모바일 포렌식 연구를 위한 서드 파티 어플리케이션 분석

류정현, 박종혁*
서울과학기술대학교 컴퓨터공학과
e-mail:{jh.ryu, jhpark1}@seoultech.ac.kr

Third Party Application Analysis For Mobile Forensics Study

Jung Hyun Ryu, Jong Hyuk Park*
*Dept of Computer Engeneering,
Seoul National University of Science and Technology(SeoulTech)

요 약

스마트폰 서드 파티 애플리케이션에 대한 포렌식 분석은 최근 수 년 간 탐구되어야 할 새로운 영역으로 떠올랐다. 현재 스마트폰 시장은 그 규모를 측정하는 것이 무의미할 만큼 커졌으며 각 스마트폰 플랫폼의 앱(App)마켓에는 셀 수 없이 많은 서드 파티 애플리케이션이 존재한다. 모바일 포렌식 소프트웨어 도구들은 일반적으로 연락처, 문자메시지, 통화기록 등의 전형적인 데이터를 수집한다. 이러한 도구들은 서드 파티 애플리케이션이 기기 내부에 저장하는 정보들을 간과하기 쉽다. 여러 제조사 중, 애플사의 모바일 기기에 설치된 많은 서드 파티 애플리케이션은 수사에 도움이 되는 많은 정보와 관련있는 디지털 증거를 남긴다. 이런 잠재적 증거들은 기기 내부에 저장되기도 하며, 비교적 손쉬운 방법으로 법정에 제출 가능하다. 스마트폰으로 이루어지는 많은 활동은 상당 부분 서드 파티 애플리케이션으로 이루어지며, 사이버 범죄 사건의 중심에 스마트폰이 있다면 서드 파티 애플리케이션 분석을 통한 핵심 증거 획득이 사건을 해결할 가능성이 높아진다.

본 논문에서는 스마트폰에서 널리 쓰이고 있는 소셜네트워크 애플리케이션인 '인스타그램(Instagram)'에서 행해진 포렌식 분석에 초점을 맞추고, 기기는 전 세계 적으로 가장 사용자 점유율이 높은 스마트폰인 아이폰에서 이루어졌다.

1. 서론

이 논문의 주 목적은 디지털 포렌식 수사과정에 도움이 되기 위해 애플사의 모바일 기기 운영체제인 iOS에서 소셜 네트워크 서비스의 다양한 보안 이슈를 알아보는 것이다.

정보는 다양한 형태로 스마트폰 내부의 다양한 곳에 저장된다. 포렌식 도구를 이용하여 스마트폰의 기본적인 사항을 분석한다면 자칫 서드 파티 애플리케이션이 남긴 정보를 간과할 수 있다.

스마트폰 애플리케이션 분석 업체인 'App Annie'가 2016년에 발표한 보고서 'App Annie 2015 Retrospective Report'에 의하면 한국의 일인당 월 평균 사용 앱의 개수는 약 38개에 달하며, 2017년 전 세계 앱의 총 사용 시간은 2016년 대비 1500억 시간 이상이 증가한 약 9000억 시간이다 [1][2].

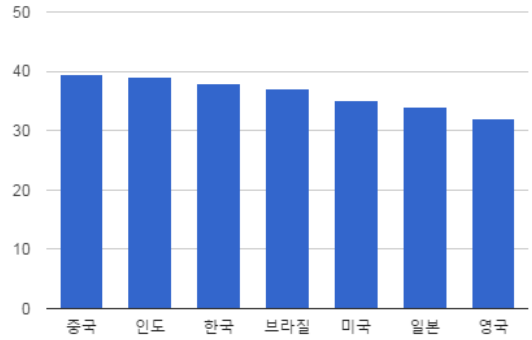
애플의 앱스토어(App Store)와 구글의 플레이스토어(Play Store)에서의 애플리케이션 다운로드 수와 매출액은 매 년 지속적으로 증가하고 있다 [3]. 이는 사용자의 스마트폰 활동 중 많은 부분을 서드 파티 애플리케이션이 차지한다는 사실을 시사한다.

만약 사이버 범죄의 열쇠가 될 하나의 스마트폰이 이처럼 대부분의 활동을 서드 파티 애플리케이션을 통해 수행했다면 모바일 기기 자체에 관한 단순한 포렌식 분석은 의미가 없을지도 모른다.

본 논문에서는 스마트폰 내의 내양하고 가치있는 서드 파티 애플리케이션의 정보를 수집하는 것에 대한 일반적인 방법론에 초점을 맞추었다. 따라서 표준 디지털 포렌식 수사과정에서 본 논문에서 다룬 애플리케이션과 유사한 애플리케이션에 대해 똑같이 적용할 수 있을 것으로 판단된다.

Acknowledgments

이 논문은 2016년도 정부 (미래창조과학부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임(No. 2016R1A2B4011069)



(그림 1) 주요 국가별 일인당 월평균 사용 앱 개수

2. 애플(Apple)사의 모바일 기기 : 아이폰(iPhone)

오늘날의 모바일 폰을 재정립했다고 평가 받는 아이폰은 2007년 발매된, 애플사의 제품 중에서 가장 인기있는 제품이다. 아이폰은 운영체제로서 iOS를 사용한다. iOS의 구조는 계층화되어있고 4개의 추상화 레이어로 구성되어있다. 아이폰에 설치된 모든 애플리케이션의 기능은 이 레이어들에 의해 결정된다 [14]. 아이폰은 미리 설치되어 있는 그들만의 기본 애플리케이션을 가지지만 사용자는 개인적으로 '앱스토어(App store)'에서 다운로드 받아 기기에 서드 파티 애플리케이션을 설치할 수 있다. iOS는 논리적으로 비교적 폐쇄적 특징을 가지고 있으며, 서드 파티 개발자들이 등록 신청 한 애플리케이션에 대해서 엄격한 정책을 운영하고 있다. 이런 특징으로 인해 다른 플랫폼 및 운영체제에 비해 애플리케이션이 폐쇄적으로 만들어져 포렌식 분석에 의해 얻을 수 있는 인텔리전스(intelligence)가 적을 수 있다.

3. 서드 파티 애플리케이션

현재 모바일 시장에는 수 백만개의 서드 파티 애플리케이션이 존재한다. 애플 앱스토어에서의 모바일 애플리케이션 다운로드 수는 2015년 6월 기준 약 1천억 건을 돌파했으며, 계속 증가하는 추세이다 [3].

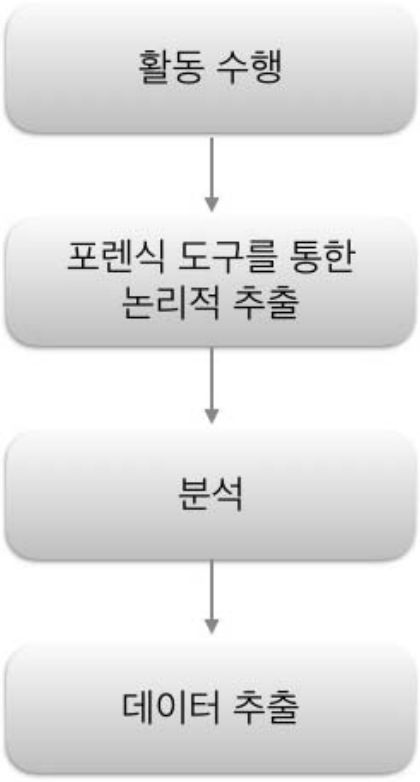
이 수 많은 애플리케이션 중 우리는 포렌식 분석 대상으로 최근 수 년 사이 큰 인기를 얻고 있는 '인스타그램(Instagram)'을 선택했다. 인스타그램은 소셜 네트워크 서비스(Social Network Service, SNS)의 일종으로 거의 모든 스마트폰 플랫폼과 운영체제에서 사용이 가능하며 현재 매우 널리 쓰이고 있는 서드 파티 애플리케이션이다. 2016년 전 세계 월 실사용자 기준으로 애플과 구글의 애플리케이션 시장에서 각각 6위 4위를 차지했다 [2].

인스타그램에서 사용자는 사진과 짧은 영상을 업로드 할 수 있으며, 다른 사용자의 소식을 '팔로우'하고 위도 및 경도나 지역의 이름이 새겨진 지오태그(geotag)이미지를 받아 볼 수 있다. 사용자는 자신의 계정을 공개하거나 개인적으로 관리할 수 있으며, Facebook, Twitter, Tumblr, Flickr와 같은 다른 대형 소셜 네트워크 서비스에 계정을 연결하여 게시물을 동시에 업로드 할 수도 있다. 이와 같이 사용자는 사진과 영상을 중심으로 각종 해시태그(Hashtag) 생성, 현재 위치 등록, '팔로잉', 코멘트 생성 등의 활동을 하게 되는데, 이로 인해 기기 내부에 다양한 정보들을 남긴다.

4. 포렌식 분석

이 논문의 주 목적은 스마트폰에서 수행되는 소셜 네트워크 서비스 애플리케이션의 활동이 해당 기기의 내부 메모리에 저장되는지의 여부와 기기에서 추출하거나 복구 가능한 데이터의 종류를 알아보는 것이다. 이 일련의 과정에 앞서 기기는 반드시 네트워크가 가능한 상태여야 한다.

애플리케이션이 종료되고 기기의 Wi-fi연결을 차단한 후, 인스타그램을 통해 특정 활동을 준비한다. 인스타그램에서 특정 활동을 완료한 후 기기의 통신 모드를 비행기 모드로 설정하여 외부로부터의 모든 신호를 차단하고 포렌식 도구를 이용하여 데이터를 추출한다. 우리는 분석 대상 기기로서 탈옥이 되지 않은 iPhone6s, 운영체제로서 iOS 10.2.1, 서드 파티 애플리케이션으로서 인스타그램 10.13, 포렌식 분석 도구로서 MSAB사의 XRY version 7.1을 선택했다.



(그림 2) 서드 파티 포렌식 분석 과정

위의 그림과 같이 애플리케이션으로 일련의 활동을 수행한 후 포렌식 도구를 통한 데이터 논리적 추출을 하였

으며, 분석을 통해 데이터를 정리하고 증거로서 가치가 있다고 판단되는 데이터를 인텔리전스로서 다시 추출하였다.

<표 1> 분석 결과의 세부 내용

	활동 내용	분석 결과
1	_ryudeo라는 사용자 이름으로 로그인	'recent-users' plist 파일에서 인스타그램 ID 고유번호와 사용자이름 _ryudeo 발견
2	인스타그램 계정의 비밀번호 입력	비밀번호 흔적 발견 불가능
3	인스타그램 내부의 사진 편집 기능 사용	편집된 사진은 아이폰 앨범 내의 'Instagram' 폴더에 저장
4	편집된 사진 상에 캡션을 생성하고 해시태그 추가	캡션에 대한 정보는 발견 불가능 했지만 사용된 해시대그는 'visited hashtag' plist 파일에서 발견 가능
5	Facebook 계정에 사진 연동	Facebook 사용자 계정과 암호화된 facebook_user_info key를 찾을 수 있었으며, 사진을 업로드한 인스타그램 계정도 발견
6	사진 게시	1. 사진을 업로드한 시각은 사진이 생성된 시각과 동일하며 원본 사진과 편집된 사진의 해시값은 상이함 2. 수정과 접근기록을 포함하는 원본 사진의 시각은 메타데이터에서 발견됐으며, 날짜와 시각은 기기의 시스템시간에 기반 3. 위치와 좌표값을 비롯한 다른 메타데이터도 발견 가능
7	다른 계정 '팔로우'	사용자 이름 _ryudeo에 의해 팔로우된 계정의 사용자 이름과 인스타그램 ID 고유번호는 'recent-users' plist 파일에서 발견 가능
8	다른 게시물에 코멘트 생성	XRY는 'status update'탭의 최신 10개의 사진만 추출하므로 사용자가 최신 10개의 상태 안에 코멘트를 생성하지 않았다면 발견 불가능
9	'팔로워'가 사용자의 사진에 코멘트 생성	XRY는 'status update'탭의 최신 10개의 사진만 추출하므로 사용자가 최신 10개의 상태 안에 코멘트를 생성하지 않았다면 발견 불가능
10	게시된 사진 삭제	인스타그램에서 게시물을 삭제하여도 아이폰 앨범의 'Instagram'폴더의 사진은 유지
11	편집을 거치지 않은 사진 업로드	인스타그램에 업로드된 사진의 흔적이나 증거 발견 불가능

위의 표와 같이 분석을 통해 얻은 서드 파티 애플리케이션의 데이터는 사용자의 활동에 따라 많은 데이터를 기기 내부에 남겼다. 이를 통해 포렌식 분석에 도움을 줄 수 있을 것이다.

5. 결론

앞서 확인한 결과에서 이메일 주소나 비밀번호와 같은 세부사항으로서 사이버 범죄 사건을 종결지을만한 강력한 증거는 찾을 수 없었다. 하지만 사용자가 본 게시물에 대한 기록, 로그인된 계정, 사용자가 게시한 게시물의 날짜와 시각 그리고 해시태그, 다른 SNS 애플리케이션의 사용 여부, 사용자가 작성한 코멘트 등을 확인하여 사용자의 행적을 파악할 수 있다. 또한 인스타그램에 업로드하기 위해 내부 편집기를 사용하여 원본 사진을 게시한 경우 아이폰 내부의 기본 애플리케이션인 앨범에 저장된 사진을 확인할 수 있었다. 이 사실을 토대로 서드 파티 애플리케이션이 기기 내부에 데이터를 남기게 되고, 남긴 데이터와 서드 파티 애플리케이션을 연관지어 증거를 찾을 수 있음을 알 수 있다. 이러한 잔여데이터는 보통 데이터를 생성한 애플리케이션으로 확인할 수 있다고 생각하지만 불가능하기 때문에 사건의 데이터를 조사할 때 잔여 데이터를 조사하는 것은 매우 중요하다 [7].

다른 모든 스마트폰 사용자는 각기 다른 사용방식을 가지고 있으며, 각기 다른 서드 파티 애플리케이션을 사용한다. 이 사실은 최근 수 년 간 폭발적으로 증가한 스마트폰 사용자에 대해 디지털 포렌식을 통한 분석을 완벽하게 만들기 위해서는 모바일 기기, 플랫폼, 운영체제에 대한 분석 뿐만 아니라 수 백만 개의 서드 파티 애플리케이션이 만들어내는 데이터에 대한 분석까지 이루어져야함을 시사한다.

모바일 포렌식을 위해 서드 파티 애플리케이션에 대한 포렌식 기법의 자세한 정립이 요구되고, 사이버 범죄에 악용될 가능성에 대비하여 서드 파티 개발에 대한 비교적 엄격한 기준이 필요해 보인다.

참고문헌

[1] App Annie (2016. 1). “App Annie 2015 Retrospective”.

[2] App Annie (2017. 1). “App Annie 2016 Retrospective”.

[3] 정보통신정책연구원. “모바일 앱(App) 마켓 최근 동향 ”(2016). 유선실.

[4] 권양섭. "유비쿼터스 컴퓨팅환경하에서 디지털 포렌식 수사절차에 관한 연구." 법학연구 16 (2016): 93-120.

[5] 윤종철, and 박용석. "KakaoTalk 의 채팅 메시지 포렌식 분석 연구 및 WhatsApp 의 Artifacts 와의 비교 분석." 한국정보통신학회논문지 20.4 (2016): 777-785.

[6] 연규철, et al. "스마트 기기에 설치된 내비게이션 어플리케이션의 위치 정보 흔적 연구." 정보보호학회논문지 26.1 (2016): 109-115.

[7] JungHeum Park, Bora Park, SangJin Lee, SeokHie Hong, Jong Hyuk Park. "Extraction of residual information in the microsoft powerpoint file from the viewpoint of digital forensics considering percom environment." Pervasive Computing and Communications, 2008. PerCom 2008. Sixth Annual IEEE International Conference on. IEEE, 2008.

[8] Muraina, Ishola D., Mustafa Muwafak Alobaedy, and Huda Haji Ibrahim. "A Framework for Preserving Data Integrity during Mobile Device Forensic in Open Source Software Environment." (2017).

[9] Kaur, Harleen, and Khairaj Ram Choudhary. "Digital Forensics: Implementation and Analysis for Google Android Framework." Information Fusion for Cyber-Security Analytics. Springer International Publishing, 2017. 307-331.

[9] Lazaridis, Ioannis, Theodoros Arampatzis, and Sotirios Pouros. "Evaluation of Digital Forensics Tools on Data Recovery and Analysis." The Third International Conference on Computer Science, Computer Engineering, and Social Media (CSCESM2016). 2016.

[10] Shankar, P. Ravi, et al. "Study on Digital Forensics in IoS Devices." E-Commerce for future & Trends 1.1 (2016): 21-28.

[11] Rajendran, S., and N. P. Gopalan. "Mobile Forensic Investigation (MFI) Life Cycle Process for Digital Data Discovery (DDD)." Proceedings of the International Conference on Soft Computing Systems. Springer India, 2016.

[12] Geddes, Mary, and Pooneh Bagheri Zadeh. "Forensic analysis of private browsing." Cyber Security And Protection Of Digital Services (Cyber Security), 2016 International Conference On. IEEE, 2016.

[13] Benkhelifa, Elhadje, Benjamin E. Thomas, and Yaser Jararweh. "Framework for Mobile Devices Analysis." Procedia Computer Science 83 (2016): 1188-1193.

[14] Al Mushcab, Reema, and Pavel Gladyshev. "Forensic analysis of instagram and path on an iPhone 5s mobile device." Computers and Communication (ISCC), 2015 IEEE Symposium on. IEEE, 2015.