사용자 정보 등을 획득하여 수사에 증거로 사용될 수 있도록 기여하였다.

본 논문은 2장에서 파일시스템의 배경지식 및 관련 연구에 대해서 설명하고, 3장에서는 데이터 획득을 위한 대상 기기 선정 및 기기들을 연결한 테스트 베드를 설명한다. 4장에서는 데이터 획득방안을 설명하고 각각의 기기에 적용, 5장에서는 획득 기법을 적용하여 획득한 데이터에 대해 설명한다. 6장에서는 개발한 도구를 설명하고 7장에서 결론을 짓는다.

II. 배경 지식 및 관련 연구

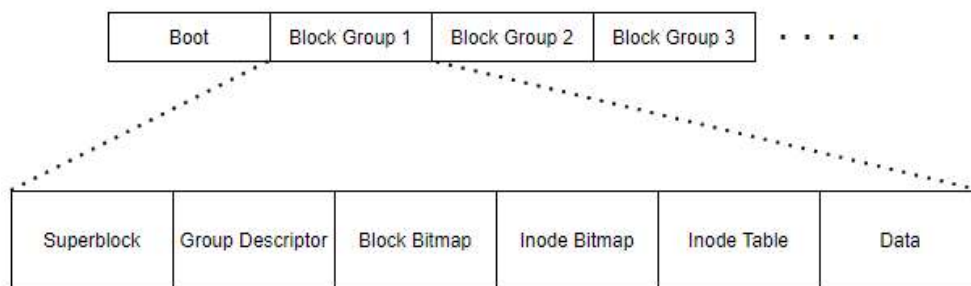
2.1 배경 지식

2.1.1 파일 시스템

파일시스템이란 컴퓨터에서 파일 및 폴더와 같은 자료를 보다 쉽게 접근이 가능하도록 해주는 시스템으로, 윈도우에 사용되는 NTFS(New Technology FileSystem), 리눅스 기반의 파일시스템인 Ext(Extended) FileSystem 등 다양한 파일시스템이 존재한다[5]. NTFS, Ext 이외에도, 윈도우에서 사용되는 FAT 등 매우 다양한 종류의 파일시스템이 존재하며, 포렌식에 있어서 기기가 어떠한 파일 시스템을 사용하는지는 매우 중요하다. 현재 많은 파일시스템에 대한 연구가 진행되어, 포렌식을 통한 파

일 추출, 파일 복구 등이 가능한 파일시스템이 존재하는 반면, 연구가 필요한 파일시스템 또한 존재하기 때문에, 기기가 어떠한 파일시스템을 사용하는지, 사용하는 파일시스템이 얼마나 분석이 되어있는지 파악하는 것이 매우 중요하다[6].

그림 2는 안드로이드 기기에 주로 탑재되는 Ext4 구조를 나타낸다. 그림 2의 Ext 파일시스템의 파티션은 파일시스템의 여러 정보를 나타내는 슈퍼블록, 메타데이터에 대한 정보가 있는 블록, 데이터 블록 등으로 구성되어 있다. 이는 단순 하나만의 파일시스템에 대한 예시이며, 다른 파일시스템의 경우 다른 구조를 가질 수 있다. 그러나 대부분의 파일시스템은 파일시스템 정보, 메타 데이터, 데이터가 저장되는 블록은 기본적으로 갖고 있기 때문에 파일시스템 분석 시, 위의 정보들을 중점적으로 분석한다.



〈Figure 2〉 Ext4 filesystem structure

현재 스마트홈 및 가전 IoT 기기들이 발전하면서, 가정에 보급되는 소형 IoT 기기들에도 파일시스템이 탑재되기 시작하였다. 또한 다양한 제조사에서 IoT 기기를 제조함에 따라 기기별 탑재되는 파일시스템의 종류가 상이하기 때문에, IoT 기기에 포렌식 기법을 적용 시, 다양한 파일시스템에 대한 기법을 적용할 수 있도록 많은 연구가 필요한 상황이다. 따라서 본 연구에서는 기기들에 대해 다양한 포렌식 기법을 적용해 데이터 획득을 시도하고, 해당 기기의 획득한 데이터를 통해 파일시스템 식별 및 분석을 진행한다.

2.2. 관련 연구

IoT 기기를 분석하는 연구는 최근에서야 그 수가 증가하고 있으나, IoT 기기 특성 상, 탑재된 파일시스템, 적용할 수 있는 기법 등이 상이하기 때문에 많은 연구를 필요로 한다. 본 장에서는 여러 IoT 기기 관련 연구를 소개한다.



〈Figure 3〉 Various IoT device filesystems

Jo.W 등은 AI 스피커를 분석 및 내부 데이터 획득과 관련된 연구를 진행했다[7]. 인증서 삽입을 통한 패킷 캡처, 칩오프(Chip-off) 등 다양한 방법을 사용하여 AI 스피커의 데이터 획득을 시도하였으며, 이를 통해 사용자 정보 및 저장된 파일 등의 여러 아티팩트를 획득하였다. 해당 연구는 AI 스피커의 데이터 획득을 진행하였으나, 현재 AI 스피커 이외에도 다양한 IoT 기기들이 출시되고 있기 때문에, 본 연구에서는 AI 스피커 이외의 추가적인 기기들에 대한 연구를 진행한다.

Boztas는 스마트 TV의 데이터 획득 관련 연구를 진행했다[8]. 해당 연구는 해킹 툴이 설치된 USB를 TV에 연결하여 툴을 실행해 데이터를 획득하였다. 그러나 현재 사용되는 파일시스템의 변화로 인해 제시된 기법을 적용할 수 없기 때문에 본 연구에서는 최신 스마트 TV의 데이터 획득을 시도한다.

Nemayire 등은 단순 TV에서 툴을 진행하는 Boztas의 연구에서 한발 나아가 최신 삼성 스마트 TV의 내부 데이터 이미지를 획득하여 연구를 진행했다[9]. 해당 연구는 VDFS 파일시스템을 MD-RED 도구를 통해 분석하였다. 그러나 해당 연구는 도구를 사용해 단순 데이터 획득만 진행하였다. 본 연구에서는 한 발 더 나아가 추가적인 데이터를 획득 및 분석하고, VDFS 파일시스템의 일부 메타데이터를 분석하여 추후 필요로 할 수 있는 VDFS 파일시스템 분석에 초석을 깔아둔다.

III. 대상 기기 선정 및 획득 방안

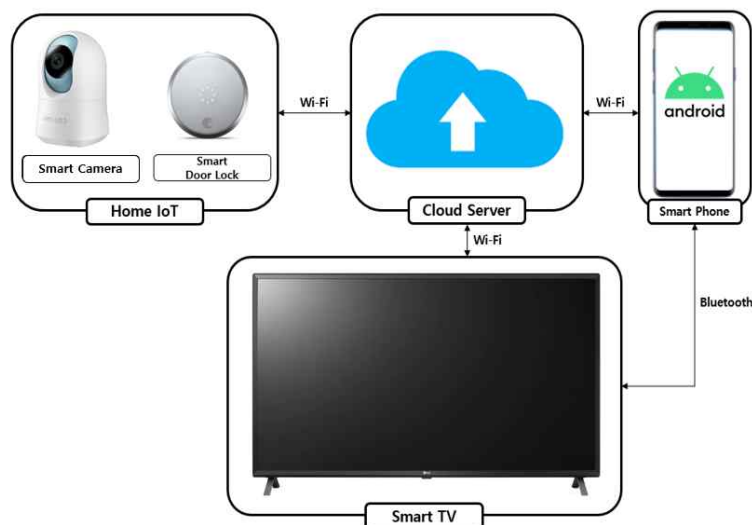
3.1 대상 기기 선정

스마트홈 가전 및 IoT 기기의 분석에 사용될 기기들은 일상에서 자주 사용하는 스마트 TV, 스마트 카메라, 스마트 도어락 기기 IoT 제품을 대상으로 선정하였다. 삼성, August, IMI Lab, 총 3개의 제조사를 선정하였으며, 선정된 기기들의 특성 및 하드웨어 분석을 진행 및 분류하여 표 1로 나타내었다.

〈Table 1〉 Target device for smart home forensics

Device	Model Name	Manufacturer	Communication	Nand Flash	Remark
Smart TV	KU43T5300AFXKR	Samsung	Wi-Fi/Bluetooth	KLM4G1FETE-B041	-
Smart Doorlock	August Smart Lock(4th Generation)	August	Wi-Fi	X	-
Smart Camera	IMI LAB SmartThings Cam 360	IMI Lab	Wi-Fi	X	-
Smart Phone	Galaxy S9	Samsung	On-cable/Wi-Fi	-	for export data from IoT Device

스마트홈 가전 및 IoT 기기들은 기능을 수행함에 따라, 기기 내부 또는 연동된 스마트폰에 사용 시간, 사용자 정보 등의 데이터가 저장될 수 있다. 따라서 본 연구에서는 IoT 기기 또는 연동된 스마트폰 기기 내부에 저장된 데이터의 획득을 시도한다. 스마트홈 가전 및 IoT 기기 분석을 위해 테스트 베드를 그림 4와 같이 스마트 기기들을 서버와 통신 및 스마트폰과 통신하도록 구축하였다. 스마트홈 가전 및 IoT 기기들의 wi-fi 통신을 통해 기능을 수행하면서 기기 내부에 저장되는 데이터를 다양한 획득 기법을 통해 획득 시도하였으며, 동시에 스마트홈 가전 및 IoT 기기에 연동된 스마트폰에 저장된 데이터 획득을 시도하였다.



〈Figure 4〉 Testbed for analyzing smart home appliances and IoT devices

3.2 획득 방안

본 장에서는 스마트홈 가전 및 IoT 기기에 적용할 수 있는 데이터를 획득 기법을 설명하고, 적용 가능성 및 획득할 수 있는 데이터에 대해 설명한다.

3.2.1 유/무선 연결

유선 연결을 통한 데이터 획득 기법은 대상 기기에 존재하는 USB 포트와 같은 통신 포트를 통해 PC와 연결하여 기기 내부에 존재하는 데이터를 획득하는 기법이다. 본 기법의 적용을 위해서는 대상 기기에 PC와 연결 가능한 포트가 존재해야 하고, 존재하는 포트가 단순 충전 및 전원 연결이 아닌 데이터 통신을 지원해야 한다. 추가적으로 기기의 데이터 접근을 위해서, 대상 기기에 탑재된 파일시스템이 PC에서 식별 가능한 파일시스템이어야 한다.

무선 통신을 통한 데이터 획득 기법은 Wi-Fi와 같은 무선 통신을 통해 대상 기기의 데이터를 획득하는 기법으로, PC와 대상 기기가 동일한 Wi-Fi에 연결되어 있어야 PC에서 데이터에 접근할 수 있다. 또한 유선 연결 데이터 획득 기법과 동일하게 PC에서 식별이 가능한 파일시스템이어야 한다.

유/무선 연결을 통한 데이터 획득 기법은 기기 내부 PCB에 Nand Flash Memory가 존재해야 적용할 수 있는 기법이다. Nand Flash Memory가 존재하여 기기 내부의 데이터에 접근이 가능하더라도 root 권한이 없기 때문에, 단순 연결을 통해서도 일부 중요 디렉토리에 접근이 어려울 수 있다. 따라서 본 기법이 적용이 가능하더라도 획득할 수 있는 데이터는 기본 디렉토리 경로, 사용자가 저장한 사진 등의 미디어파일 등으로 한정될 것이다.

3.2.2 UART/JTAG

UART 및 JTAG는 PCB에 존재하는 각각의 포트와 통신하여 데이터를 획득할 수 있는 기법이다. UART를 통한 데이터 획득 기법은 PCB에 존재하는 UART 핀들 중 RX, TX 핀이 시리얼 입출력을 지원하므로, PC와 연결하여 putty와 같은 터미널 응용 프로그램을 통한 시리얼 통신이 가능하다. 시리얼 통신을 통해 대상 기기의 U-Boot Shell에 접근 시 내부 데이터를 획득할 수 있다. 그러나 최근 제작되는 제품들은 UART 핀이 숨겨져 있거나, 제작 단계에서 제거하기도 하며, UART 핀의 종류가 다양하기 때문에 육안으로 식별이 어렵다. 따라서 UART 핀의 식별을 위해 오실로스코프와 같은 도구를 사용하거나 통전 테스트를 통해 UART 핀을 식별해야 한다. UART 핀을 통한 시리얼 통신은 데이터 통신량이 크지 않으므로 데이터 획득에 많은 시간이 소비될 수 있으나, 시리얼 통신을 통해 내부 Shell에 접근한 경우, 대상 기기의 데이터를 대부분 획득할 수 있다.

JTAG를 통한 데이터 획득 기법은 시스템 개발 시 사용되는 디버깅 포트인 JTAG 포트를 통해 데이터를 획득할 수 있는 기법이다. JTAG 핀은 총 9개의 핀이 존재하지만 5개의 핀(TDI, TMS, TCK, NTRST, TDO)을 통해 제어가 가능하다. JTAG 핀이 존재할 시, 기기를 디버깅 모드로 부팅하여 플래시 메모리를 이미징하는 방법을 통해 대상 기기의 데이터를 획득할 수 있다. 그러나 JTAG 핀 또한 UART 포트와 동일하게 제조사에서 개발 단계 이후 제거하거나 pin map을 알아볼 수 없도록 숨기기 때문에 시각적으로 식별이 불가능한 경우가 많다. 따라서 JTAG 및 UART를 통한 데이터 획득 기법이 적용 가능할 경우 대부분의 데이터를 획득할 수 있지만, 적용할 수 있는 IoT 기기가 제한적이다.

3.2.3 칩오프

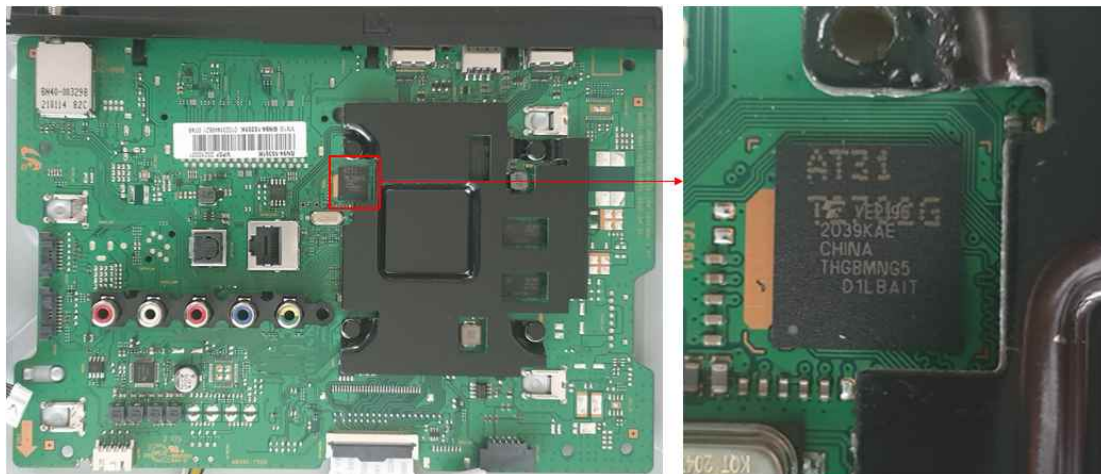
칩오프는 소프트웨어 또는 하드웨어 수준에서의 접근을 통한 내부 데이터 획득이 어려울 경우 수행 가능한 기법으로 IoT 기기를 분해하여 획득할 수 있는 PCB에 존재하는 NAND Flash Memory를 고온의 열기를 통해 물리적으로 분리하여 데이터를 수집하는 기법이다. 그러나 칩오프 기법은 기기에 치명적인 손상을 줄 수 있기 때문에 최종적으로 진행해야 하며, 본 기법의 적용 과정에서 과도한 열을 통해 Nand Flash Memory가 손상될 수 있다. 또한 최근 제작되는 일부 IoT 기기들의 경우 Nand Flash Memory가 SoC(System on Chip) 내부에 구현되어 있기 때문에, 칩오프를 하여도 데이터를 획득하는데 어려움이 발생할 수 있다. 따라서 Nand Flash Memory가 eMMC 형태로 독자적으로 구현되어 있는 경우 칩오프를 통한 데이터 획득이 가능하다. 칩오프를 통해 획득한 NAND Flash Memory는 규격에 맞는 리더기를 통해 PC에 마운트 할 수 있으며, 데이터를 RAW 이미지 형태로 획득할 수 있다. 따라서 칩오프 기법의 경우 기기 파손 및, 데이터 손상 우려가 있으나 숙련자에 의해 기법의 적용이 가능할 경우, 대상 기기의 모든 데이터를 획득할 수 있다.

IV. 데이터 획득

본 장에서는 선정된 기기에 대해 데이터를 획득할 수 있는 다양한 기법들을 적용하고, 기기별로 적용 가능한 기법 및 불가능한 기법을 설명한다. 추가적으로 적용 가능한 기법에 대해서 데이터 획득을 시도하고 그 결과를 정리한다.

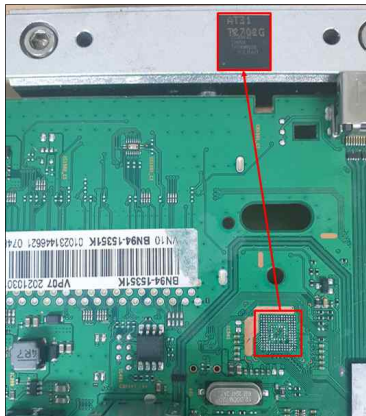
4.1 스마트 TV

스마트 TV는 삼성에서 출시한 KU43T5300AFXKR 모델을 대상으로 연구를 진행하였다. KU43T5300AFXKR 모델을 분석한 결과, 기기 외부 및 PCB에 유선 상으로 연결이 가능한 포트를 발견할 수 없었으며, Wi-Fi 및 Bluetooth를 지원하나 무선 adb 연결과 같은 데이터 획득을 위한 연결은 지원하지 않으므로, 유무선 연결을 통한 데이터 획득은 불가능하다. 추가적으로 JTAG 및 UART를 통한 데이터 획득 방안의 적용을 위해 PCB 분석을 진행하였다. PCB 상에서 일부 연결 가능한 포트를 발견할 수 있었으나, 어떠한 포트인지 식별이 어렵고 PCB에 대한 정보가 존재하지 않아 JTAG 및 UART 핀을 통한 데이터 획득이 불가능하였다. 추후 오실로스코프와 같은 도구를 사용하여 JTAG 및 UART 포트를 식별하여 연결할 수 있는 가능성이 존재한다. 분석 결과 그림 5에서 볼 수 있듯이 PCB에서 Nand Flash Memory가 존재함을 확인할 수 있었으며, Nand Flash Memory를 분석한 결과 삼성에서 제작한 eMMC 형태의 KLM4G1FETE-B041 칩임을 확인하였다. 본 칩은 4GB 용량, 153 Ball 규격을 사용함을 확인하였다.

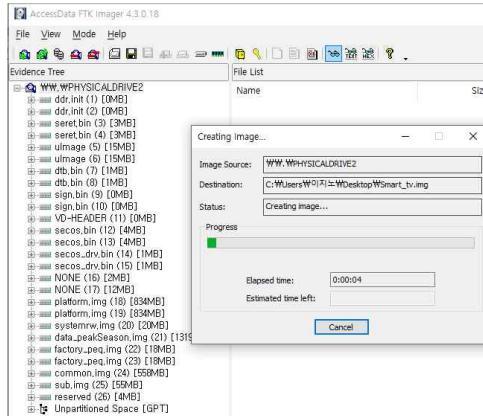


〈Figure 5〉 Nand Flash Memory of the smart TV KU43T5300AFXKR model

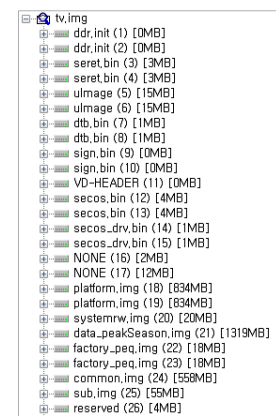
스마트 TV의 데이터 획득을 위해 그림 6과 같이 칩오프를 진행하여 Nand Flash Memory를 PCB 상에서 제거 및 획득 후, 크기 및 153 Ball 규격에 맞는 Allsocket사의 리더기를 통해 PC와의 연결을 진행하였다. 그 후 그림 7과 같이 FTK imager 프로그램 기능인 데이터 이미지 추출 통해 스마트 TV의 데이터를 획득했다. 획득한 데이터는 26개의 파티션으로 구성되어 있으며, 그중 7개의 파티션은 아무런 데이터가 저장되어 있지 않았다. 파티션 분석 시 데이터가 저장되어 있을 것이라 추측되는 크기가 큰 18,19,21,24번 파티션 위주로 분석을 진행하였다. 그림 8에서는 스마트 tv에 존재하는 파티션을 확인할 수 있으며, 내부에 데이터가 존재 유무를 표시하고, 파티션 별 사이즈를 정리하여 표 2로 나타내었다.



〈Figure 6〉 Chip-off



〈Figure 7〉 Data image export



〈Figure 8〉 Smart tv partition

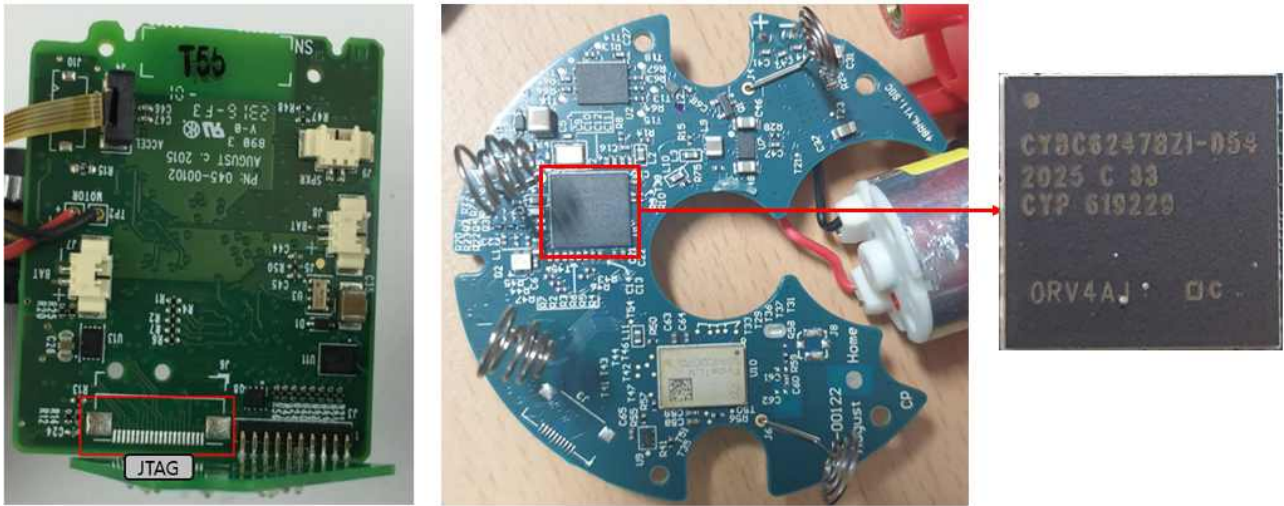
〈Table 2〉 partition size of KU43T5300AFXKR

Partition	Size	Data	Partition	Size	Data
ddr.init	512 KB	X	secos_drv.bin	1 MB	X
ddr.init	512 KB		secos_drv.bin	1 MB	
secret.bin	3 MB		NONE	2 MB	X
secret.bin	3 MB		NONE	12 MB	
ulmage	15 MB		platform.img	834 MB	
ulmage	15 MB		platform.img	834 MB	
dtb.bin	1.5 MB	X	systemrw.img	20 MB	
dtb.bin	1.5 MB		data_peakSeason.i mg	1.3 GB	
sign.bin	64 KB	X	factory_peq.i mg	18 MB	X
sign.bin	64 KB		factory_peq.i mg	18 MB	
VD-HEADER	64 KB		common.img	560 MB	
secos.bin	4 MB		sub.img	56 MB	
secos.bin	4 MB		reserved	4 MB	X

4.2 스마트 도어락

스마트 도어락은 August에서 출시한 August Smart Lock 4세대 모델을 대상으로 연구를 진행하였다. August Smart Lock 모델은 스마트폰과의 연동을 통해 무선으로 문의 개폐를 조종할 수 있는 간단한 기능을 제공한다. August Smart Lock의 경우 유선으로 연결할 수 있는 포트가 존재하지 않으며, 무선으로 스마트폰과 연결은 가능하지만 데이터 통신을 통한 데이터 획득은 불가능하다. 기존의 August Smart Lock 3세대의 경우 JTAG를 통한 디버깅이 가능했으나, 그림 9에서 볼 수 있듯이 좌측의 3세대와 우측의 4세대는 전혀 다른 PCB를 사용하기 때문에 JTAG를 통한 데이터 획득 기법의 적용이 어렵다. 또한 August Smart Lock 4세대의 PCB를 분석한 결과 시각적으로 UART 및 JTAG 포트를 식별할 수 없어 데이터 획득이 불가

능하다. 미식별 포트의 경우 추후 오실로스코프와 같은 도구를 사용하여 JTAG 및 UART 포트를 식별하여 연결할 수 있는 가능성이 존재한다. PCB 분석 결과 그림 9의 우측 사진과 같이 ARM 칩은 확인할 수 있었으나 내부 저장공간이 존재하지 않음을 확인하였기 때문에 칩오프 기술의 적용이 불가능하다. 따라서 스마트 도어락 August Smart Lock의 기기 자체에서의 데이터 획득이 불가능하다.



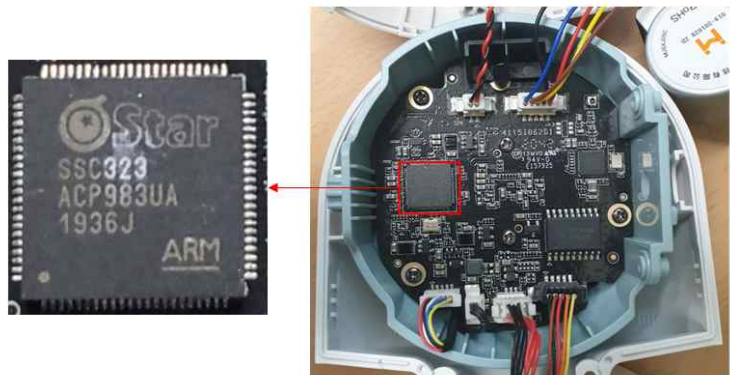
〈Figure 9〉 August Smart Lock 4th Generation (left)3rd PCB / (right)4th PCB

4.3 스마트 카메라

스마트 카메라는 IMI LAB에서 출시한 IMI LAB SmartThings Cam 360 모델을 대상으로 연구를 진행하였다. IMI LAB SmartThings Cam 360 모델은 그림 10과 같이 외부에 연결 가능한 5 pin 포트가 존재하나, 데이터 통신이 아닌 단순 충전용 포트로 확인되었다. 무선 연결의 경우 스마트폰의 SmartThings 앱을 통해 IMI LAB SmartThings Cam 360 기기와 연동이 가능하지만, 단순 조작만 가능하며 데이터 획득을 위한 무선 통신 연결은 불가능함을 확인했다. 따라서 IMI LAB SmartThings Cam 360 기기의 PCB를 분석한 결과 시각적으로 UART 및 JTAG 포트를 식별할 수 없어 데이터 획득이 불가능하다. 미식별 포트의 경우 추후 오실로스코프와 같은 도구를 사용하여 JTAG 및 UART 포트를 식별하여 연결할 수 있는 가능성이 존재한다. 그림 11은 PCB상에 존재하는 ARM 칩은 나타내고, PCB 상에 Nand Flash Memory가 존재하지 않고, 기기에서 촬영된 영상이 즉각적으로 서버에 업로드 됨을 확인하여, 칩오프 기술의 적용이 불가능함을 확인했다. 따라서 IMI LAB SmartThings Cam 360 기기 자체에서의 데이터 획득이 불가능하다.



〈Figure 10〉 Outside 5 pin



〈Figure 11〉 IMI Lab SmartThings Cam 360 PCB

V. 데이터 분석

본 장에서는 획득한 데이터를 분석하여 기기별로 아티팩트를 도출 및 정리했다. 데이터 획득 기법 중 칩오프 기법이 적용 가능한 스마트 TV만 기기 자체에서 데이터를 획득하여 분석할 수 있었으며, 스마트 TV를 제외한 기기의 경우 자체에서 기기 자체에서 데이터 획득이 아닌, 기기와 연동된 스마트폰에 저장된 데이터를 분석하였다. 데이터 분석에 사용된 프로그램은 표 3에서 확인할 수 있다.

〈Table 3〉 The program used to develop tools

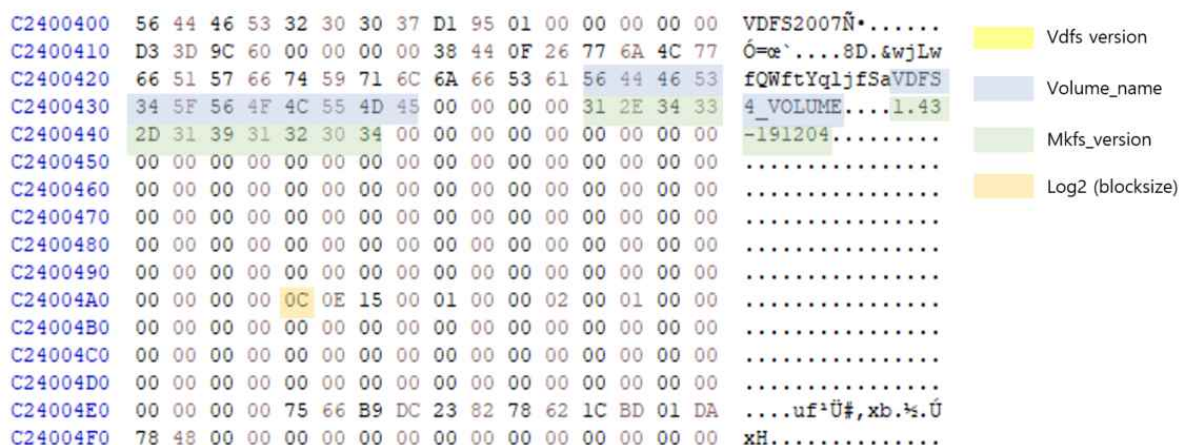
Software	Version	Information
FTK Imager	4.3.0.18	Filesystem analysis tool
Encase	21.2	Filesystem analysis tool
Hxd	2.5.0.0	Filesystem analysis tool

5.1 스마트 TV

칩오프를 통해 스마트 TV의 데이터를 획득하였으며, 26개의 파티션이 존재함을 확인했다. 26개의 파티션 중 5개의 파티션이 데이터 분석 결과 VDFS라는 파일시스템을 사용함을 확인했으며, VDFS 내부에 데이터가 저장됨을 알 수 있었다. 따라서 본 장에서는 VDFS에 대해 설명하고, Encase 도구를 사용해 데이터 추출 및 키워드 분석을 통해 획득한 아티팩트를 설명한다.

스마트 TV에서 획득한 데이터를 FTK Imager 도구를 통해 확인한 결과, 26개의 파티션이 존재함을 확인하였으며, 5개의 파티션의 Superblock에서 그림 12와 같이 'VDFS2007'이라는 매직 넘버를 확인할 수 있었다. 이는 삼성의 파일시스템인 VDFS의 매직 넘버임을 확인했다. VDFS는 삼성에서 자체 제작하고 독점화하고 있는 파일시스템이다. VDFS에 대한 공식 문서가 존재하지 않고, 관련된 정보가 거의 존재하지 않는다. VDFS는 eMMCFs라는 파일시스템을 기반으로 제작되었으며, 기반이 된 eMMCFs 또한 삼성 자체에서 개발한 삼성 eMMC 칩 전용 파일시스템으로 공개되지 않았기 때문에 많은 정보를 확인할 수 없었다. 따라서 공개된 정보가 많지 않아, 파일시스템 분석을 진행하였다.

그림 12의 superblock에서 볼륨 이름, mkfs 버전 등의 정보를 확인할 수 있었으며, block size가 0x0C(12)로 log2 x값이 12가 나오는 4096 byte가 block size임을 알 수 있다.

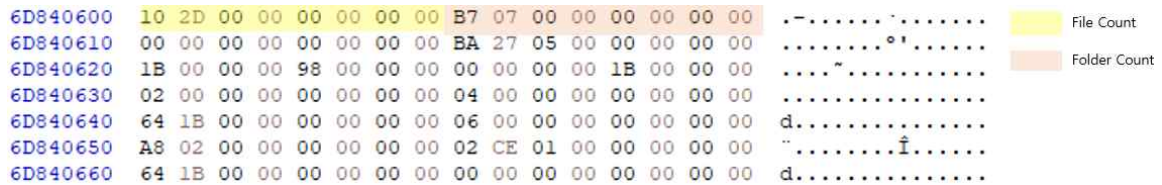


〈Figure 12〉 VDFS Superblock

VDFS 파티션의 0x600 오프셋에는 파일 및 폴더의 개수를 알 수 있다. 21번째 파티션의 파일 개수는 0x2D10으로 11536개의 파일이 있으며 폴더의 경우 0x7B7로 총 1975개로, VDFS 파일 시스템 내부의 파일 및 폴더의 개수를 확인할 수 있다. 각각의 VDFS 파티션의 파일 및 폴더 개수를 정리하여 표 4로 정리하였다.

〈Table 4〉 Number of file and folders of VDFS partition


Partition	File	Folder	Artifact
17	136	35	-
19	24789	1	System Partition
20	10	6	-
21	11536	1975	Device, Wifi information, E-mail Data Partition
24	16259	1	System Partition



〈Figure 13〉 Number 21 VDFS partition files and folders

파일 시스템 분석 후, Encase 도구를 사용해 VDFS 파티션에서 파일 카빙 및 키워드 검색과 같은 아티팩트 분석을 진행했다. 스마트 TV에서 획득한 전체 아티팩트를 표 5에 정리한 후, 획득한 아티팩트 별 정보를 서술하였다.

〈Table 5〉 Smart TV Data Acquisition Performance Artifact Table

Device	Method	Artifact	Information
Smart Full HD LED Smart TV	Keyword Filter	T-KTS2AKUC-2013.3/ KU43T5300AFXKR/ OACL3NCR300644H	TV firmware information, model name, serial number.
		DESKTOP-1G6J8RE 2021-07-12T08:05:07	Connected Wi-Fi information, connection time
		testmju429@gmail.com / jinnxxx@naver.com	All logged-in accounts email addresses
		Mirroring-app-tv 2021-04-26 15:19:30	Successful mirroring with smartphones and time information
		[power off][14:02:19]	Smart TV's on/off time information
		"action_play_url": " https://www.youtube.com " "action_play_url": " https://www.jr.naver.com "	Internet access history
	File Carving		The internet capture screen logged in to

Encase의 키워드 검색 기능을 사용하여 일부 아티팩트를 획득할 수 있었다. deviceinfo, firmware 등을 키워드로 설정하여 검색한 결과 그림 14와 같이 기기에 설치된 펌웨어 정보, 기기 명, 기기의 시리얼 넘버 데이터와 같은 기기 정보가 존재함을 확인했으며, 사용자 행위와 관련된 정보 또한 Encase의 키워드 검색 기능을 이용해 확인할 수 있었다. wifi, ipv4 등의 키워드를 통해 그림 15와 같이 연결되었던 Wi-Fi 이름, Wi-Fi가 연결된 시각, Wi-Fi의 IP 주소를 획득할 수 있다. 그림 16은 사용자가 로그인했던 E-mail 주소를 나타내며, gmail, naver 등과 같은 다양한 도메인을 키워드로 지정해 검색하였다. E-mail 주소는 현재 연동되어있는 E-mail 뿐만 아니라 과거에 연동했었던 E-mail 주소 또한 저장되어 있음을 확인할 수 있었다.

```
7d86c3877_4445534b544f502d3147364
a3852452034373938_managed_psk] Name=DESKTOP-1G6J8RE 4798 SSID=4445
534b544f502d3147364a3852452034373
938 Frequency=2412 Enc=true LastC
onected=true BSSID.List.Count=1
Favorite=true AutoConnect=true Mo
dified=2021-07-12T08:05:07.005126
Z IPv4.method=dhcp IPv4.DHCP.Last
Address=192.168.137.182 IPv6.meth
od=auto IPv6.privacy=preferred Nam
eservers.IPv4method=dhcp UID=0 Pa
ssphrase=e05d794d71f3aa4caba7calb
```

〈Figure 15〉 Wi-Fi information

```
.....<deviceinfo><du
id>ZPCN4Z5WRWN62</duid><firmw
areversion>T-KTS2AKUC-2013.3<
/firmwareversion><modelname>K
U43T5300AFXKR</modelname><ser
ialnumber>OACL3NCR300644H</se
rialnumber></deviceinfo>.....
```

〈Figure 14〉 TV device information

```
.. ..testmju429@gma
il.comtestmju429@gmail.comte
stmju429@gmail.comorg.tizen.
ssoservice.. ///..5.....
.....jinn@naver.comjin
n@naver.comjinn@naver.
```

〈Figure 16〉 User E-mail

스마트폰의 SmartThings 앱을 통해 미러링이 가능하다. 미러링 정보 데이터는 mirroring 키워드 검색을 통해 확인할 수 있었으며, 그림 17과 같이 접속 시간, 접속 날짜 등을 확인할 수 있었으나, 연동된 기기에 대한 정보와 같은 사용자 정보는 획득할 수 없었다. 인터넷 접속기록 또한 url, 도메인 주소 등의 키워드를 통해 그림 18과 같이 확인할 수 있었으며, 어떤 사이트에 접속했는지, url과 접속한 사이트의 캡처화면이 어떠한 파일명으로 저장되는지 확인할 수 있다.

```
1417] 2021-04-26 15:19:26 SUCCESS: 378
org.tizen.tv-viewer

[ 1418] 2021-04-26 15:19:27 TERMIN
ATED 3963

[ 1419] 2021-04-26 15:19:27
LAUNCHING org.tizen.ScreenMirror
ing-app-tv

[ 1420] 2021-04-26 1
5:19:27 SUCCESS: 1270 org.tizen.Scree
nMirroring-app-tv

[ 1421] 2021-
04-26 15:19:30 RESUMING org.tize
n.tv-viewer

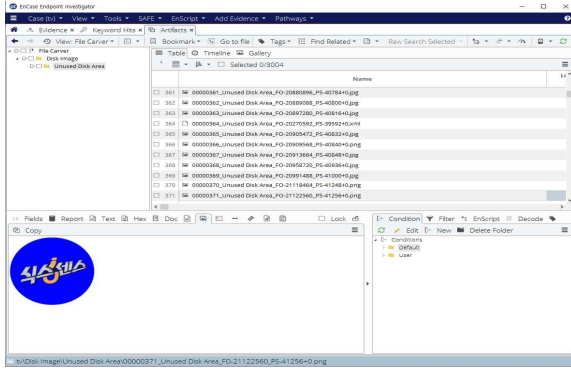
[ 1422
] 2021-04-26 15:19:30 SUCCESS: 378 o
rg.tizen.tv-viewer
```

〈Figure 17〉 Mirroring time data

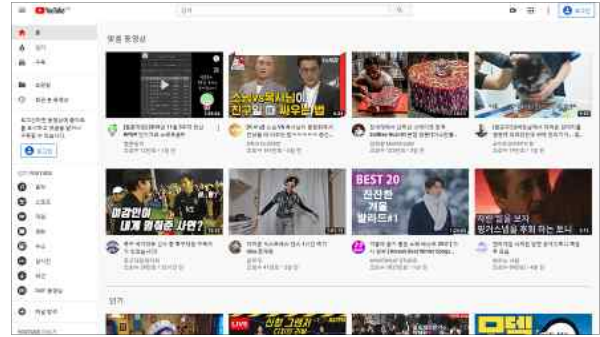
```
launcherNormalIcon":"/home/owner/apps_r
w/com.samsung.tv.csfs/shared/trusted//
data/image/fsdm/12855.png", "launcherTy
pe":"launcher", "title":"YouTube", "subt
itle":""," "action_play_url":"https://ww
w.youtube.com", "aciton type":"APP LAUN
CH", "isLock":false}, {"id":"2734", "name
":"2734", "nameSID":null, "appId":"org.t
izen.browser", "appType":"pxdb_app", "ic
on":"/home/owner/apps_rw/com.samsung.t
v.csfs/shared/trusted//data/image/fsdm
/1197.png", "launcherNormalIcon":"/home
/owner/apps_rw/com.samsung.tv.csfs/sha
red/trusted//data/image/fsdm/1197.png"
, "launcherType":"launcher", "title":"iY
~ëx`i-`ë,,n|`ë²,,", "subtitle":""," "actio
n_play_url":"https://jr.naver.com", "ac
iton_type":"APP_LAUNCH", "isLock":false
}, {"id":"2735", "name":"2735", "nameSID"
```

〈Figure 18〉 Internet access history

Keyword Filter 뿐만 아니라 File Carving 기능을 이용해 스마트 tv의 일부 데이터를 획득할 수 있다. 그러나 VDFS의 구조에 대한 정보가 존재하지 않아 크기가 한 블록(0x1000)이 넘어가는 파일의 경우 파일 카빙이 정상적으로 진행되지 않은 이슈가 존재한다. 파일 크기가 작은 일부 썸네일 파일들의 경우 그림 19와 같이 카빙이 정상적으로 진행되며, 그림 20에서 확인할 수 있듯이, 접속했던 인터넷 사이트가 png 파일로 캡처되어 저장됨을 확인할 수 있었다.



〈Figure 19〉 Thumbnails obtained through Carving



〈Figure 20〉 The captured internet site

5.2 스마트 도어락

연동된 기기를 통해 스마트 도어락 August Smart Lock의 데이터를 획득하였으며, 연동 기기로는 루팅된 스마트폰 갤럭시 S9을 사용하였다. 연동된 기기에 저장된 데이터를 분석한 결과 로그, 위치 정보, 사용자 정보 와 같은 아티팩트를 획득할 수 있었다.

스마트 도어락의 아티팩트 분석의 경우 연동된 스마트폰을 통해 진행했다. 스마트 도어락과 연동된 스마트폰에서 데이터를 획득하여 표 6에 정리한 후, 획득한 아티팩트 별 정보를 서술하였다.

〈Table 6〉 Smart TV Data Acquisition Performance Artifact Table

Device	App name (Package directory)	Detail path	Information
August Smart Lock (4th Generation)	August (/data/data/com.august.luna)	/databases/ModelDatabase.db	User information such as user name, contact number, email, door lock name
	August (/data/data/com.august.luna)	/databases/LocationDatabase.db	Location information of the connection device.
		/databases/RemoteLogQueue.db	Remote control log information

스마트폰에 설치된 August의 Smart Lock의 자사 앱인 August 앱의 디렉토리 '/data/data/com.august.luna'에서 사용자 데이터를 획득하였다. 'ModelDatabase.db' 파일에는 그림 21,22와 같이 앱에 연결된 도어락 정보, 사용자 정보 등을 확인할 수 있다. 'Userdata' 테이블에서는 앱에 등록된 사용자의 이름, userID, 핸드폰 번호, 이메일 등의 사용자 정보를 확인할 수 있으며, 'LockData' 테이블에서는 같이 앱에 등록된 도어락의 시리얼 넘버, 맥주소와 같은 기기정보를 확인할 수 있었다.

테이블(T): UserData						
userID	firstName	lastName	phone	email	pictureUrl	
필터	필터	필터	필터	필터	필터	
1 f076f9ae-a4b7-4cbf-ae01-5616e2f32b9a	노	지	+82106609[redacted]	jino95[redacted]@gmail.com	NULL	
2 d3ed5fd9-5038-4d86-9dc0-ce5e631f50a3	minju	Kim	NULL	NULL	NULL	
3 c606848a-a6a1-4ddd-a1e1-dcea614dc6d0	shin	dongwon	+82104538[redacted]	ehd[redacted]@naver.com	https://d33mytkkohwnk6.cloudfront.net/user/...	

〈Figure 21〉 User information in the Model Database.db file

데이터(T): LockData										
sku	ouseNar	type	LockID	HouseID	LockName	SerialNumber	Firmware\	macAddress	pubsubChannel	ownerIDs
필터	필터	필터	필터	필터	필터	필터	필터	필터	필터	필터
1	AUG-SL05...	무리 집	5 E006FB672BE14ED...	e9aee00f-849c-4138-...	알 문	L5V15000YP	1.1.10	78:9C:85:15:10:06	e6cf5207-4241-4f8...	c606848a-...

<Figure 22> Connection door lock information of the Model Database.db file

사용자 행위 관련 정보 또한 획득할 수 있었으며, August 앱의 'LocationDatabase.db' 파일에는 앱에 등록된 도어락의 위치 정보, 연결 네트워크 정보 등을 확인할 수 있었다. 그림 23과 같이 'UserLocation' 테이블에서는 사용자의 위도 및 경도 정보, 시각 정보, deviceID 등의 사용기록을 확인할 수 있었다. 또한 그림 24와 같이 'RemoteLogQueue.db' 파일에는 August 앱을 사용하여 스마트 도어락을 원격으로 제어한 로그 정보를 확인할 수 있다.

데이터(T): UserLocation				
timestamp	longitude	latitude	actionTaken	deviceID
필터	필터	필터	필터	필터
1	1626328912036	127.045977897942	37.2867362546877	{"a":"ENABLED... E006FB672BE14ED08C04AE4900FA4C54

<Figure 23> User location information in the Location Database.db file

데이터(T): RemoteLogModel		
rowID	timestamp	log
필터	필터	필터
1	1069 1626529575748	{"Auto-Unlock":{"Android SDK":"28","Device":"SM-G960N","Manufacturer":"samsung","App Version":"11.5.0","Scheduled Job":"Abrupt stop","userId":"c606848a-a6a1-4ddd-a1e...
2	1070 1626529576203	{"Auto-Unlock":{"Android SDK":"28","Device":"SM-G960N","Manufacturer":"samsung","App Version":"11.5.0","Scheduled Job":"Abrupt stop","userId":"c606848a-a6a1-4ddd-a1e...

<Figure 24> Remote door lock control information of the RemoteLogQueue.db file

5.3 스마트 카메라

연동된 기기를 통해 스마트 카메라 IMI LAB SmartThings Cam 360의 데이터를 획득하였으며, 연동 기기로는 루팅되어진 스마트폰 갤럭시 S9을 사용하였다. 연동 기기에 저장된 데이터를 분석한 결과 로그, 위치 정보, 사용자 정보 와 같은 아티팩트를 획득할 수 있었다.

스마트 카메라의 아티팩트 분석의 경우 연동된 스마트폰을 통해 진행했다. 스마트 도어락과 연동된 스마트폰에서 데이터를 획득하여 표 7로 정리한 후, 획득한 아티팩트 별 정보를 서술하였다.

<Table 7> Smart TV Data Acquisition Performance Artifact Table

Device	App name (Package directory)	Detail path	Information
SmartThings Cam 360	SmartThings (/data/data/com.samsung.android.oneconnect)	/database/CommonData.db	User information such as email and name.
		/database/Cloud.db	Connected device information
	SmartThings (/data/data/com.samsung.android.oneconnect)	/database/CamActivityHistory.db	Camera motion log information

IMI LAB SmartThings Cam 360의 경우 SmartThings 앱을 사용하기 때문에 스마트폰 내부의 SmartThings 앱 디렉터리의 '/data/data/com.samsung.android.oneconnect'에서 스마트 카메라에 대한 사용자 데이터를 획득하였다. 디렉터리의 'CommonData.db' 파일에서는 그림 25와 같이 SmartThings 앱 사용자와 기본 설정에 대한 정보를 확인할 수 있었다. 또한

‘Cloud.db’ 파일에서는 SmartThings에 연결된 기기의 정보를 확인할 수 있다. 그림 26과 같이 Cloud.db 파일의 ‘devices’ 테이블에서 연결된 기기의 이름, 디바이스 id, 모델명 등의 정보를 확인할 수 있었다.

locationid	owner
4c853bc6-22cb-48f5-9b53-5cb5f885bbf1	{ "email": "jinno950512@gmail.com", "uuid": "311c30c8-57e2-0a47-e611-6cd8dd82eb3", "name": "진오 이", "samsungAccountid": "x7qsgnopp" }

〈Figure 25〉 CommonData.User information in the db file

deviceId	groupId	locationid	deviceName	nick	permission	modelid
9e619a6a-49be-4542-877d-2ddadaeff117	9b5038a8-aa46-4022-967-2ac18c645a11	4c853bc6-22cb-48f5-9b53-5cb5f885bbf1	ST-4	홈카메라 360	1	oic.d.camera&SmartThings@SmartThings...
5dd1b6b6-bd0c-423b-bd73-c5f6ad1ba6d5	9b5038a8-aa46-4022-967-2ac18c645a11	4c853bc6-22cb-48f5-9b53-5cb5f885bbf1	앞 문	문	1	oic.d.smartlock&SmartThings@SmartThings...

〈Figure 26〉 Connected device information in the Cloud.db file

사용자 행위 관련 정보 또한 획득할 수 있었으며, IMI LAB SmartThings Cam 360의 데이터가 저장된 SmartThings 앱 디렉터리의 ‘CamActivityHistory.db’ 파일에서 카메라의 동작과 관련된 로그를 확인할 수 있다. 그림 27과 같이 카메라의 움직임 센서, 소리 센서에 기록된 로그, 비디오 녹화 로그 등의 정보를 시간 순서대로 확인할 수 있다.

epoch	date	capability	attribute	value	recReason	clipState	clipUrl
1	1626325869952	15일 14:11	switch	switch	on	NULL	NULL
2	1626325869953	15일 14:11	soundDetection	supportedSoundTypes	["babyCrying"]	NULL	NULL
3	1626325876397	15일 14:11	motionSensor	motion	active	NULL	NULL
4	1626325878400	15일 14:11	soundSensor	sound	detected	NULL	NULL
5	1626325887704	15일 14:11	signalStrength	lqi	34	NULL	NULL
6	1626325887705	15일 14:11	signalStrength	rss	-73	NULL	NULL
7	1626325889943	15일 14:11	signalStrength	rss	-73	NULL	NULL
8	1626325894837	15일 14:11	soundSensor	sound	not detected	NULL	NULL
9	1626325896969	15일 14:11	soundSensor	sound	not detected	NULL	NULL
10	1626325897003	15일 14:11	motionSensor	motion	inactive	NULL	NULL
11	1626325899727	15일 14:11	motionSensor	motion	active	NULL	NULL
12	1626325902801	15일 14:11	soundSensor	sound	detected	NULL	NULL
13	1626325902809	15일 14:11	signalStrength	rss	-74	NULL	NULL
14	1626325915204	15일 14:11	signalStrength	rss	-74	NULL	NULL
15	1626325953798	15일 14:12	soundSensor	sound	not detected	NULL	NULL
16	1626325953829	15일 14:12	motionSensor	motion	inactive	NULL	NULL
17	1626325956594	15일 14:12	motionSensor	motion	active	NULL	NULL
18	1626325976832	15일 14:12	videoCapture	clip	{ "status": "INITIATED", "clipPath": "https://..." }	manual	failed
19	1626326017961	15일 14:13	motionSensor	motion	inactive	NULL	NULL
20	1626326018655	15일 14:13	motionSensor	motion	active	NULL	NULL
21	1626326019735	15일 14:13	soundSensor	sound	detected	NULL	NULL
22	1626326105559	15일 14:15	soundSensor	sound	not detected	NULL	NULL
23	1626326105590	15일 14:15	motionSensor	motion	inactive	NULL	NULL
24	1626326107970	15일 14:15	motionSensor	motion	active	NULL	NULL

〈Figure 27〉 Log information of CamActivityHistory.db file

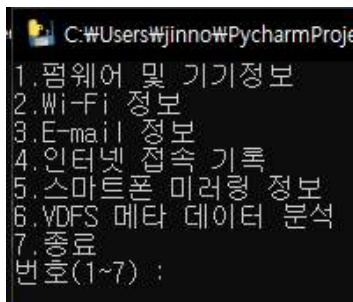
VI. 도구 개발 및 검증

스마트홈 가전 및 IoT 기기 포렌식을 수행하여 스마트 TV의 VDFS 파일시스템에서의 데이터 획득을 통해 사용자 정보, 시간 기록 정보 등과 같은 아티팩트를 도출하였다. 스마트 TV 사용자 정보 또는 시간 기록 아티팩트는 범죄 발생 시, 수사에서 알리바이 혹은 증거를 제공해 줄 수 있는 중요한 정보가 될 수 있다. 따라서 삼성 스마트 TV에 사용되는 VDFS 파일시스템에서 아티팩트를 추출할 수 있는 분석 도구를 개발한다. 본 도구는 VDFS 파일시스템을 분석하여 기본적인 메타데이터를 분석하고, 펌웨어 및 기기정보와 같은 기본적인 정보를 추출한다. 도구 개발 시 python을 사용하여 개발을 진행했으며, 도구 개발에 사용된 소프트웨어는 표 8에서 확인할 수 있다.

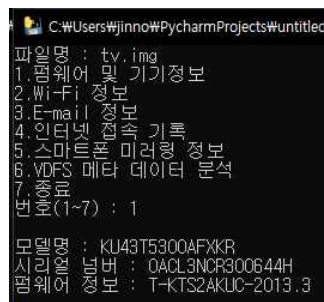
〈Table 8〉 The program used to develop tools

Software	Version	Information
Python	3.7.1	Language used to develop tool
Pycharm	11.0.7	Python program
Encase	21.2	Artifact acquisition program

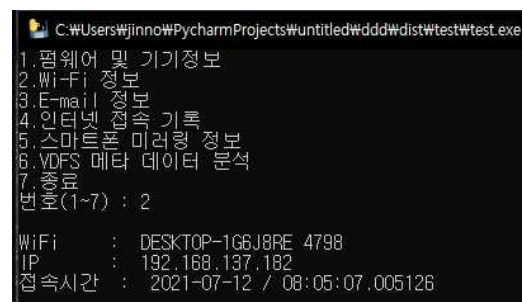
그림 28은 VDFS 파일시스템을 분석하여 도구를 통해 획득할 수 있는 아티팩트를 나타내며 번호 입력 시 파일 전체를 조사하여, 각 번호에 해당되는 아티팩트가 출력되도록 한다. 그림 29는 기기에 설치된 펌웨어 정보와 기기 자체의 모델명, 시리얼 정보와 같은 기본정보를 추출함을 보여준다. Wi-Fi 정보는 기기 사용 시 접속했던 Wi-Fi 이름, IP 및 접속 시간을 추출하며 그림 30에서 확인할 수 있다.



〈Figure 28〉 Artifact list



〈Figure 29〉 Firmware



〈Figure 30〉 Logged Wi-Fi information

E-mail 아티팩트의 경우 사용자가 원하는 도메인을 입력 시, 입력한 도메인을 포함한 메일 주소를 출력하며 그림 31에서 확인할 수 있다. 추가로 접속한 인터넷 url, 스마트폰 미러링 시각 등 수사 시에 증거로 사용될 수 있는 아티팩트 또한 추출이 가능하다. 그림 32는 VDFS 파티션의 메타 데이터를 분석한 정보를 출력한 화면이다. 번호 입력 시, VDFS 파티션에 대한 파티션 명, 버전, 파티션 개수와 같은 기본 정보를 확인할 수 있으며, 파티션 번호 입력을 통해 해당 파티션의 파일 및 폴더 개수를 확인할 수 있다.

본 도구는 VDFS 파일시스템을 도구에 입력 시, 이미지를 분석하여 크리덴셜을 출력하도록 개발하였다. 본 도구를 통해 사용자 정보 및, 수사에 도움이 될 수 있는 여러 시간 관련 데이터를 획득할 수 있으며, 획득한 데이터를 통해 범죄 수사 시에 삼성 스마트 TV를 통한 증거 확보에 도움이 될 수 있도록 한다.

```

1.펌웨어 및 기기정보
2.Wi-Fi 정보
3.E-mail 정보
4.인터넷 접속 기록
5.스마트폰 미러링 정보
6.VDFS 메타 데이터 분석
7.종료
번호(1~7) : 3

검색할 이메일 도메인 입력(ex: @gmail.com) : gmail.com
E-mail : testmju429@gmail.com

```

〈Figure 31〉 E-mail information

```

1.펌웨어 및 기기정보
2.Wi-Fi 정보
3.E-mail 정보
4.인터넷 접속 기록
5.스마트폰 미러링 정보
6.VDFS 메타 데이터 분석
7.종료
번호(1~7) : 6

VDFS 파일시스템
VDFS Volume Name : VDFS4_VOLUME
VDFS mkfs Version : 1.43-191204
VDFS 파티션 개수 : 5
파티션 정보확인 (Y or N) : Y
파티션 번호( 1 ~ 5 )
1
파일 개수 : 136
폴더 개수 : 35

```

〈Figure 32〉 VDFS partition metadata

VII. 결론

기술의 발전으로 AI 스피커, 스마트 가전제품 등 다양한 IoT 기기들이 제조되고 있으며, 이에 따라 IoT 기기들의 가정 보급률 또한 상승하고 있다. IoT 기기를 통한 일상생활의 편리성이 상승하고 있으나, 이와 비례하여 개인정보 유출 등의 보안 범죄들이 발생하고 있다. 보안사고 발생 시, 디지털 포렌식을 통해 IoT 기기 내부 또는 클라우드에 존재하는 데이터를 획득할 수 있으나, 현재 매우 다양한 종류의 IoT 기기가 존재하기 때문에 적용할 수 있는 기법 또는 방법이 모두 상이하다. 이에 따라 본 연구에서는 가정에서 주로 사용되고 있으며, 사용자 관련 데이터가 저장될 것으로 추정되는 IoT 기기를 대상으로 선정 했으며, 기기별 인터페이스 및 하드웨어 분석을 통해 적용 가능한 데이터 획득 기법을 연구하였다.

기기 인터페이스 및 하드웨어 분석을 진행한 결과 스마트 TV의 Nand Flash Memory가 존재함을 확인했으며, 칩오프를 통한 데이터 이미지 획득에 성공할 수 있었다. 획득한 데이터 분석을 통해 삼성 스마트 TV는 VDFS 파일시스템을 사용함을 확인했다. 이에 따라 VDFS의 메타데이터를 분석하고, 아티팩트를 분석 및 추출하였다. 삼성 스마트 TV를 통해 TV 모델명과 같은 기본적인 정보부터, TV 시청 시각, 접속한 인터넷 사이트와 같이 알리바이 및 범죄의 증거로 사용될 수 있는 정보 및 사용자 E-mail과 같은 크리덴셜 또한 존재함을 확인했다. 그러나 소형 IoT 기기들의 경우 분석 결과 Nand Flash Memory가 존재하지 않아 기기 자체의 데이터 획득이 불가능하기 때문에, 서버와 연동되어 있는 기기인 스마트폰을 통해 데이터를 획득하였다. 스마트폰을 통해 획득한 IoT 기기 아티팩트로는 연결된 기기 정보, 작동 시각, 위치 정보 등 매우 중요한 데이터가 존재했다. 분석 결과 삼성 스마트 TV의 데이터 획득을 통해 획득할 수 있는 아티팩트는 수사에 사용될 수 있다고 판단되므로, 삼성 스마트 TV의 내부 아티팩트를 획득할 수 있는 도구를 개발하였다.

본 연구를 통해 Nand Flash Memory가 존재하지 않는 다양한 IoT 기기들의 데이터 획득이 스마트폰을 통해 가능함을 확인하였고, 삼성 스마트 TV의 파일시스템인 VDFS와 획득한 아티팩트 분석을 진행했으며, 삼성 스마트 TV의 분석에 사용 가능한 도구를 개발하였다. 따라서 본 연구를 통해 추후에 진행될 수사 시 스마트 TV에서 획득한 데이터를 획득하는데 기여할 수 있고, 획득한 데이터가 VDFS를 사용할 경우 개발한 도구를 통해 아티팩트 획득에 도움이 될 것이라 생각한다. 또한 추후에 있을 추가 연구를 통해 VDFS 메타데이터를 분석하고, 분석한 메타데이터를 통해 데이터를 db 파일과 같은 형태로 추출해 보다 많은 아티팩트를 효율적으로 획득할 수 있을 것으로 기대된다.

참 고 문 헌 (References)

- [1] Wang, H., Zhang, Z., & Taleb, T. (2018). Special issue on security and privacy of IoT. *World Wide Web*, 21(1), 1-6.
- [2] CCTVnews, "IoT devices are increasing. Hacking fear still lingers.", Available: <https://www.cctvnews.co.kr/news/articleView.html?idxno=217963>. 2021.11.01. confirmed
- [3] Junjanews "Investigate crimes with home IoT data.It's the first digital forensic technology ever.", Available: <https://m.etnews.com/20210802000190>, 2021.11.04. confirmed
- [4] Techworld, '스마트 홈' 시장, 올해 14.1% 성장...기존 전망치 대비 7.5%p↓, <http://www.epnc.co.kr/news/articleView.html?idxno=107716>, 2020.11.03. confirmed
- [5] Shin, Y., Kim, H., Jo, W., & Shon, T. (2019, December). An Security Analysis of Ext Filesystem metadata. In 2019 4th Technology Innovation Management and Engineering Science International Conference (TIMES-iCON) (pp. 1-5). IEEE.
- [6] Dewald, A., & Seufert, S. (2017). AFEIC: Advanced forensic Ext4 inode carving. *Digital Investigation*, 20, S83-S91.
- [7] Jo, W., Shin, Y., Kim, H., Yoo, D., Kim, D., Kang, C., ... & Shon, T. (2019). Digital forensic practices and methodologies for AI speaker ecosystems. *Digital Investigation*, 29, S80-S93.
- [8] Boztas, A., Riethoven, A. R. J., & Roeloffs, M. (2015). Smart TV forensics: Digital traces on televisions. *Digital Investigation*, 12, S72-S80.
- [9] Nemayire, T., Ogbole, A., Park, S., Kim, K., Jeong, Y., & Jang, Y. (2019). A 2018 Samsung Smart TV Data Acquisition Method Analysis. *디지털포렌식연구*, 13(3), 205-218.

저 자 소 개



이 진 오 (Jino Lee)

준회원

2021년 : 아주대학교 사이버보안학과 졸업

2021년 3월~현재 : 아주대학교 AI융합네트워크학과 석사과정

관심분야 : 파일시스템 포렌식, IoT 포렌식 등



손 태 식 (Taeshik Shon)

평생회원

2000년 : 아주대학교 정보및컴퓨터공학부 졸업(학사)

2002년 : 아주대학교 정보통신전문대학원 졸업(석사)

2005년 : 고려대학교 정보보호대학원 졸업(박사)

2004년 ~2005년 : University of Minnesota 방문연구원

2005년 ~2011년 : 삼성전자 통신·DMC 연구소 책임연구원

2017년 ~2018년 : Illinois Institute of Technology 방문교수

2011년 ~ 현재 : 아주대학교 정보통신대학 사이버보안학과 교수

관심분야 : Digital Forensics, ICS/Automotive Security