블루투스 HCI 스눕 로그를 통한 사건 현장 파악

양재옥*, 방민제*, 이성원**, 조태남***
*우석대학교 정보보안학과
**(주)아이제론
***우석대학교 IT전자융합공학과
e-mail:yjo0109@stu.woosuk.ac.kr*, bmj8777@naver.com*,
forensic@izerone.co.kr**, tncho@ws.ac.kr***

Identification of the Crime Scene through Bluethooth HCI Snoop Log

Jae-Ok Yang*, Min-Je Bang*, Seong-Won Lee**, Taenam Cho***
*Dept. of Information Security, Woosuk University
**Ltd. Izerone
***Dept. of IT&Electronics Engineering, Woosuk University

요 약

사건 현장을 재현하는 것은 수사에서 매우 중요한 일이다. CCTV가 현장 파악에 유용하기는 하지만 세부적인 상황파악에는 한계가 있다. 현대는 디지털 시대인 만큼 사건 현장에서는 많은 디지털 흔적이 남게 된다. 스마트폰의 디지털 흔적도 사고경위 파악에 유용하다. 본 논문에서는 특히 안드로이드 스마트폰의 블루투스 디지털 기록을 이용하여 보다 정교하게 현장을 재현하는 방법에 대하여 연구하였다.

1. 서론

CCTV가 곳곳에 설치되어 있어 여기에 저장된 영상이 사건 현장을 파악하는데 매우 유용하기는 하지만, CCTV가 설치되지 않은 곳도 많고 설치된 곳이라도 사각지대가 존재한다. 또한 낮은 해상도로 정확한 파악이 어려울 경우도 있고 영상만 저장할 뿐 소리는 저장하지 않기 때문에 정확한 현장 파악을 하기는 어려우며, 사건 당시 희생자나 피의자가 무엇을 하고 있었는지 상세히 보여주지는 못한다. 반면에 스마트폰은 현대인의 필수품이 되어 사건 현장에는 스마트폰이 존재할 확률이 매우 높으며 스마트폰이 저장하고 있는 정보도 매우 많다. 따라서 스마트폰은 디지털 포렌식에 있어서 중요한 분석 자료가 된다. 한편 스마트폰은 현장의 증거물이 되기도 하지만, 스마트폰 사용이 교통사고 등의 사고를 발생시키는 원인이 되기도 한다.

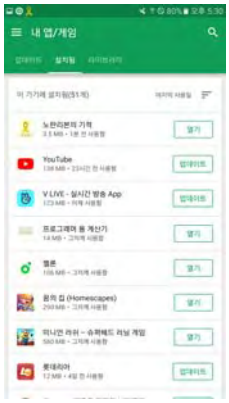
본 논문에서는 현대인의 필수품인 스마트폰 중에서 우리나라 시장 점유율이 가장 높은 안드로이드 스마트폰을 이용하여 수집할 수 있는 다양한 정보와 분석 방법을 연구하였다. 특히 블루투스 통신을 이용한 데이터의 송수신과 핸즈프리 기기를 사용한 통화 및 음악 감상이나 영상 시청에 대한 기록을 분석함으로써 사건 당시 희생자나 피의자의 행위를 파악함으로써 사건 정황과 경위를 좀 더 정확하게 파악할 수 있다.

2. 안드로이드 스마트폰 디지털 정보 분석

본 절에서는 사건 당시 희생자나 피의자가 스마트폰을 이용하여 어떤 행위를 하고 있었는지를 파악하기 위해 가장 손쉽게 접근할 수 있는 PlayStore 앱 정보, 다소 전문 기술이 필요한 ADB를 이용한 앱 실행 기록, 포렌식 전문툴인 AXIOM 그리고 블루투스 이용 기록인 HCI 스눕 로그를 통한 정보 수집 및 분석 방법에 대해 기술한다.

2.1 PlayStore 앱 실행 기록

안드로이드 스마트폰의 기본 앱인 PlayStore는 앱의 설치 및 업데이트 기능을 제공한다. 이 앱을 이용하면 다운로드하여 설치한 앱들의 몇 주 전까지의 사용 기록을 확인할 수 있다. 하지만, (그림 1)과 같이 실행 후 1시간 이상 경과된 경우에는 시간 단위로만 실행시각을 제공하며 하루가 지난 경우에는 일별로만 제공하기 때문에 자세한 실행 시각을 파악할 수 없다.



(그림 1) PlayStore의 앱 실행기록

2.2 응용프로그램 데이터

안드로이드 응용프로그램은 실행에 필요한 자료나 실행했던 기록을 일정한 폴더에 데이터베이스로 저장한다. <표 1>은 안드로이드 5.0.1에서 사용하는 응용프로그램 데이터의 표준 경로이며, 기기와 버전에 따라 다를 수 있다.

<표 1> 안드로이드 응용프로그램 데이터 경로

데이터베이스	경로
Contacts	/data/data/com.android.providers.contacts/databases/contacts2.db
Web history	/data/data/com.android.browser/databases/browser2.db
Calendar	/data/data/com.android.providers.calendar/databases/calendar.db
Youtube history	/data/data/com.google.android.youtube/databases/history.db
Bluetooth	/data/data/com.android.bluetooth/databases/btopp.db

이러한 데이터베이스로부터 연락처, 웹 히스토리, 일정 정보, 유투브 히스토리, 블루투스 전송 내역 등을 확인할 수 있다. 이 데이터는 안드로이드 개발자를 위해 무료로 제공되는 툴인 ADB(Android Debug Bridge)를[1] 이용하여 접근할 수 있다. (그림 2)는 분석하고자 하는 스마트폰을 루팅하여[2] ADB로 다운로드받은 btopp.db를 SQLite 브라우저로[3] 추출한 예이다. 예에서 볼 수 있듯이 블루투스를 이용한 데이터 전송에 대한 전송 시각, 파일명, 타입, 상대 MAC 주소 등을 알 수 있다. 단, 기타의 블루투스 기기 사용에 대한 기록은 제공하지 않는다.

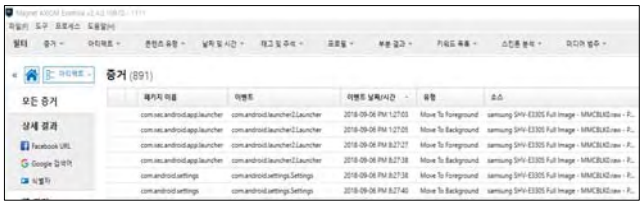
(그림 2) ADB를 통한 블루투스 사용 기록

2.3 Magnet AXIOM

Magnet AXIOM은[4] 스마트폰, 컴퓨터, 클라우드에서 다양한 증거 데이터를 수집하여 분석관이 쉽게 분석할 수 있도록 도와주는 디지털 포렌식 도구이다. 스마트폰 포렌식의 경우, 파일에 대한 정보(파일명, 파일 확장자, 생성시간, 수정시간, 접근시간), Wi-Fi Profiles, 블루투스 통신 기기, 스마트폰의 계정 정보, 통화 기록, 연락처, 설치된 응용 프로그램, 파일시스템 정보 등 쉽게 분석할 수 있는 증거 항목 별로 확인할 수 있다. (그림 3)은 Magnet AXIOM을 이용하여 스마트폰의 파일 시스템 파티션별로 블루투스 데이터베이스와 같은 저장된 자료의 목록을 보여준다. 하지만 ADB를 이용할 때와 같이 데이터베이스를 추출하여 내용을 보여 주지는 않는다.

(그림 3) AXIOM을 이용한 스마트폰 파일시스템 분석

또한, AXIOM에서는 안드로이드 실행기록을 볼 수 있는데, 앱의 패키지 이름으로 목록이 제공되며 PlayStore 와는 달리 다운로드한 앱들 뿐만 아니라 스마트폰의 기본적으로 설치된 앱의 사용 기록도 확인할 수 있다. (그림 4)는 AXIOM으로 확인한 앱의 실행 기록이다. 그러나 여기서는 앱의 실행시각만 알 수 있을 뿐, 종료시각을 알 수 없기 때문에 사건이 발생한 특정 시간대에 사용자가 실행한 앱을 정확하게 알 수 없다.



(그림 4) AXIOM을 이용한 앱 실행 기록 분석

또한, 블루투스 기록 정보 중 블루투스 통신을 한 기기들은 한 눈에 확인할 수 있는 반면, 어떤 파일이 블루투스를 이용하여 전송되었는지는 확인하기 어렵다.

2.4 블루투스 HCI 스눕(snoop) 로그

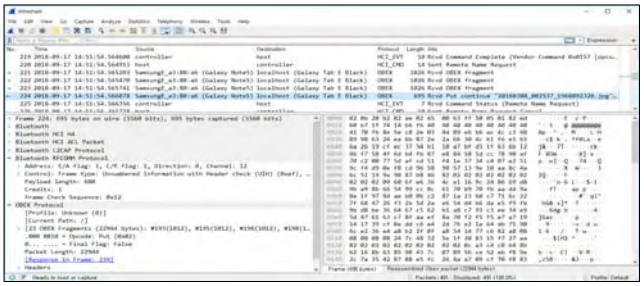
안드로이드 스마트폰은 다양한 개발자 옵션을 보유하고 있는데, 그 중의 하나로서 스마트폰과의 블루투스 통신 정보가 HCI 스눕 로그에 저장된다. 안드로이드 5.0.1 버전의

경우에는 /sdcard/Android/data 폴더에 실행 중인 블루투스 통신에 대한 로그 파일인 btsnoop_hci.log와 최근에 종료한 블루투스 통신에 대한 로그 파일인 btsnoop_hci.log.last가 존재한다.

블루투스 통신 정보를 확인하면 일반적인 통화내역 뿐만 아니라 핸즈프리 기기를 사용했는지도 알 수 있으며, 단순한 웹 접속 기록 외에도 블루투스 기기로 스트리밍을 이용하였는지 등도 확인할 수 있어, 사용자의 당시 상황을 좀 더 명확하게 파악할 수 있다.

HCI 스눕 로그에는 사용한 블루투스 프로파일(profile)들이 저장되어 있어 이로부터 사용자가 사용한 서비스를 알 수 있다. 블루투스 프로파일이란 블루투스 장치간의 통신 서비스에 필요한 전송 프로토콜, 파라미터 등의 속성을 규정한 것이다[5]. 블루투스 프로파일에는 여러 가지가 있는데, 주로 사용되는 프로파일에는 파일전송에 관련된 FTP(File Transfer Profile), 이어폰을 통한 통화에 관련된 HSP(HeadSet Profile), HFP(Hans-Free Profile) 음악 재생과 원격제어에 관련된 A2DP(Advanced Audio Distribution Profile), AVRCP(Audio/Visual Remote Control Profile), AVDTP(Audio/Visual Distribution Transport Profile) 등이 있다[6][7].

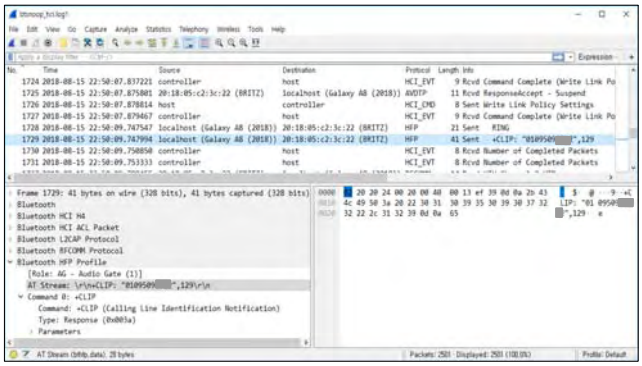
(그림 5)는 통신 패킷 분석 툴인 Wireshark를 통하여 HCI 스눕 로그를 확인한 예로서, 2018년 9월 17일 14시 51분 54초에 파일 전송 프로토콜인 OBEX를 사용하여 Galaxy Note5 사용자가 Galaxy Tab E Black 사용자에게 20160308_002537_1968092320.jpg를 전송한 기록을 보여준다. 또한 전송한 파일 내용도 16진수로 확인할 수 있는데, 이를 복사하여 저장하면 이미지를 확인할 수 있다.



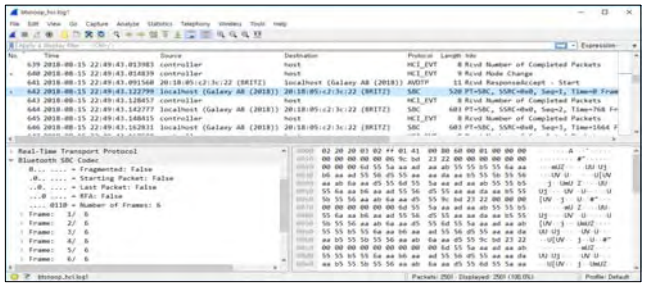
(그림 5) HCI 스눕 로그 - 파일 전송 기록

(그림 6)은 2018년 8월 15일 22시 50분 09초의 통화기록을 보여주는데, Galaxy A8 사용자가 BRITZ 기기를 통해 통화 프로파일인 HFP를 사용하여 “0109509****”로 전화했음을 알 수 있다. 즉, 사용자는 당시에 블루투스 핸즈프리 기기를 이용하여 통화했음을 말해 준다.

(그림 7)에서는 2018년 8월 15일 22시 49분 43초에 Galaxy A8 사용자가 BRITZ라는 기기를 이용하여 A2DP 프로파일의 기본 표준 압축 코덱인 SBC(Sub-Band Codec)을 사용한 것을 알 수 있다. 따라서 블루투스 이어폰 등을 이용하여 음악을 감상했다고 추측할 수 있다.



(그림 6) HCI 스눕 기록 - 통화 기록



(그림 7) HCI 스눕 로그 - 스트리밍 기록

그러나 실제로는 실험에서는 구글 크롬 앱을 이용하여 유투브를 감상하였는데, HCI 스눕 로그에서는 스트리밍의 기록만 확인할 수 있을 뿐 음악 감상인지 동영상 감상인지의 여부까지는 확인할 수 없다. AXIOM에서 크롬의 웹 히스토리를 살펴보면 블루투스 HCI 스눕 로그 시간에 유투브 사이트에 접속한 사실을 확인함으로써, 블루투스 이어폰 등을 통해 구글 크롬 앱으로 유투브를 감상했음을 확인할 수 있다.

2.5 사건 현장 파악을 위한 정보의 활용

본 논문에서 제시한 분석 방법과 데이터는 활용할 수 있는 무수히 많은 정보 중의 극히 일부일 것이다. 앞에서 기술한 바와 같이 각 데이터들은 동일한 이벤트에 대해서 제공하는 정보가 다르기 때문에 상황에 따라 유용한 방법과 데이터를 사용하는 것이 바람직할 것이다.

예를 든다면, 사건 당시 희생자/피의자가 스마트폰을 사용하고 있었는지, 사용했다면 어떤 앱을 실행하고 있었는지를 PlayStore나 Axiom으로 확인하고, 만약 희생자/피의자가 통화 중이었다면 ADB를 통하여 누구와 통화했는지 알 수 있고, 블루투스 핸즈프리 기기를 소유하고 있다면

HCI 스눕 로그를 통하여 희생자/피의자가 자유로운 상태로 통화 중이었는지, 이어폰의 사용으로 인해 외부 소리로부터 차단된 상태일 가능성이 있는지 알 수 있다. 또한 HCI 스눕 기록과 AXIOM 분석을 통하여 유투브 감상 중이었다는 것이 확인된다면 제대로 주변을 살펴보지 못했다는 것을 추측할 있다. 또한 전송한 데이터의 내용이 중요하다면 HCI 스눕 로그나 ADB를 통하여 데이터를 확인할 수도 있다.

3. 결론 및 향후 연구

사건 현장의 재현과 파악은 수사에 있어서 매우 중요한 요소이나 완벽하게 파악하는 것은 거의 불가능할 것이다. 본 논문에서는 대부분의 사람들이 소지하고 있는 안드로이드 스마트폰에 저장된 데이터를 이용하여 현장을 파악하기 위한 유용한 정보들과 이에 대한 분석 방법을 연구하였다. 그러나 이러한 정보들은 각기 다른 목적을 가지고 그에 맞는 정보들만을 제공하기 때문에, 다양한 정보의 수집과 통합적 분석이 필요하다. 본 논문에서는 특히 블루투스 통신에 관련된 정보들을 분석하여, 다양한 정보를 논리적으로 연결할 수 있도록 함으로써 좀 더 정확하게 희생자나 피의자의 당시 상황을 파악할 수 있도록 하였다.

본 논문에서 중점적으로 연구했던 블루투스 HCI 스눕 로그는 개발자 옵션으로서 사용자가 활성화시키지 않으면 작동되지 않는다. 이 데이터가 디지털 포렌식에 중요한 단서를 제공할 수 있으므로, 디폴트로 활성화되도록 하는 것을 제안한다.

향후, 다양한 분석 시나리오를 기반으로 한 필요 데이터의 수집 방법과 분석 절차에 대해 연구가 필요하다.

ACKNOWLEDGMENT

본 연구는 한국연구재단의 연구 지원
(NRF-2017R1D1A3B03032637)에 의한 것임

참고문헌

[1] ADB, http://adbshell.com/
[2] Jung-Hoon Oh & Sang-Jin Lee, “A Study on the Analysis Methodology of Smartphone for Android Forensics”, Journal of Digital Forensics , (9), 2012
[3] SQLite, https://www.sqlite.org/index.html
[4] Magnet AXIOM, https://www.magnetforensics.com/magnet-axiom/
[5] Bluetooth Profiles, https://www.bluetooth.com/ko-kr/specifications/profiles-overview
[6] Bluetooth Core Specification, http://www.bluetooth.com/
[7] https://www.bluetooth.com/ko-kr/specifications/profiles-overview