스마트 홈 플랫폼 헤이홈에 대한 디지털 포렌식 아티팩트 분석

문상민*, 서승희**, 이창훈†

서울과학기술대학교 (*대학생, **대학원생, † 교수)

Digital Forensic Analysis for Smart-home Platform Hejhome

Sangmin Moon*, Seunghee Seo**, Changhoon Lee†

Seoul National University of Science and Technology

(*Undergraduate student, **Graduate student, † Professor)

요 약

스마트 홈은 IoT(Internet of Things) 기기들을 이용해 거주자에게 편의성을 제공하고 거주 공간 안에서 일어나는 상황을 파악할 수 있게 하는 기술이다. 특히 스마트 홈 기기들의 데이터 중에서 문의 개폐, 온도 및 습도, 움직임 등의 정보는 디지털 포렌식 수사 과정에서 수사관이 사건의 발생 시간 및 경과, 현장 상황 파악을 할 수 있도록 한다. 하지만 국내 스마트 홈 환경에 대한 디지털 포렌식 관점에서의 분석 연구는 아직 미흡하다. 따라서, 본 논문에서는 국내 스마트 홈 플랫폼인 헤이홈에서 환경을 직접 구축하여 실험을 수행한다. 또한, 스마트폰, 클라우드 데이터를 수집하고 디지털 포렌식 관점에서 유의미한 데이터를 분석한다. 분석의 결과로 헤이홈 애플리케이션에서 연결 기기와 접근 시간에 대한 아티팩트를 수집하고 헤이홈 API를 활용하여 문의 개폐, 온도 및 습도, 움직임 등의 아티팩트를 수집한 뒤 활용 방안을 제시한다.

I. 서론

스마트 홈 디바이스는 주변 환경 정보를 수집하고 이를 기반으로 다른 기기와 상호작용하거나 사용자 지정 명령을 수행한다.[1] 이러한 스마트 홈 기기들의 데이터는 사건의 발생 시간 및 경과, 현장 상황 파악을 할 수 있도록 하여 디지털 포렌식적 관점에서 그 의미가 크다. 실제로, 2015년 미국의 아칸소(Arkansas) 주에서 발생한 살인 사건에서 아마존 사의 스마트 스피커인 '아마존 에코'의 녹음 데이터와 IoT 온수기의 기록이 사건 현장 상황에 관한 증거로 제출된 바 있다.

스마트 홈 아티팩트는 OS의 종류와 IoT 기기의 분류별로 데이터 수집 방법, 아티팩트의 형태 및 내용이 다르기 때문에 폭 넓은 연구가 필요하다. 국외 스마트 홈 환경에 관한 연구[1][2][3]는 다수 진행되었으나 iOS 환경에서 국내 스마트 홈에 대한 연구는 미비하다.

이에 따라 본 논문에서는 국내에서 스마트 홈 서비스를 제공하고 있는 헤이홈 플랫폼을 대상으로 iOS 환경의 헤이홈 애플리케이션 파일 구조를 Checkra1n 탈옥을 통해 습득하고 분석한다. 해당 방식은 이스라엘 모바일 포렌식 업체인 셀레브라이트(Cellebrite) 사에서도 사용하는 방식으로 데이터의 변조 없이 데이터를 수집할 수 있다.[4] 또한, 스마트 홈 디바이스 유형별 수집 가능한 아티팩트를 분류하고 API를 통해 연결된 기기, 센서별 상태, 기록 모니터링 등의 정황 아티팩트를 조사한다.

본 논문은 2장에서 관련 연구에 대해 의의와 한계점을 서술하고, 3장에서 헤이홈 분석 환경에 대해 그림과 표로 나타낸다. 4장에서는 헤이홈 아티팩트 수집 및 분석 결과를 정리하고 5

† 교신저자: chlee@seoultech.ac.kr

이 논문은 2021년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구임 (No.2021-0-00540, GPU/ASIC 기반 암호알고리즘 고속화 설계 및 구현 기술개발)

장에서 결론으로 마무리한다.

II. 관련 연구

김소람[2] 등은 Samsung SmartThings와 Google NestHub, Kasa Cam으로 구성된 환경에서 안드로이드용 스마트 홈 애플리케이션에 대해 아티팩트를 분석하였고 Google web API로 기록된 데이터에 대한 아티팩트를 분류, 분석하였다. 해당 연구는 가장 많이 사용되는 스마트 홈 환경인 Samsung SmartThings에 대한 연구뿐만 아니라, Google의 스마트 스피커인 Nest Hub에 대한 아티팩트도 조사하였다는 점에서 의의가 크다. 정현지[3] 등은 Amazon Alexa ecosystem에 대해 iOS 환경과 안드로이드 환경, 또한 API에 대해서도 분석을 진행하였고 아티팩트를 수집, 분류하였다. 해당 연구는 해외에서 가장 많이 사용되고 있는 스마트 스피커인 Amazon Alexa를 다양한 환경에서 분석하고 아티팩트를 수집, 분류하였다는 점에서 의의가 크다. 뿐만 아니라, 모바일 애플리케이션과 웹 브라우저에서 아티팩트를 수집, 분류, 분석할 수 있는 CIFT(Cloud-based IoT Forensic Toolkit)라는 툴을 제안하였다.

기존의 논문들로부터 스마트 홈 환경에서 상당히 많은 아티팩트를 분류해낼 수 있다는 것을 알 수 있었다. 하지만, 주로 Amazon과 Google같이 해외의 스마트 홈 플랫폼을 분석하였고 데이터 수집 방식이 Android 백업, iTunes 백업과 같이 다양하지 못하다는 한계점이 있다. 본 논문에서는 앞선 논문들과 달리 iOS 환경에서 탈옥과 OpenSSH(Open Secure Shell), SFTP(Secure File Transfer Protocol)을 통해 모바일 애플리케이션 분석을 진행하였으며 OAuth 인증 과정에 필요한 accessToken 획득 방법과 API를 통해 아티팩트를 수집하는 방법을 제시하였다.

III. 헤이홈 아티팩트 분석 환경

헤이홈의 센서는 스마트 허브를 통해 통신하며 스마트 허브는 LAN선을 통해 연결된다. 스마트 허브와 각 센서들은 2.4Ghz의 대역폭을 갖는 Zigbee 프로토콜을 이용한다. 센서에서 감지한 정보들은 허브를 통해 클라우드로 데이터를 송수신하고 있음을 파악할 수 있다. 저장된 데이터 및 상태는 헤이홈 애플리케이션 또는 웹 인터페이스인 헤이홈 스퀘어에서 모니터링 및 조작을 할 수 있으며 이는 로그인이 필요하다. 헤이홈은 클라우드와 데이터 송수신을 위한 API를 제공하며 이는 OAuth 방식을 사용한다. OAuth 인증 과정은 로그인 시 JSessionID가 발급되고 인증 코드를 발급받는다. 인증 코드와 Redirect URI, Client ID를 헤더에 포함시키고 accessToken을 요청하면 accessToken이 발급된다. accessToken은 유효 기간이 180일이다.

3.1 헤이홈 분석 환경 구성

본 연구에서 구성한 헤이홈 아티팩트 분석 환경은 그림 1과 같다.

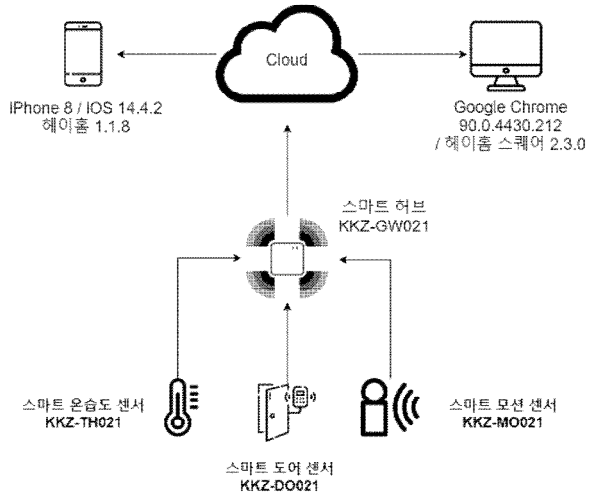

그림 1. 헤이홈 아티팩트 분석 환경

본 연구는 모두 센서를 이용하여 사건 현장을 파악하는 데 도움이 되는 정황 아티팩트를 수집하는 데에 집중한다. 스마트 도어 센서, 스마트 온습도 센서, 스마트 모션 센서 총 3가지 센서를 헤이홈 허브에 연동하고 센서에서 수집된 데이터는 클라우드로 전송되어 iPhone의 헤이홈 애플리케이션과 웹의 헤이홈 Square에서 확인할 수 있다. 스마트 도어 센서로부터 문의 열림, 닫힘 정보를 얻게 되고, 스마트 모션 센서로부터 탐지된 움직임 정보를 얻게 된다. 마

지막으로 스마트 온습도 센서로부터 온도와 습도 정보를 얻게 된다. 스마트 허브는 데이터들을 클라우드 DB로 전송하는 역할을 하고 저장된 상태 및 기록은 스마트폰의 헤이홈 애플리케이션과 PC의 웹 인터페이스를 통해 볼 수 있다. 표 1은 실험 기기를 모델 및 버전, 기능에 따라 정리한 표이다.

Device Name	Model or Version	Function
iPhone 8	iOS 14.4.2, 헤이홈 1.1.8	클라우드 DB에 저장된 스마트 홈 기기들의 상태 및 기록 확인 가능, 기기 제어 가능
스마트 허브	KKZ-GW021	센서가 감지한 데이터를 클라우드 DB로 전송
스마트 도어 센서	KKZ-DO021	문의 열림, 닫힘 감지
스마트 모션 센서	KKZ-MO021	움직임 탐지
스마트 온습도 센서	KKZ-TH021	온도, 습도 감지

표 1. 헤이홈 아티팩트 분석 기기 모델 및 버전

IV. 헤이홈 아티팩트 수집 및 분석 결과

4.1 헤이홈 애플리케이션 분석 결과

4.1.1 헤이홈 애플리케이션에서 아티팩트 수집

본 연구에서는 iOS 환경에서 Checkra1n 탈옥으로 진행하였다. 데이터 수집 방법은 탈옥 후 사용할 수 있는 OpenSSH와 SFTP를 이용하였다.

4.1.2 헤이홈 애플리케이션 아티팩트

iOS 환경의 헤이홈 애플리케이션과 서버와의 통신 관련 데이터는 Library/Caches/com.goqual/Cache.db에 저장된다. 또한, Documents/panel에는 표 2와 같이 연결된 허브와 센서의 기능이 json 형식으로 저장되어 있으며 __access_time__.json에는 그림 2와 같이 연결된 기기들에 대한 마지막 접근 시간이 유닉스 시간으로 기록된다.

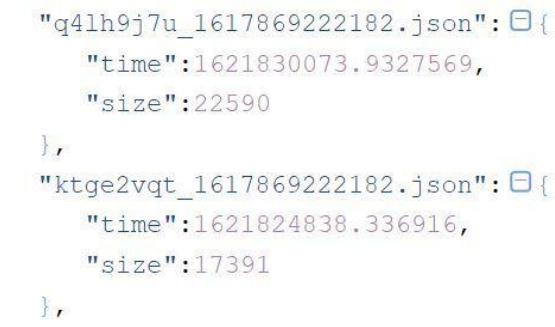

그림 2. __access_time__.json에 기록된 연결 센서의 마지막 접근 시간

Json File Name	Description
ktge2vqt_1617869222182.json	스마트 도어 센서에 대한 기능 정의
q4lh9j7u_1617869222182.json	스마트 온습도 센서에 대한 기능 정의
smmlguju_1620964881365.json	스마트 모션 센서에 대한 기능 정의
Yacg23r2ew8vosz_1617869222182.json	스마트 허브에 대한 기능 정의

표 2. 헤이홈에 연결된 센서와 관련한 아티팩트

4.2 헤이홈 스퀘어 분석 결과

4.2.1 헤이홈 스퀘어에서 토큰 수집 방법

헤이홈의 모회사인 고큐에서는 Goqual API를 제공하고 있으며 Hej home Square라는 Web Interface를 제공하고 있다. accessToken을 얻는 방법은 총 두 가지인데 ID와 PW를 알고 있다면 https://square.hej.so/square의 로그인을 통해 개발자 도구 네트워크 탭의 Request 헤더에서 accessToken을 얻을 수 있다. 만약 사용자가 Hej home square를 사용한 적이 있다면 해당 사이트의 쿠키에서 accessToken을 얻을 수 있다. 다음으로, accessToken의 주인이 아니더라도 로그인을 하게 되면 JSessionID가 생기는데 이 두 가지를 Request 헤더에 포함시키면 API를 이용할 수 있고 기기 목록 조회, 히스토리 조회 등을 볼 수 있다.

4.2.1 헤이홈 API 아티팩트 분석

표 3은 아티팩트로써 의미를 가지는 API와 그에 따른 Response 및 아티팩트 활용 방안을 나타낸다. 현재 모션 센서 히스토리에 대한

API는 헤이홈에서 제공하고 있지 않다.

API	Response	Description
https://goqual.io/openapi/devices	{ "id": "ebxx3t", "name": "도어 센서", "familyId": "xx07", "online": true }	사용자가 소유중인 기기 목록 확인 가능
https://goqual.io/openapi/history/temperature/line?device-id={{TH}}&date-type=month	{ "date": "2021-05-30T09:00:00.000", "value": 27 }	온도 및 습도가 현장 상황에 미친 영향 파악 가능
https://goqual.io/openapi/device/{{Door}}	{ "id":"ebxx3t", state":"CLOSED" }	도어 히스토리로 외부 침입여부 파악 가능

표 3. 헤이홈 API, Response 및 포렌식 관점에서의 아티팩트 활용 방안

그림 3은 실제 API 요청 헤더 및 응답을 나타낸 그림이다.

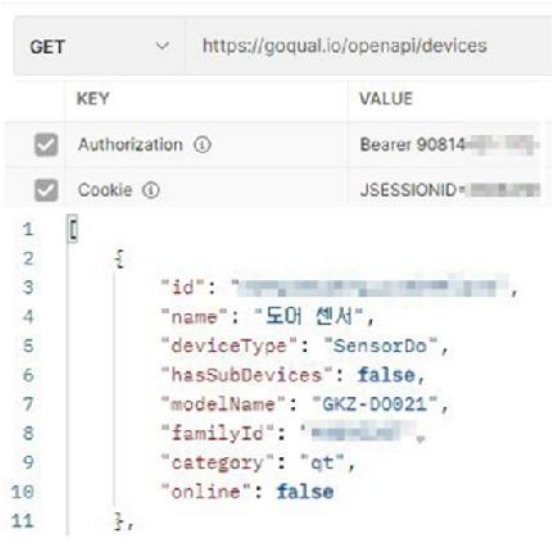

그림 3. 헤이홈 API 요청 헤더 및 응답

Ⅴ. 결론

본 논문에서는 국내 스마트 홈 플랫폼 헤이홈을 중심으로 iOS 환경에서 스마트 홈 애플리케이션 파일 구조를 분석하였다. 또한, 애플리케이션과 API를 이용하여 아티팩트를 분류하였고 및 활용 방안을 서술하였다. 본 논문의 결과로 국내에서 많이 연구되지 않은 스마트 홈 애플리케이션에서 연결 기기 및 접근 시간의 아티팩트를 수집하였고 aceessToken을 획득 후 API를 이용한 아티팩트 수집 방법을 제시하였다. 본 연구는 향후 센서와 더불어 조작 가능한 IoT 기기를 추가로 활용하여 더 많은 사용자 행위와 관련한 아티팩트를 수집 및 분석할 수 있을 것이다.

[참고문헌]

[1] 강수진, 신수민, 김소람, 김기윤, &김종성. (2021). 샤오미 스마트홈 아티팩트 분석 및 활용방안 연구. *디지털포렌식연구* , *15* (1), 54-66.

[2] Kim, S., Park, M., Lee, S., &Kim, J. (2020). Smart Home Forensics－Data Analysis of IoT Devices. *Electronics* , *9* (8), 1215.

[3] Chung, H., Park, J., &Lee, S. (2017). Digital forensic approaches for Amazon Alexa ecosystem. *Digital Investigation* , *22* , S15-S25.

[4] "Celebrite 사에서 제공하는 checkm8과 checkra1n에 대한 Webinar", https://www.cellebrite.com/en/checkm8-and-checkra1n-full-filesystem-extractions-for-ios-devices/ [Accessed 2021. 06.01.]

[5] 이경식. (2016). 맥 포렌식을 통한 아이폰 아티팩트 분석 기법. *정보보호학회지* , *26* (5), 17-21.

[6] 김기윤, 허욱, 이세훈, &김종성. (2019). 보안 메신저 SureSpot 애플리케이션에 대한 포렌식 분석. *디지털포렌식연구* , *13* (3), 175-188.

[7] 서승희, 남기훈, 김역, &이창훈. (2018). 국내 랜덤 챗 어플리케이션에서 사용자의 행위에 따른 아티팩트 분석. *디지털포렌식연구* , *12* (3), 1-7.