J. Internet Comput. Serv.
ISSN 1598-0170 (Print) / ISSN 2287-1136 (Online)
http://www.jics.or.kr

스마트 홈 헤이 홈 Air의 클라우드 아티팩트 원격 수집 방안 연구☆

A Study on the remote acuisition of HejHome Air Cloud artifacts

김 주 은[1] 서 승 희[1] 차 해 성[1] 김 역[2] 이 창 훈[1*]
Ju-eun Kim Seung-hee Seo Hae-seong Cha Yeok Kim Chang-hoon Lee

요 약

IoT(Internet of Things) 디바이스의 사용이 확대됨에 따라 경찰청의 디지털 포렌식 적용 범위가 스마트 홈 영역으로 확대되었다. 이에 따라 스마트 홈 플랫폼 데이터를 수집하기 위해 진행된 기존 연구들은 대부분 모바일 기기의 로컬 데이터 분석과 네트워크 관점의 분석 등의 연구가 주로 수행되었다. 하지만 증거 분석을 위해 유의미한 데이터는 스마트 홈 플랫폼의 클라우드 스토리지에 주로 저장되어있다. 따라서 본 논문에서는 사용자가 헤이 홈 앱 기반의 "헤이 홈 스퀘어" 서비스를 이용할 때 PC에 기록되는 Microsoft Edge, Google Chrome, Mozilia Firefox, Opera와 같은 웹 브라우저들의 쿠키 데이터베이스를 통해 사용자 계정의 accessToken을 획득하여 헤이 홈 Air 환경에서 클라우드에 저장된 데이터의 수집 방안을 연구했다. 데이터는 헤이 홈의 모회사가 제공하는 OpenAPI를 활용해 클라우드로 직접 접근하여 수집하였다. 본 논문에서는 스마트 온·습도 센서, 스마트 도어 센서, 스마트 모션 센서로 환경을 구성하여 실험를 수행했고 날짜 및 장소별 온·습도 데이터, 사용한 디바이스 리스트, 방 내 모션 감지 기록 등의 아티팩트를 수집할 수 있는 것을 확인하였다. 이와 같은 아티팩트 분석 결과를 통해 알 수 있는 사건 당시의 온·습도 등의 정보는 포렌식 수사 과정에서 단서로 활용될 수 있다. 또한 본 논문에서 제안한 OpenAPI를 활용한 클라우드 데이터 수집 방안은 데이터 수집 과정에서 발생할 수 있는 변조 가능성을 배제하고, API를 이용해 결과를 호출하기 때문에 디지털 포렌식의 원칙인 무결성의 원칙과 재현성의 원칙을 따른다.

☞ 주제어 : 스마트 홈, 디지털 포렌식, 인증 토큰 획득, Open API, 클라우드 포렌식

ABSTRACT

As the use of Internet of Things (IoT) devices has expanded, digital forensics coverage of the National Police Agency has expanded to smart home areas. Accordingly, most of the existing studies conducted to acquire smart home platform data were mainly conducted to analyze local data of mobile devices and analyze network perspectives. However, meaningful data for evidence analysis is mainly stored on cloud storage on smart home platforms. Therefore, in this paper, we study how to acquire stored in the cloud in a Hey Home Air environment by extracting accessToken of user accounts through a cookie database of browsers such as Microsoft Edge, Google Chrome, Mozilia Firefox, and Opera, which are recorded on a PC when users use the Hey Home app-based "Hey Home Square" service. In this paper, the it was configured with smart temperature and humidity sensors, smart door sensors, and smart motion sensors, and artifacts such as temperature and humidity data by date and place, device list used, and motion detection records were collected. Information such as temperature and humidity at the time of the incident can be seen from the results of the artifact analysis and can be used in the forensic investigation process. In addition, the cloud data acquisition method using OpenAPI proposed in this paper excludes the possibility of modulation during the data collection process and uses the API method, so it follows the principle of integrity and reproducibility, which are the principles of digital forensics.

☞ keyword : Smart home, Dgital forensics, AccessToken , Open API, Cloud forensics

1 Department of Computer Science and engineering, Seoul National University of Science and Technology, Seoul, 01811, Korea.
2 Institute of Electr ic and Infor mation Technology, Seoul National Univer sity of Science and Technology, Seoul, 01811, Korea.
* Corresponding author (chlee@seoultech.ac.kr)
[Received 13 July 2022, Reviewed 26 July 2022(R2 4 September 2022), Accepted 5 October 2022]

☆ This paper was funded by the government (Ministry of Science and ICT) in 2022 with the support of the Institute of Information & Communications. Technology Planning & Evaluation. (No.2019-0-00097, Development of Security Chip and Real-Time Control Protocol Security Technology for Smart Factory Network Infrastructure)
☆ 본 논문은 2022년도 한국인터넷정보학회 춘계학술대회 우수논문 추천에 따라 확장 및 수정된 논문임.

1. 서 론

경찰청은 작년, 디지털 포렌식 분석 건수가 2017년 34,541건에서 2020년 63,034건으로 약 2배 증가했고 2021년 상반기에만 50,161건을 기록하여 디지털 포렌식 역할 비중이 커지고 있는 상황임을 보여주었다.[1]

그 중 IoT 기술이 발달함에 따라 다양한 센서나 모듈, AI가 추가된 IoT 기기의 활용 영역이 확장되면서 생활에 밀접하게 관여하는 가전제품 및 가정설비에도 IoT 기능이 포함되는 경우가 많아져 최근 스마트 홈 데이터에 대한 디지털 포렌식 수사 관점에서의 관심이 높아지고 있다. 이러한 현 상황을 반영하여 최근 대검과 경찰청은 범죄 사건의 증거를 수집하기 위해 수사 범위를 스마트 홈 영역까지 확대하여 포렌식 기법 연구를 진행하고 있다.[2] 스마트 홈은 윈도우나 안드로이드 운영체제를 플랫폼으로 사용하는 PC나 모바일 기기와는 달리 장비 제조사에 따라 운영환경이 결정되기 때문에 각 운영환경에 적합한 아티팩트 수집 기법 연구가 요구된다. 따라서 스마트 홈 데이터의 아티팩트 분석 연구는 각 운영환경에 맞게 수집 및 분석이 요구된다.

스마트 홈 플랫폼에서는 기기와 센서들의 데이터를 대부분 클라우드로 전송하고 클라우드 스토리지에서 저장, 관리한다. 구글 홈과 아마존 Alexa와 관련된 연구 이외의 스마트 홈 아티팩트 수집 관점에서 진행된 연구들은 대부분 네트워크 패킷 데이터를 이용해 분석하는 네트워크 스니핑 기법과 웹 프록시 도구를 활용한 MITM(Man-in-the-middle)방식, 그리고 칩오프(chip-off)와 같이 센서 등의 기기에 남아 있는 데이터를 수집하여 분석한 연구들이다.[3]

하지만 이러한 기존 IoT 데이터 수집은 클라우드에 직접 접근하는 것이 아니라 네트워크나 센서 장비의 메모리에서 추출하는 것이기 때문에 온전한 데이터를 확인할 수 없다는 한계가 존재한다. 또한 디지털 포렌식 수사 관점에서 IoT 기기와 데이터는 이미징이나 압수에 적절하지 않은 상황이 발생할 수 있고, 비정형성을 갖고 있기 때문에 수사에 필요한 데이터 선별이 쉽지 않다.

헤이 홈의 모회사인 ㈜고퀄은 헤이 홈 서비스를 다른 클라이언트들에게 자사의 서비스를 편리하게 활용할 수 있도록 공개적으로 OpenAPI를 제공하고 있다.[4] 본 논문에서는 이 OpenAPI를 이용함으로써 클라우드로 직접 접근이 가능하도록 하고 이에 따라 비정형적인 데이터가 아닌 온전한 데이터를 획득할 수 있는 방안을 연구한다. 또한 ㈜고퀄 OpenAPI에서 이용되는 OAuth 2.0 프로토콜의 사용자 인증 토큰인 accessToken을 추출하여 피압수자의 계정 정보 없이 클라우드의 데이터를 수집함으로써 디지털 포렌식 관점에서 유의미한 아티팩트를 수집하는 방안을 제시한다.

2. 관련 연구

스마트 홈의 아티팩트 분석 및 수집 연구는 다양한 플랫폼에서 진행되고 있다. 그 중 SJ Kang 외 4명[5]은 샤오미 스마트 홈 플랫폼에 대해 모바일 기기의 로컬 데이터 분석 관점에서 연구를 수행하였다. 모바일 기기의 내·외부 저장소에서 Mi home 앱의 로그 파일을 분석하여 아티팩트를 수집한 결과를 보였다. 또한 MJ Kim 외 1명[6]은 네트워크 패킷 분석 관점으로 스마트 TV, 스마트 카메라를 이용해 스마트 홈 환경을 구성하여 아티팩트 수집 연구를 수행하였다. 네트워크 스니핑과 웹 프록시 도구를 이용한 MITM 기법으로 데이터를 분석한 결과를 보였다. 이러한 연구 결과들은 클라우드에 직접 접근하여 획득한 데이터가 아니기에 유의미한 아티팩트의 수집에는 한계가 있다.

SR Kim 외 3명[7]은 스마트 홈과 스마트 카메라 기기로 구성된 실험환경에서 주로 모바일 기기의 데이터 분석 연구를 수행하였지만, 구글 홈 플랫폼 데이터 수집에서 구글 홈의 프라이빗 APIs를 이용해 IoT 기기의 ip 정보를 주입하여 클라우드에 저장된 기기의 연결 정보 등을 얻을 수 있음 또한 보였다. 그리고, YJ Chung 외 2명[8]은 아마존의 스마트 스피커인 Amazon Alexa 환경에서 API 사용을 통한 데이터 수집 관점으로 연구를 수행하였다. 웹 브라우저의 캐시를 통해 사용자 인증 토큰을 획득하였고, 비공식적인 API를 이용해 클라우드에 저장된 사용자의 행위 데이터를 수집함을 보였다. 이와 같이 API를 이용해 클라우드 아티팩트 수집을 수행한 연구는 그 결과가 유의미한 것을 입증하였다.

㈜고퀄 OpenAPI에서 지원하는 OAuth 2.0 프로토콜은 리소스를 가진 소유자를 대신해 리소스 소유자와 HTTP 서비스 간의 접속을 허용함으로써 서드파티 응용프로그램이 접근 권한을 취득할 수 있도록 하는 프로토콜이다. 접근 권한을 원하는 서드파티 응용프로그램의 클라이언트와 리소스 소유자, 인증 서버가 상호 작용하며 처리하는 프로세스로, 이 프로세스에서 인증 서버는 클라이언트에게 accessToken을 부여한다. 클라이언트는 해당 토큰으로 리소스 서버에서 인증을 받고 서비스 이용 권한을 인가받게 된다. 이를 활용한 연구로, GH Nam 외 3명[9]은

모바일 기기에서 OAuth 2.0 프로토콜의 인증 토큰 데이터를 수집한 뒤, 로그인 우회 방식으로 Naver, Google, Tencent QQ와 같은 서드파티 프로그램들의 사용자 아티팩트를 수집하는 방안을 제시한 연구가 있다.

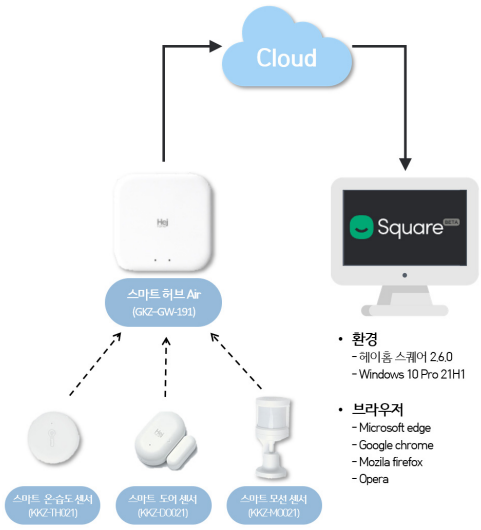
본 논문과 관련된 기존 연구인 SM Moon 외 2명[10]은 스마트 홈 헤이 홈 플랫폼에서 API를 이용한 아티팩트 분석 관점으로 연구를 수행하였으며, 센서에 따른 결과를 보였다. 하지만 웹 브라우저에 직접 접속하여 사용자 인증 토큰 정보를 수집하는 기법은 웹 브라우저 기록에 대한 무결성이 보존되기 어렵다는 한계가 존재했다. 본 논문에서는 토큰 정보 추출 과정에서 무결성을 보장할 수 있는 새로운 방안과 복호화 방법을 제안했다. 또한, 신형 헤이 홈 허브를 사용하며 더 많은 종류의 웹 브라우저에서 실험을 진행한 결과를 제시했다.

3. 분석 대상 및 환경

헤이 홈 스퀘어 서비스는 헤이 홈 스마트 홈 플랫폼의 클라우드 서버를 기반으로 사용자가 설정한 장소, 연결된 기기 리스트, 데이터의 대시보드 등의 정보를 제공하는 서비스이다. 그림 1과 같이 온·습도 센서, 도어 센서, 모션 센서를 각각 구성하고 이를 연결해주는 스마트 허브 Air를 통해 입력받은 데이터는 클라우드 스토리지로 저장된다. 헤이 홈의 웹이나 앱으로 서비스를 이용할 때 클라우드 서버로부터 입력된 데이터 이용이 가능하다. 실험에 사용한 헤이 홈 서비스 제공기기는 표 1과 같다. 처음 사용자의 계정을 생성하고 허브에 연결하는 것은 헤이 홈 앱을 통해 가능하다. 헤이 홈 서비스에서 제공하는 헤이 홈 스퀘어 서비스는 Microsoft Edge, Google Chrome, Mozila Firefox, Opera 총 4가지 웹 브라우저에서 사용하였다. ㈜고퀄의 OpenAPI를 이용해 결과를 가져오는 과정은 웹상에서 API 테스트 기능 서비스를 제공하는 Postman을 활용하였다.

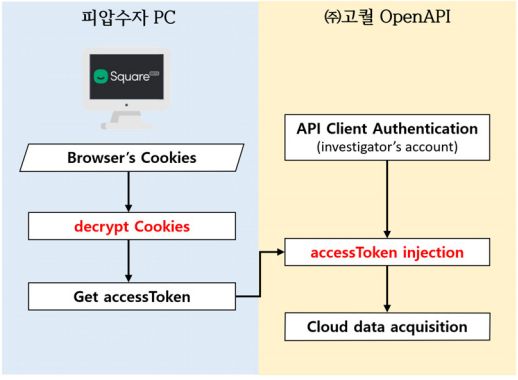
(표 1) 실험에 사용된 분석 대상 장비
(Table 1) Analysis target equipment used in the experiment

기기명	상세 정보
스마트 허브 Air (GKZ - GW-191)	Zigbee 무선 통신 방식의 제품들과 통신하기 위한 스마트 허브
스마트 온·습도 센서 (KKZ - TH021)	실시간으로 온도 및 습도를 측정하는 센서 장치
스마트 도어 센서 (KKZ - DO021)	문에 설치하여 열림/닫힘에 대한 데이터를 기록하는 센서 장치
스마트 모션 센서 (KKZ - MO021)	움직임을 감지하는 센서 장치



(그림 1) 헤이 홈 Air 분석 환경 구성
(Figure 1) Hej Home Air Analysis Environment Configuration

4. 헤이 홈 Air 클라우드 아티팩트 수집 방법



(그림 2) 헤이 홈 Air환경 클라우드 아티팩트 수집 흐름도
(Figure 2) Artifact Acquisition based on Hej Home Air Flow Chart

피압수자가 자신의 PC에서 웹 브라우저를 사용했다면, 로컬 경로에서 사용한 웹 브라우저의 쿠키 데이터베이스 파일을 얻을 수 있다. 본 논문에서는 피압수자가 웹 브라우저를 통해 헤이 홈 스퀘어 서비스를 사용했다고 가정했을 때, 암호화된 데이터가 포함된 쿠키 데이터베이스 파일을 복호화하여 헤이 홈 서비스의 계정인증을 위

한 access Token을 얻는 방안을 연구했다. 헤이 홈 서비스의 인증을 위한 accessToken의 정보는 square.hej.so를 host_key로 가진다.

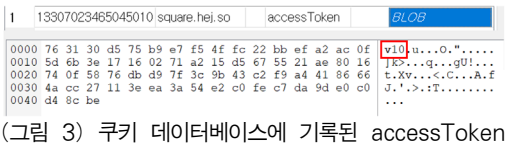
또한, ㈜고퀄의 OpenAPI는 클라이언트가 ㈜고퀄에 요청하여 Client_id와 Client Secret을 발급받은 후, 클라이언트 인증이 완료되면 이용할 수 있다. 이에 따라 ㈜고퀄의 OpenAPI에서 사용자의 accessToken을 통해 클라우드 데이터를 획득할 수 있다는 것을 이용했다. 본 논문에서는 피압수자의 클라우드 아티팩트 수집을 위해 디지털 포렌식 수사관의 관점에서 클라이언트 계정을 발급받은 후, 피압수자 PC의 쿠키 데이터베이스에서 얻은 암호화된 accessToken의 값을 복호화한 후 클라우드 아티팩트를 얻을 수 있는 방안을 제시했다.

먼저 피압수자의 PC에서 헤이 홈 서비스 인증을 위한 accessToken을 추출하는 과정이 필요하다. 웹 브라우저를 통해 헤이 홈 스퀘어의 서비스 이용 행위를 한 뒤에 쿠키 데이터베이스 파일을 확인한다. 웹 브라우저별로 쿠키 저장 경로나 방식이 각각 다르기 때문에 Microsoft Edge, Google Chrome, Mozila Firefox, Opera 총 4가지 웹 브라우저에서 실험을 진행했다. 피압수자의 계정 정보 없이 클라우드에 접근하기 위해 디지털 포렌식 수사관의 아이디로 로그인하여 기본 권한을 먼저 얻는다, 그 다음 API의 header로 피압수자 계정의 accessToken을 주입하여 해당하는 사용자의 헤이 홈 클라우드 데이터를 얻는다.

4.1 accessToken 수집 및 복호화

4.1.1 accessToken 수집 및 복호화 방안

사용자가 웹 브라우저를 사용했다면 그 흔적은 로컬에 쿠키 데이터베이스로 남게 된다. 웹 브라우저의 쿠키 데이터베이스 파일은 웹 브라우저 창이 종료되거나 컴퓨터가 재부팅되어도 여전히 남아있다. 하지만 웹 브라우저별 쿠키 데이터는 모두 일정 기간의 자동 삭제 시점이 지나면 찾을 수 없다는 한계가 있다.



(그림 3) 쿠키 데이터베이스에 기록된 accessToken 데이터의 헤더

(Figure 3) Header of accessToken data recorded in cookie database

PC의 웹 브라우저를 통해 헤이 홈 스퀘어에 로그인할 때 사용자의 accessToken 정보가 로컬 경로의 쿠키 데이터베이스에 기록된다. 각 웹 브라우저별 해당 경로는 표 2와 같다. 웹 브라우저 중 Mozila Firefox를 제외한 Microsoft Edge, Google Chrome, Opera의 쿠키 데이터베이스에 accessToken이 기록됨을 알 수 있었다.

(표 2) 브라우저별 쿠키 파일의 accessToken 경로

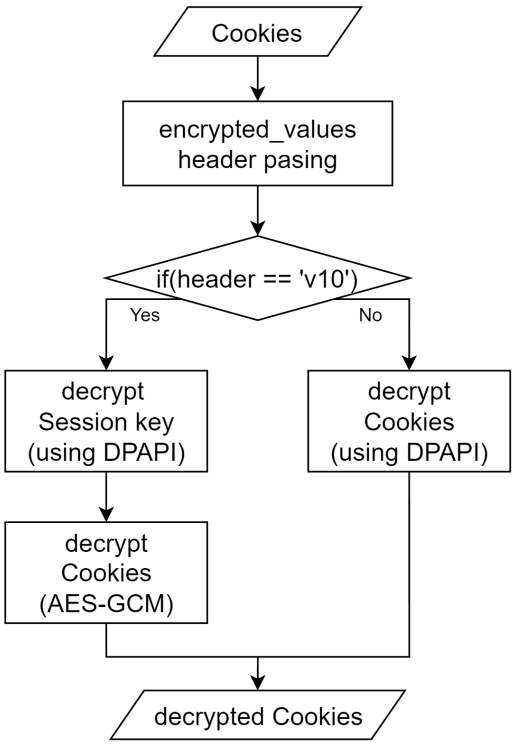
(Table 2) Path to AccessToken in each browser's Cookie file

브라우저	경로	host_key	칼럼명	암호화
Microsoft Edge (103.0.1264.49)	C:\Users\{username}\AppData\Local\Microsoft\Edge\User Data\Default\Network\Cookies	square.hej.so	access Token	O
Google Chrome (103.0.5060.114)	C:\Users\{username}\AppData\Local\Google\Chrome\User Data\Default\Network	square.hej.so	access Token	O
Opera (87.0.4390.36ver)	C:\Users\{username}\AppData\Roaming\Opera Software\Opera Stable\Network\Cookies	square.hej.so	access Token	O
Mozila Firefox (102.0.1ver)	C:\Users\{username}\AppData\Roaming\Mozilla\Firefox\Profiles\6dcs6jks.default-release\Cookies.sqlite	X	X	X

하지만 쿠키 데이터베이스의 파일 경로를 찾더라도 실험 대상인 웹 브라우저 중 쿠키에 존재하는 acessToken값은 그림 3와 같이 BLOB(Binary Large OBject) 형태로 암호화되어 존재하기 때문에 실제 값을 바로 확인하기 어렵다.

그림 3과 같이 위 세 개의 웹 브라우저에서 기록된 쿠키 데이터베이스의 BLOB 데이터에는 'v10' 헤더를 포함

한다. 윈도우 환경에서는 저장된 쿠키 데이터의 복호화 방법이 그림 4와 같이 쿠키 데이터의 처음 3바이트 값이 'v10'인지 여부에 따라 나뉜다.



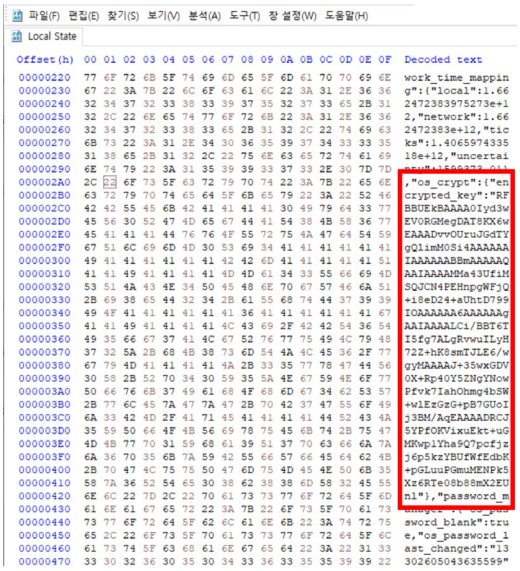
(그림 4) 쿠키 데이터 복호화 흐름도

(Figure 4) Decrypt Cookie Data Flow Chart

4.1.2 암호 알고리즘을 이용한 복호화

윈도우 환경에서 제공되는 DPAPI(Data Protection Application Programming Interface)는 Windows 2000 이상부터 지원되며 데이터 보호 관련 API로 암복호화에 필요한 기능을 제공하는 인터페이스이다. 'v10' 헤더를 가진 쿠키 데이터는 쿠키 데이터를 암호화할 때 DPAPI를 이용해 생성된 세션 키를 가져와 복호화하여 키를 유도한 후, 유도한 키를 이용해 AES256 GCM모드로 쿠키 데이터를 복호화할 수 있다. 쿠키 데이터 암호화 시에 사용된 세션 키는 그림 5와 같이 'Local State' 파일에 암호화되어 저장되고, 저장되는 경로는 각 웹 브라우저별로 표 3와 같다. 세션 키는 'Local State' 파일 내에서 ["os_crypt"] ["encrypted_key"] 키워드를 통해 확인할 수 있다.

획득한 세션 키 복호화를 위해 사용하는 DPAPI는 암호 알고리즘에 대한 사용이 미숙한 사용자들을 위해 윈도우에서 제공하는 기능으로, 암호화와 복호화를 위한 CryptprotectData()와 CryptUnprotectData() 두 가지 함수를 포함하여 5개의 사용자 인터페이스 함수를 제공하고 있다.



(그림 5) 쿠키 데이터 암호화 시 사용된 세션 키

(Figure 5) Header of accessToken data recorded in cookie database

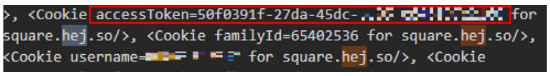
(표 3) 브라우저별 세션 키의 저장 경로

(Table 3) Path to Session Key in each browsers

브라우저	세션 키 저장 경로
Microsoft Edge (103.0.1264.49)	C:\Users\{username}\AppData\Local\Microsoft\Edge\User Data\Local State
Google Chrome (103.0.5060.114)	C:\Users\{username}\AppData\Local\Google\Chrome\User Data\Local State
Opera (87.0.4390.36)	C:\Users\{username}\AppData\Roaming\Opera Software\Opera Stable\Local State

그림 5의 세션 키는 wincrypt.h의 CryptGenKey() 함수를 통해 생성된 값이다. dpapi.h에서 CryptprotectData() 함수를 호출하여 암호화하고, Base64로 인코딩되어 지정된 로컬 경로에 저장된다.[11] 이에 따라, 지정된 경로에서 확인된 세션 키를 Base64로 디코딩 한 후, CryptUnprotectData() 함

수를 이용하면 accessToken 값의 복호화에 사용되는 세션 키를 해독할 수 있다. 한편, DPAPI를 이용해 데이터를 해독하려면 암호화한 사용자와 동일한 로그온 자격 증명을 가진 사용자여야 한다는 조건이 있다.[12] 따라서 쿠키 데이터베이스 파일을 이용해 쿠키 데이터를 복호화하는 과정은 모두 피압수자의 PC에서 진행되어야 한다. 복호화한 세션 키를 이용해 BLOB 데이터를 블록 암호 GCM 모드로 AES-256 알고리즘을 수행하여 복호화하면 그림 3과 같이 쿠키 데이터 내부의 accessToken을 얻을 수 있다.



(그림 6) Cookies 복호화 결과
(Figure 6) Cookies Decryption Results

4.1.3 DPAPI를 이용한 복호화

웹 브라우저의 쿠키 데이터베이스 파일 내에 암호화된 BLOB 데이터의 헤더가 'v10'이 아닌 경우에는 세션 키를 구하는 과정을 생략하고 암호 해독 인터페이스 함수인 CryptUnprotectData()에 BLOB 데이터의 원본을 파라미터로 하여 호출한다. DPAPI를 사용하기 위해 4.1.2 암호알고리즘을 이용한 복호화 방법과 마찬가지로 암호화한 사용자와 동일한 로그온 자격 증명을 가진 사용자만 해독 가능하다는 조건이 존재한다.

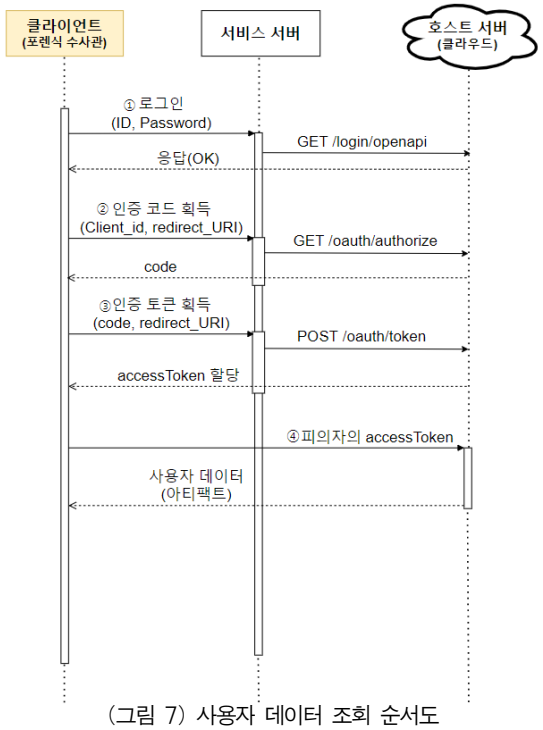
4.2 사용자 데이터 조회 및 수집

피압수자 PC에서 클라우드 접근을 위한 accessToken을 수집한 뒤, 획득한 accessToken를 이용해서 헤이 홈 클라우드의 사용자 아티팩트 수집을 위해서는 그림 7와 같이 ㈜고퀄의 OpenAPI를 이용해서 별도의 Oauth 인증과정이 필요하다.

㈜고퀄의 OpenAPI를 사용하기 위해서 디지털 포렌식 수사관 계정의 ① ID, Password 로그인을 통해 인증 서버로부터 Basic Auth를 완료한다. 그 후 응답을 받았다면 ② 인증 코드 획득을 위해 Client_id와 redirect_URI 값의 전송이 필요하다. Client_id는 ㈜고퀄에 OpenAPI 클라이언트 등록 시 ㈜고퀄로부터 응답받은 값이고, redirect_URI는 클라이언트 등록 시 직접 설정한 값으로 헤더를 통해 인증 서버에 전송한다. 이를 통해 결과 페이지의 헤더에서 발급된 인증코드를 얻을 수 있다. 이 후 accessToken을 발급받기 위해 ③ 인증 토큰 획득 과정을 수행한다. 획득한 인증 코드와 redirect_URI를 다시 헤더로 전송하여 디지털 포렌식 수사관 계정의 accessToken을 발급받는다. 3단계의 과정으로 ㈜고퀄의 OpenAPI를 사용할 수 있게 된다. ④의 과정부터 추출한 피의자의 accessToken을 이용해 ㈜고퀄이 제공하는 API를 사용하면, 헤이 홈 클라우드 서버에 접근하여 토큰과 매칭되는 피압수자의 클라우드 데이터를 얻을 수 있다. 이때, accessToken은 'Bearer {{accessToken}}' 형태로 주입하여 원하는 데이터에 대한 요청을 보낸다.

(표 4) ㈜고퀄의 OpenAPI에서 사용된 API 주소
(Table 4) API url in Corp. Goqual's open API used in the experiment

설명	API 주소
로그인	https://goqual.io/oauth/login?vendor=OpenAPI
인증 코드 획득	https://goqual.io/oauth/authorize/?response_type=code&client_id={{CLIENT_ID}}&scope=OpenAPI&reirect_uri={{REDIRECT_URI}}
인증 토큰 획득	https://goqual.io/oauth/token?grant_type=authorization_code&code={{CODE}}&redirect_uri={{REDIRECT_URI}}
devices 목록 상태 조회	https://goqual.io/OpenAPI/devices/state
장소 목록 조회	https://goqual.io/openapi/homes
방 목록 조회	https://goqual.io/openapi/homes/{{homeId}}/rooms
온·습도 조회	https://goqual.io/openapi/device/{{TH_id}}
습도 히스토리 조회	https://goqual.io/openapi/history/humidity/line?device-id={{TH_id}}&date-type=month
온도 히스토리 조회	https://goqual.io/openapi/history/temperature/line?device-id={{TH_id}}&date-type=month
도어센서 조회	https://goqual.io/openapi/device/{{Door_id}}
모션센서 조회	https://goqual.io/openapi/device/{{mo_id}}



(그림 7) 사용자 데이터 조회 순서도
(Figure 7) User data inquiry sequence

실험에 사용된 센서에 대해 ㈜고퀄이 제공하는 OpenAPI의 상세 주소는 표 4와 같다.

5. 헤이 홈 Air 클라우드 아티팩트 수집 결과

㈜고퀄 OpenAPI의 기능은 크게 장소/방의 조회, 기기 조회, 제어 등이 있다. 헤이 홈 zigbee 통신을 기반으로 한 온·습도 센서, 모션 센서, 도어 센서를 허브에 연결하여 사용했을 때 얻을 수 있는 아티팩트는 표 5를 통해 데이터의 종류와 출력 형태를 정리하였다. 범죄 사건과 관련하여 피압수자가 기기의 위치를 저장해놓은 장소 정보, 날짜와 시간이 기록된 히스토리 정보는 증거로써 중요한 아티팩트이다. 또한, 헤이 홈에서 클라우드 아티팩트를 얻을 수 있는 헤이 홈 제품은 실험에 사용한 기기 이외에도 누수 감지, 연기 감지, 도어락 등 대략 45개가 더 존재하므로 헤이 홈 단독 플랫폼으로 스마트 홈을 구성한 피압수자에 대하여 논문의 실험을 적용한다면 의미있는 아티팩트를 수집할 수 있을 것으로 보인다.

기존의 IoT 환경에서의 아티팩트 수집·분석 연구에서

(표 5) 헤이 홈 Air 클라우드 아티팩트 수집 결과
(Table 5) Hey Home Air Cloud Artifacts Collection Results

데이터 종류	형태
device state list	"id": "[디바이스 식별 번호]", "deviceType": "[센서명(문자열)]", "deviceState": { "state": "[센서 상태(문자열)]", "battery": 배터리 상태 }...
home list	"result": [{ "name": "[장소명(문자열)]", "homeId": [장소 식별 번호] }...]

room list	{
	"home": "[장소명(문자열)]",
	"rooms": [방이름(문자열),
	...
	]
	}

TH sensor (온습도)	"id": "[디바이스 식별 번호]",
	"deviceType": "[센서명(문자열)]",
	"deviceState": {
	"temperature": [온도],
	"humidity": [습도]
	}

humidity history	"result": [{ "date": "[기록일자(YYYY-MM-DD hh:mm:ss.sss)]", "value": [습도] }..].
temperature history	"result": [{ "date": "[기록일자(YYYY-MM-DD hh:mm:ss.sss)]", "value": [온도] }...]

DO sensor(문)	"id": "[디바이스 식별 번호]",
	"deviceType": "[센서명(문자열)]"
	"deviceState": {
	"state": "[디바이스 상태(문자열)]"
	}

MO sensor(모션)	"id": "[디바이스 식별 번호]",
	"deviceType": "[센서명(문자열)]"
	"deviceState": {
	"battery": [배터리 잔량],
	"state": [디바이스 상태(문자열)]
	}

는 주로 펌웨어 레벨의 파일 시스템 로그 분석 또는 네트워크 분석 등의 기법을 사용하였다. 이러한 기법으로 데이터를 수집할 때 접속 시간과 같은 데이터가 손상될 수 있다. 그러나 본 논문에서는 헤이 홈 플랫폼 자체에서 제공하는 공개 API를 통해 클라우드에 접근하여 아티팩트를 수집·분석한다. 이에 따라 디지털 포렌식 수사관에 의해 데이터가 손상될 가능성이 적고, 수집된 데이터 또한 API 요청에 의한 결과로 항상 같은 값을 유지한다.

6. 결 론

IoT 디바이스의 대중화가 가속화 되면서 클라우드 스토리지에 저장된 아티팩트 분석의 중요성이 증가함에 따라, 본 연구에선 로컬 PC에 기록된 웹 브라우저의 쿠키 데이터베이스를 통해 사용자의 accessToken을 획득하여 Microsoft의 DPAPI를 이용한 복호화 과정을 보였다. 또한 accessToken을 추출한 이후 ㈜고퀄의 OpenAPI를 이용해 먼저 로그인과 OAuth2.0 인증과정을 수행하고, 데이터 요청 시 추출한 accessToken을 헤더에 주입한 뒤, 응답을 통한 클라우드 데이터를 분석하여 아티팩트 목록을 정리하였다.

본 논문에서 고려해야할 점은 쿠키 데이터베이스의 저장 기간이 브라우저별 혹은 사용자가 설정한 기준별로 다를 수 있다는 점이 있다. 그리고 ㈜고퀄 OpenAPI에서 동작하는 accessToken의 유효기간이 180일로 지정되어 있어, accessToken이 쿠키에 남아있더라도 유효기간 만료로 인해서 다시 로그인해야 하는 상황이 발생할 가능성이 있다. 또한, accessToken이 쿠키로 저장되지 않거나 헤이 홈에서 자체적인 알고리즘으로 인코딩되어 저장되는 경우 제약이 발생할 수 있다. 마지막으로 본문에서 언급한 것과 같이 윈도우에서 동작하는 DPAPI는 복호화 동작 시에 사용되는 세션 키가 암호화할 때 로컬에 저장되었기 때문에, 암호화 시에 동작했던 피의자 본인의 PC 환경에서만 복호화가 가능한 점이 존재한다.

본 논문에서 제안한 기법을 이용해 OpenAPI를 제공하는 다른 스마트 홈 플랫폼에서도 토큰을 이용한 아티팩트 수집·분석 기법을 활용할 수 있을 것이다. 향후 연구에서는 웹 서비스에만 한정되는 것이 아니라 많이 사용되는 모바일 앱 서비스를 통해 모바일 기기에서 accessToken과 같은 크리덴셜 데이터를 획득하는 방안을 연구하고자 한다.

본 논문에서 제안한 OpenAPI를 활용한 클라우드 데이터 수집 방안은 기존 연구와 같이 모바일 기기나 IoT 디바이스, 혹은 네트워크 관점에서 데이터를 수집할 시 발생할 수 있는 접속 기록 갱신 등의 데이터 변조 위험성이 적다는 장점이 있고, API 요청을 통해 클라우드 데이터를 수집하기 때문에 수집 시점이 다르더라도 같은 데이터 결과를 가진다는 장점이 있다. 이에 따라 본 논문에서 제안된 클라우드 아티팩트 수집 기법은 디지털 포렌식의 원칙인 무결성의 원칙과 재현성의 원칙을 보장한다. 또한, 도출된 아티팩트 분석 결과는 포렌식 수사 과정에서 사건 발생 당시 현장의 온·습도 등의 단서를 파악하는데 활용될 수 있다.

참고문헌(Reference)

[1] SH Kim, “Last year, the number of digital forensic analyses doubled in three years”, ITBizNews, 2021.10.10., access 2022.07.09. https://www.itbiznews.com/news/articleView.html?idxno=51592

[2] YC Jung, “Smart home data to secure criminal cues.. Supreme Prosecutors’ Office Launches Research on Forensic Techniques”, etnews, 2022.03.17., access 2022.07.09. https://www.etnews.com/20220317000157

[3] MJ Kim, TS Shon, “Smart Home IoT Forensics Technology Trends”, REVIEW OF KIISC, Vol. 31, No. 6, pp. 31-35, 2021.

[4] Corp.Goqual, ″Hej home OpenAPI Guide-API List“, goqual.notion.site, 2022.08.26., access 2022.09.07. https://goqual.notion.site/OpenAPI-Guide-1177102881b345c3aa001d15d1788601

[5] SJ Kang, SM Shin, SR Kim, GY Kim, JS Kim, “Artifacts Analysis of Xiaomi Smart Home and Utilization Method for Digital Forensics”. Journal of Digital Forensics, Vol. 15, No. 1, pp. 54-66, 2021.

[6] MJ Kim, TS Shon, ″Research on Network-based Smart Home Device Forensic Technology″, Journal of Digital Forensics, Vol. 15, No. 4, pp. 84-94, 2021.

[7] SR Kim, MS Park, SH Kim, JS Kim, “Smart Home Forensics－Data Analysis of IoT Devices”, Electronics, vol. 9, No. 8, pp.1215-1228, 2020. https://doi.org/10.3390/electronics9081215

[8] YJ Chung, JH Park, SJ Lee, “Digital forensic approaches for Amazon Alexa ecosystem”, Digital Investigation, Vol. 22, Supplement, pp. S15-S25, 2017.

https://doi.org/10.1016/j.diin.2017.06.010

[9] GH Nam, SH Gong, BJ Seok, CH Lee, "Study onRemote Data Acquisition Methods Using OAuth Protocol of Android Operating System", Journal of the Korea Institute of Information Security & Cryptology, Vol. 28, No. 1, pp. 111-122, 2018. https://doi.org/10.13089/JKIISC.2018.28.1.111

[10] SM Moon, SH Seo, CH Lee, "Digital Forensic Analysis for Smart-home Platform Hejhome", Summer Conference of Korea Institute of information Security & Cryptology, 2021.

[11] Microsoft Docs, "dpapi.h header", Microsoft technical documentation, 2022.08.03., access 2022.09.07. https://docs.microsoft.com/en-us/windows/win32/api/dpapi/

[12] Microsoft Docs, "CryptGenKey function (wincrypt.h)", Microsoft technical documentation, 2021.10.13., access 2022.09.07. https://docs.microsoft.com/en-us/windows/win32/api/wincrypt/nf-wincrypt-cryptgenkey

◐ 저 자 소 개 ◑

김 주 은(Ju-eun Kim)
2022년 동의대학교 컴퓨터공학과(공학사)
2022년~현재 서울과학기술대학교 대학원 컴퓨터공학과(석사과정)
관심분야 : 디지털 포렌식, 랜섬웨어, etc.
E-mail : jek0104@seoultech.ac.kr

서 승 희(Seung-hee Seo)
2017년 서울과학기술대학교 컴퓨터공학(공학사)
2019년 서울과학기술대학교 컴퓨터공학(공학석사)
2020년~현재 서울과학기술대학교 대학원 컴퓨터공학과(박사과정)
관심분야 : 모바일 포렌식, 메모리 포렌식, 디지털 포렌식, etc.
E-mail : sh.seo@seoultech.ac.kr

◐ 저 자 소 개 ◑

차 해 성(Hae-seong Cha)
2022년 서울과학기술대학교 컴퓨터공학과(공학사)
2022년~현재 서울과학기술대학교 대학원 컴퓨터공학과(석사과정)
관심분야 : CTI, 인공지능, 악성코드, etc.
E-mail : haeseongcha@seoultech.ac.kr

김 역(Yeog Kim)
1992년 성신여자대학교 전산학과(이학사)
2003년 고려대학교 정보보호대학원(공학석사)
2010년 고려대학교 정보경영전문대학원(공학박사)
2005년~2007년 동양미래대학교 전임강사
2017년~현재 서울과학기술대학교 전기정보기술연구소 일반 연구원(책임급)
관심분야 : 정보보호(Personal Information), 디지털 포렌식(Digital Forensics), 암호모듈평가, etc.
E-mail : yeogkim@gmail.com

이 창 훈(Chang-hoon Lee)
2001년 한양대학교 자연과학부 수학전공(이학사)
2003년 고려대학교 정보보호대학원(공학석사)
2008년 고려대학교 정보경영전문대학원 정보보호전공(공학박사)
2008년~2008년 고려대학교 정보보호연구원 연구교수
2009년~2012년 한신대학교 컴퓨터공학부 조교수
2012년~2015년 서울과학기술대학교 컴퓨터공학과 조교수
2015년~2020년 서울과학기술대학교 컴퓨터공학과 부교수
2020년~현재 서울과학기술대학교 컴퓨터공학과 교수
관심분야 : 암호, 디지털포렌식, 사이버보안, etc.
E-mail : chlee@seoultech.ac.kr