범죄사고 조사를 위한 스마트 홈 플랫폼 증거물 수집 및 활용방안 연구

김유빈[1]*, 이종범[1], 엄익채[2]
전남대학교 시스템보안 연구센터(대학원생[1], 교수[2])

Research on the Collection and Utilization of Evidence from Smart Home Platform for Criminal Accident Investigation

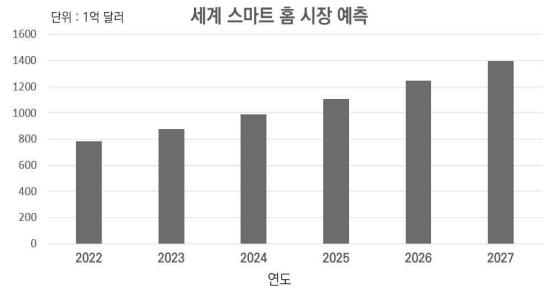
You-Bin Kim[1]*, Jong-Bum Lee[1], Ieck-Chae Euom[2]

요약 : 스마트 홈 기기는 다른 사물인터넷 기기와 다르게 다양한 센서 정보를 수집하기 때문에 범죄사고가 발생했을 많은 증거를 생성할 수 있다. 그러나 스마트 홈 기기는 제조사 및 기기가 다양해 저장하는 방식이 달라 표준화된 로그 수집 및 분석이 부족하고 범죄사고를 위한 활용방안이 부족하다. 따라서, 본 연구는 스마트 홈 환경을 구축하여 범죄사고에 조사에 활용할 수 있는 로그를 수집하고 식별해 활용방안을 제시해 범죄사고 조사를 위한 기반을 마련하였다.

Key Words : Smart Home, Digital Forensic, IoT, Log Collection

1. 서 론

사물인터넷의 증가로 실생활에 밀접하게 사용되는 스마트 홈 기기도 증가하였다. [그림 1]과 같이 전 세계 스마트 홈 관련 수익이 2022년에는 783억 달러에 달했고, 2027년에는 1400억 달러까지 증가할 것이라고 통계업체 'FutureMarketInsights'는 예상하였다[1]. 다양한 센서로 정보를 수집하는 스마트 홈 기기는 범죄사고에 관련한 많은 증거를 남길 수 있다. 실제로 2019년 7월 스마트 홈 기기인 스마트 스피커에 저장된 녹음 기록을 이용해 사용자의 무죄를 입증하였다[2]. 따라서 스마트 홈 기기는 범죄사고 조사를 위한 주요 분석 대상이다. 그러나 스마트 홈 기기의 제조사 및 기기별로 로그 및 증거물을 저장하는 방식이 달라 표준화된 증거물 수집과 이를 분석하는 방법이 부족하다. 이에 따라 본 연구는 스마트 홈 기기 실험 환경을 구축하여 로그를 수집하고 분석한다. 그리고 생성되는 로그 중 범죄사고에 활용에 효과적인 증거물을 제시하고 이를 범죄 시나리오를 통해 뒷받침한다.



[그림 1] 세계 스마트 홈 시장 전망

2. 관련 연구 및 배경

2.1 관련 연구

스마트 홈 기기를 대상으로 범죄사고 증거 수집에 관한 연구는 다양하게 이루어지고 있다. Kang.s 외 3명은 샤오미 스마트 홈 플랫폼을 대상으로 생성되는 각종 센서 정보 및 기기 정보를 수집하였고, 범죄 시나리오를 구상해 추가적인 활용방안을 제시하였다[3]. Lee.J외 1명은 스마트 홈 기기 대상으로 하드웨어를 통한 접근, 인터페이스를 통한 접근과 같이 다양한 방법을 사용하여 증거물 수집을 시도하였다[4]. 스마트 홈 기기 증거 수집에 관한 연구는 다양한 기기의 증거 수집과 분석 그리고 활용방안이 필요하다. 따라서 본 연구는 추가적인 스마트 홈 기기의 증거 수집과 이를 활용할 수 있는 방안을 제시한다.

2.1 스마트 홈

스마트 홈은 집에서 사용하는 사물인터넷으로 각 기기는 서로 연결되어 사용자와 상호 작용할 수 있도록 만든 시스템이다. 스마트 홈 기기는 플랫폼마다 연결되는 기기가 다르며, 본 연구는 삼성이 개발한 스마트싱스 플랫폼을 다룬다. 스마트싱스의 스마트 홈 기기는 허브와 연결되는 기기와 클라우드로 바로 연결되는 기기 그리고 서드파티 클라우드를 통해 연결하는 기기가 있다. 각 기기의 데이터는 클라우드 서버에 저장되며 사용자는 애플리케이션을 통해 클라우드 데이터를 받아와 기기를 제어하고 관리할 수 있다.

3. 실험 환경 구축 및 아티팩트 수집 및 분석

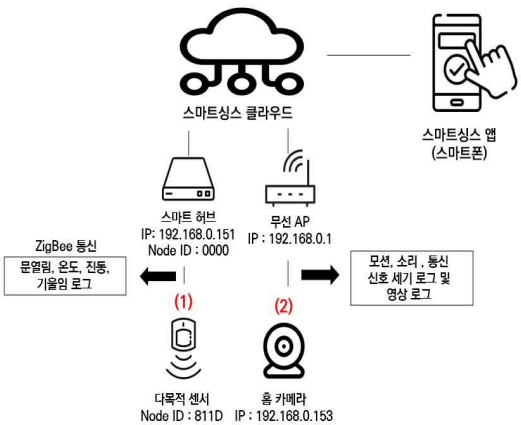
3.1 실험환경 구축

본 연구는 삼성 스마트싱스를 대상으로 스마트 홈을 구축하였다. 스마트 홈 기기, 애플리케이션, 분석 도구, 스마트폰으로 실험하였으며, 소프트웨어/펌웨어 버전은 [표 1]과 같다.

[표 1] Smart home devices and analytics tool

분류	이름	버전
스마트 홈 기기	SmartThings 허브 v3	000.047.00011
	SmartThings 다목적 센서	-
	SmartThings 카메라 360	2.1.3
애플리케이션	SmartThings App	1.8.01.22
분석 도구	DB Browser for SQLite	3.1.12
스마트폰	Galaxy A 12	andoroid 12

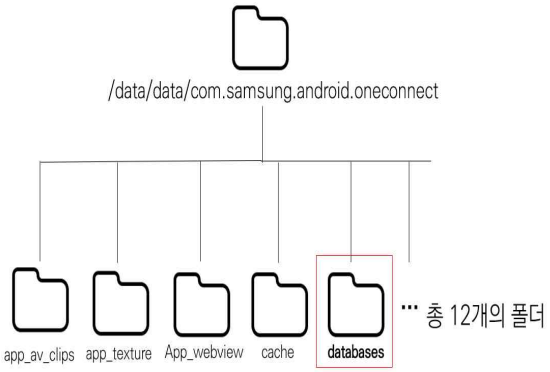
실험은 스마트 홈 기기가 허브와 연결되는 방식(1)과 허브와 연결되지 않고 직접 클라우드에 데이터를 저장하는 방식(2)으로 두 가지 통신 환경으로 구상하였다. 실험 환경에 대한 전체적인 구성은 [그림 2]와 같이 설정하였고, 스마트싱스에 저장된 로그에 접근하기 위해 스마트폰을 루팅하였다.



[그림 2] Setting up an experimental environment

3.2 아티팩트 수집

스마트싱스 애플리케이션에 저장되는 패키지 폴더명은 com.samsung.android.oneconnect이다. 패키지는 내부 저장소에 저장되며, 루팅된 스마트폰으로 접근할 수 있다. [그림 3]와 같이 패키지 내에는 12개의 폴더가 존재했으며, 폴더 중 로그 정보가 가장 많은 database 폴더를 수집 및 분석하였다. database 폴더에는 58개의 데이터베이스 파일이 존재하며 58개의 데이터베이스 파일을 식별할 수 있었으며 33개의 파일에서만 해석할 수 있는 데이터를 획득할 수 있었다. 33개의 파일 중 9개의 파일은 내용이 중복돼 제외하였고, 남은 24개의 데이터베이스 파일의 테이블 수, 필드 수, 그리고 얻을 수 있는 주요 내용으로 [표 3]과 같이 정리하였다.



[그림 3] SmartThings Package Folder

3.3 아티팩트 분석

데이터베이스에 저장되는 로그들은 센서와 관련 없는 정보가 저장되거나 중복되는 정보가 많아 범죄사고에 바로 활용하기에 어려움이 있다. [표 2]는 범죄사고에 활용할 수 있는 데이터베이스를 선정하였고, 다음 장에는 선정된 데이터베이스의 타당성을 범죄사고 시나리오를 통해 검증하였다.

[표 2] Selected databases

데이터베이스	정보
Cloud.db	연결된 기기 정보
CamActivityHisory.db	카메라 관련 로그 정보
history.db	연결된 기기의 로그 정보
PersistentLogData.db	프로세스 관련 로그 정보

4. 시나리오를 통한 아티팩트 활용

본 장에서는 가상의 범죄 수사 시나리오를 제시하며 이를 바탕으로 스마트싱스 기기가 생성한 아티팩트 활용방안을 제시한다.

4.1 시나리오 설정

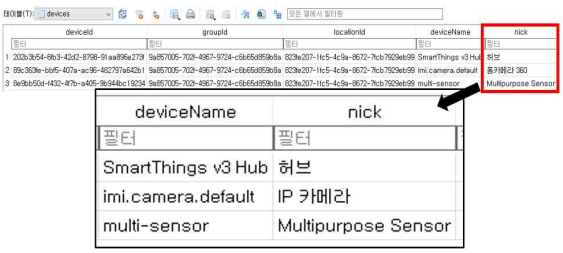
피해자는 고가의 미술품을 집에 보관하고 있으며, 보안의 목적으로 창문에는 다목적 센서가 장착되어 있으며 거실에는 홈 카메라를 설치하였다. 피해자는 약 10일간의 여행 후 집에 도착했을 때 미술품이 도난당한 사실을 발견하고 경찰에 도난 신고를 했고 외부 수사관이 도착하여 스마트 홈 기기를 분석하였다.

[표 3] Databases created in SmartThings

데이터 베이스	총 테이블 수	총 필드 수	내용
ATMEntityDatabase.db	7	63	연결된 기기 정보 및 생성되는 로그 값 정보
CamActivityHisory.db	3	13	카메라 관련 로그 정보
Catalog.Db.db	7	117	스마트싱스와 연결 가능한 기기 정보
Cloud.db	9	73	연결된 기기 정보
CommonData.db	8	42	연결한 사용자 정보
ControlsProvider.db	3	33	연결된 기기 아이콘 정보
DashboardDeviceData.db	3	17	사용자 대시보드에 표시된 정보
DashboardUi.db	7	40	연결된 기기 정보
DeviceCapbilityStatusData.db	5	30	연결된 기기의 마지막 로그 정보
DeviceData.db	3	30	허브 정보 및 연결된 기기 기능 정보
DeviceHealthData.db	3	6	연결된 기기 연결 상태 정보
DevicePresentationData.db	4	25	연결된 기기에서 생성될 수 있는 로그에 대한 정보
EasySetupContentsDb.db	9	57	스마트싱스 앱에서 사용하는 도움말 정보
FavoriteData.db	3	12	스마트싱스 앱 즐겨찾기 관련 정보
history.db	3	10	연결된 기기의 로그 정보
InternalSettings.db	3	7	사용자의 정보, 클라우스 서버 ip 정보, 클라우드 토큰 등 클라우드 관련 정보
LandingUi.db	12	153	각종 센서 로그 정보
NotificationDb.db	3	27	연결된 기기의 알림 정보
notifications.db	3	29	스마트싱스 기기 알림 정보
PersistentLogData.db	3	12	데이터베이스 업데이트 및 각종 이벤트 정보
PersistentServiceData.db	3	16	연결된 기기 관련 정보
SeviceData.db	11	107	스마트싱스 관련 기기 정보
SmartApps.db	4	15	스마트싱스와 연결 가능한 기기의 id 정보
SummaryData.db	4	7	온도 측정 관련 로그

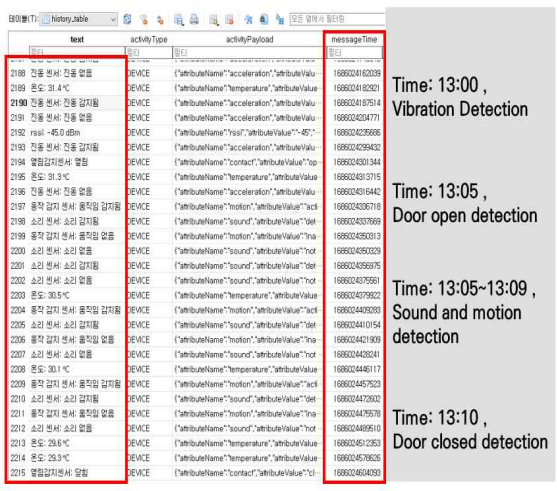
4.2 사고 조사

수사관은 우선 Cloud.db 파일을 열어 스마트싱스와 연결된 스마트 홈 기기를 [그림 4]와 같이 확인했다.



[그림 4] Cloud.db File Contents

기기를 확인 후 관련 로그를 분석하기 위해 스마트싱스 관리 앱을 접속하였지만 사고가 발생한 지 일주일이 지나 기록이 남지 않았다. 스마트싱스 내부 폴더에 존재하는 history.db 파일은 시간이 지나도 기록이 삭제되지 않음으로 history.db 파일을 분석하였다. 만약 history.db 파일이 손상되거나 삭제됐다면 카메라 관련 로그가 기록되는 CamActivityHistory.db 파일과 모든 프로세스가 저장되는 PersistentLogData.db를 이용해서 증거를 획득할 수 있다. [그림 5]는 history.db 파일을 타임스탬프와 로그를 종합해 분석한 내용이다.



[그림 5] history.db File Analysis

4.3 사고 재구성

분석 결과를 바탕으로 사고를 재구성할 수 있었다. 피해자가 집을 비운 이틀 뒤인 진동 탐지 로그를 통해 범죄자가 창문 잠금 장치 해제를 13시부터 시도했음을 확인하였다. 13시 5분에 문열림 센서 로그를 이용해 범죄자는 창문을 통해 집에 침입했으며 5~9분 사이에 동작 및 사운드 감지 로그를 통해 미술품을 훔쳤음을 추측하였다. 13시 10분에 문닫힘 센서 로그를 마지막으로 13시 5분부터 5분간 범죄자가 집에 침입했음을 확인하였다.

5. 결론

사물인터넷 발전으로 스마트 홈 기기의 사용량도 늘어났다. 스마트 홈 기기는 다양한 센서로 이루어졌기 때문에 범죄사고가 발생했을 시 주요 증거물로 활용될 수 있다. 하지만 스마트 홈 기기는 플랫폼 및 기기마다 로그가 저장되는 형태가 달라 이를 사전에 분석하고 연구할 필요가 있다. 본 논문은 스마트 홈 제품 중 스마트싱스 기기로 환경을 구축해 분석하고 수집 가능한 정보를 식별하였고 이를 표로 정리하였다. 또한, 범죄사고 조사에 효과적으로 활용할 수 있는 데이터베이스 파일을 제시하였다. 제시된 파일을 가상의 범죄 시나리오를 통해 타당성을 검증하였다. 향후 연구로는 다양한 플랫폼의 스마트 홈 기기 분석과 추가적인 로그에 대한 활용방안이 필요하다.

Acknowledgment

"이 논문은 2023년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구임"(IITP-2022-0-01203)

본 연구는 과학기술정보통신부 및 정보통신기획 평가원의 지역지능화혁신인재양성사업의 연구결과로 수행되었음 (IITP-2023-RS-2022-00156287).

참고문헌

[1] “FutureMarketInsights”, Smart Home Market Value & Industry Growth (2023-2032), https://www.futuremarketinsights.com/reports/smart-home-solutions-market

[2] “WIRED”, Meet the Star Witness: Your Smart Speaker, https://www.wired.com/story/star-witness-your-smart-speaker/

[3] 강수진, 신수민, 김소람, 김기윤, and 김종성, 샤오미 스마트홈 아티팩트 분석 및 활용방안 연구, 디지털포렌식연구 15(1), 54-66.

[4] 이진오, and 손태식, 스마트홈 가전 및 IoT 기기 포렌식을 통한 범죄 수사에 사용될 수 있는 아티팩트 획득, 디지털포렌식연구 16.2 (2022): 98-115.