IoT 단말기에서 증거추출 포렌식 연구

송진영* · 박대우*

*호서대학교 벤처대학원

Extract of evidence on the IoT Device

Jin-young Song* · Dea-woo Park**

*Hoseo Graduate School of Venture

E-mail : jedisong2083@gmail.com*, prof_pdw@naver.com**

요 약

IoT 기술의 발달로 IoT와 연계된 단말기가 활용되고 있다. 하지만 IoT가 사회 전반에 활용되면서 보안사고가 발생하고 있다. IoT 보안 사고는 개인의 위험과 사회의 혼란으로 연결될 수 있다. 본 연구에서는 IoT 스마트워치 단말기에서 보안 침해사고가 발생한 증거를 추출한다. IoT 보안 침해사고 환경을 분석하고 원본성과 무결성을 확보하기 위한 Hashing 함수를 추출한다. 그리고 IoT 스마트워치 단말기에서 Forensic 증거를 추출하여 원본성과 무결성을 검증하고 Forensic 보고서를 작성하여 법적 증거자료로 채택되도록 연구한다.

ABSTRACT

With the development of IoT technology, terminals connected with IoT are being used. However, security incidents are occurring as IoT is applied to society as a whole. IoT security incidents can be linked to personal risk and social disruption. In this study, we extract the evidence of security breach in IoT device. Analyze IoT security breach environment and extract Hashing function to secure original integrity and integrity. Then, the Forensic evidence is extracted from the IoT security device to verify the integrity of the original and Forensic reports should be written and studied to be used as legal evidence.

키워드

IoT 단말 포렌식, 증거 추출, Memory. 해외분석툴

Ⅰ. 서 론

최근 정보통신 및 IT 기술의 발달로 인해 가전기기, 모바일 장비, 웨어러블 기기들이 인간의 통제없이 유·무선 통신을 통해 데이터를 분석하거나 처리하고 있다. 특히 IoT의 발달은 각종 데이터를 수집 및 처리하여 사용자가 실생활에서 보다 나은 환경을 제공하고 있다[1].

하지만 IoT 단말 기기의 증가와 기술 발달은 디지털 포렌식 수사 시 증거 확보 및 분석에 많은 어려움이 발생한다. 가령 IoT 기기 중 스마트워치는 각 기기마다 수많은 OS(Android, iOS, Tizen 등), 제조사가 존재하고 있고 시스템 내부에 접근하는 방법이 달라 분석이 용이하지 않다.

그럼에도 IoT 단말기기에 디지털 포렌식이 필요한 이유는 이러한 IoT 단말 기기에서 범죄에 증명될 증거나 단서를 제공 받을 수 있기 때문이다. 즉, 사용자의 각종 건강 데이터(심장박동수, 일일활동 등), 위치 파악 등 다양한 정보를 확보할 수 있기 때문에 범행 시점을 특정 하는 등 다양한 사례가 나올 수 있다[2].

IoT 기기 중 스마트워치를 통해 증거를 추출하여 원본성과 무결성을 검증하고 수사에 활용될 수 있도록 하여야 한다[3].

따라서 본 연구에서는 IoT 기기 중 스마트워치의 자료를 imaging하고 포렌식 증거를 추출하여 법정 증거자료로 채택될 수 있도록 연구한다.

Ⅱ. 관련 연구

2.1 디지털 포렌식

디지털 포렌식은 디지털 증거물을 사법기관에 제출하기 위해 수사준비단계, 증거물 획득단계, 증거물보관 및 이송단계, 증거물분석단계, 보고서 작성단계를 말한다[4]. 과거에 얻을 수 없었던 증거나 단서들을 제공해 준다는 점에서 획기적인 방법이다. 컴퓨터 포렌식은 사이버 해킹 공격, 사이버 범죄시 범죄자들은 컴퓨터, 이메일, IT 기기, 스마트폰 등의 운영체제, 애플리케이션, 메모리 등에 다양한 전자적 증거를 남기게 되면서, 사이버 범죄자 추적 및 조사에 핵심적인 요소가 되고 있다.

2.2 포렌식 증거추출 툴

디지털 포렌식 툴은 수사에 활용될 목적으로 개발된 도구를 의미한다. 국내 수사기관에서는 증거 수집, 분석 및 보고서 작성 등 일련의 과정을 통합해주는 사용 툴을 사용하고 있다[5].

대표적으로는 Guidance Software의 EnCase와 AccessData의 FTK(Forensic ToolKit)을 사용하고 있으며, 국내에서 개발된 도구로는 Final Data의 Final Forensics, 검찰청의 D.E.A.S(Digital Evidence Analysis System for computer forensics) 등이 있다[6][7].

2.3 IoT 단말 운영

IoT 단말은 크게 가전기기, 모바일 장비, 웨어러블 기기 3가지로 분류할 수 있다.

가전기기는 냉장고, 세탁기, 에어컨 등 일상생활에 쓰이는 가전기기에 IoT 기술을 접목시켜 외부에서도 인터넷을 통해 접근이 가능하도록 설계된 형태를 말한다[8]. 모바일 장비는 스마트폰이나 스마트패드 등 이동통신망을 활용하여 각종 IoT 기기에 접근 및 제어할 수 있는 기기를 말한다. 웨어러블 장비는 대표적인 기기로는 스마트워치가 있으며, 스마트워치는 사용자의 신체에 접촉하여 각종 신체건강상태, 위치, 통신 등 기능을 수행하여 손쉽게 사용자의 현황을 파악할 수 있다[9].

최근에는 AI 스피커, 스마트 도어락 등 다양한 IoT 기기들이 개발 및 시판 중에 있다.

III. IoT 단말에서 포렌식 증거 추출

3.1 포렌식 증거추출 환경

본 논문에서는 스마트워치 중 모토로라社에서 출시한 Moto 360 제품을 이용하여 증거 추출 및 분석을 실시한다.

모토로라 Moto 360 주요사양	
CPU	ARM Cortex-A8 1GHz
메모리	512MB LPDDR, 4GB 내장
통신	WiFi 802.11b/g, 블루투스4.0
운영체제	Android Wear 1.0

표 1. 모토로라 Moto 360 주요사양

Android Wear OS와 PC와의 통신 설정을 하기 위해 Android SDK에서 제공하는 ADB(Android Debug Bridge)을 설치 후 실행하도록 한다.

3.2 장치 연결

Moto 360은 무선기기로 유선 USB로 제어가 불가능하여 스마트폰에 Moto 360을 연결 후 Android Wear OS의 ADB 디버깅과 블루투스 디버깅 기능을 이용하여 분석용 PC에서 스마트워치 Moto 360 기기 내부에 접근을 시도한다.

그림 1. 스마트워치 ADB 접근 흐름도

3.3 Imaging 작업

ADB Shell을 통해 dd명령어를 이용하여 스마트워치인 Moto 360 디바이스의 디렉토리와 파일을 Imaging 작업을 실시한다. 이때 Imaging 파일의 Hash 값을 생성하여 무결성을 확보한다.

IV. IoT 단말에서 증거 추출 포렌식

4.1 증거추출 포렌식

추출된 Imaging 파일은 FTK 프로그램과 sqlite3 DB 프로그램을 활용하여 Moto 360에서 추출된 디렉토리를 구분하고 분석을 실시한다.

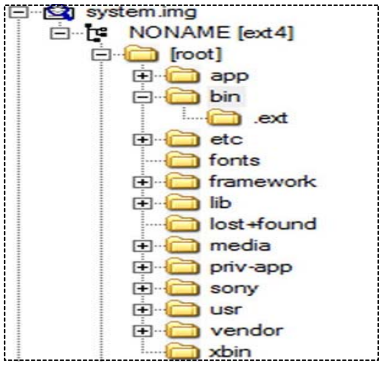

그림 2. Moto 360 Imaging 분석

스마트워치 디바이스에서 주요 분석 내용은 시스템에서의 세부 사항(설치된 응용 프로그램, 시스템 파일정보, 네트워크 주요 내용 등)과 응용 프로그램(캘린더, 메일, 메시지, 활동내역 등) 주요 정보 수집이 가능하다.

4.2 IoT 포렌식 기술 응용

Android Wear OS는 기본적으로 Android OS와 유사한 시스템 구조를 가지고 있어 스마트폰 포렌식 방식과 크게 다르지 않다[10]. 하지만 스마트폰보다 적은 메모리로 구성되어 있어 응용 프로그램을 직접 설치하기 보다는 DB 형태로 저장되어 스마트폰에서 데이터를 읽고 불러들이는 형식으로 되어있다. 즉, 중요 정보 저장 파일만 스마트워치 디바이스에 저장이 되어 동작하는 사실을 알 수 있다.

Ⅴ. 결 론

본 논문은 스마트워치 디바이스에 대한 디지털 포렌식 체계적인 조사 방법을 제안하고 있다.

IoT 단말에서 증거 추출을 위한 환경을 구성하고 스마트워치 내부 메모리에 접근하기 위해 Android Wear OS 에서의 ADB 디버깅과 블루투스 디버깅 기능과 Andorid SDK의 ADB를 이용한다. 스마트워치 단말 내부 메모리 접근 후 무결성 검증을 위한 Imaging 작업을 실시 하였다. 스마트워치 단말에서 증거 추출을 위한 포렌식을 수행하여 IoT 단말에 대한 포렌식을 통한 증거자료와 포렌식 기술을 확보하였다.

참고문헌

[1] 양진숙, 김주연. 뉴미디어 시대의 웨어러블 디바이스 사례분석 연구. 한국디자인문화학회지, 20(2), 354-364. 2014

[2] 김동관, 정대용, 이철수. 무선 공유기의 디지털 포렌식 프로세스 모델에 관한 연구. 디지털포렌식연구, 11(1), 17-35. 2017

[3] 이규안, 박대우, 신용태. 휴대폰 압수수색 표준절차와 포렌식 무결성 입증. 한국통신학회논문지, 33(6), 512-519. 2008

[4] 김기환, 박대우, 신용태. 모바일 포렌식에서의 무결성 입증방안 연구. 한국컴퓨터정보학회지, 15(1), 37-46. 2007

[5] 이태림, 신상욱. 디지털 포렌식을 위한 증거분석 도구의 신뢰성 검증. 정보보호학회논문지, 21(3), 165-176. 2011

[6] 윤경배, 천우성, 박대우. 압수 수색된 안드로이드와 윈도우모바일 스마트폰의 포렌식 증거 자료. 한국정보통신학회논문지, 17(2), 323-331. 2013

[7] 이종찬, 박상준. 포렌식에서 디지털 증거의 우선순위 스케쥴링. 한국정보통신학회논문지, 17(9), 2055-2062. 2013

[8] 장기만, 황종선, 정회경. XML기반의 IoT 시뮬레이션 시스템. 한국정보통신학회논문지, 20(3), 663-668. 2016

[9] 김선태, 임채덕, 정희범, 한동원. 경량 IoT 디바이스 플랫폼 동향 연구. 한국정보기술학회지, 13(2), 1-8. 2015

[10] 이정기, 양철승, 김준하, 김강진. 안드로이드 기반 스마트 홈 디바이스의 통신 데이터 보안 및 통합 관리 플랫폼 연구개발. 한국정보통신학회논문지, 19(5), 1173-1179. 2015