스마트폰 포렌식: 소셜 네트워크 서비스에서의 불법 콘텐츠 사용정보 추출

여정호, 김응모
성균관대학교 정보통신대학원
e-mail: jhyeo@copyright.or.kr,
umkim@ece.skku.ac.kr

Smart Phone Forensic: Extracting the Historical Information of Criminal Contents in Social Network Service

Jung Ho Yeo, Ung Mo Kim
School of Information and Communications, SungKyunKwan University

요 약

스마트폰의 빠른 확산과 웹 기술의 발전과 더불어 스마트폰을 통한 불법 콘텐츠 유출 가능성이 심화됨에 따라 스마트폰 포렌식에 대한 연구가 활발히 진행되고 있다. 스마트폰 내 증거 데이터는 기존의 모바일 디바이스에서 제공되었던 문자메시지, 송수신 히스토리 정보 외에 이메일, 웹 검색 히스토리, 사용자 이동경로, 소셜 네트워크 클라이언트 파일도 중요한 기록 정보로 제공된다. 이에 본 연구에서는 스마트폰 내 저장되어 있는 불법 콘텐츠 사용 흔적을 추출하여 소셜 네트워크에서의 불법 콘텐츠 유통 상황을 대응하고자 한다.

1. 서론

최근 스마트폰이 IT 모바일 시장의 새로운 패러다임으로 발전됨에 따라 스마트폰이 포렌식 기술에서 차지하는 비중이 날로 늘어나고 있다. 스마트폰은 개방형 운영체제(Open Operating System)를 사용하여 단말 제조사뿐만 아니라 이동 통신사, 써드 파티(3rd party) 업체에서 새로운 어플리케이션 프로그램을 제공하고 단말기에서 동작할 수 있도록 하는 고차원적 운영체제의 존재가 기존 모바일 기기와 차이점이라 할 수 있다. 스마트폰을 매체로 산업기술 및 영업비밀 유출행위, 저작권 위반행위 등 사이버 범죄가 많이 발생한다. 따라서 스마트폰을 악용한 범죄행위에 대응하여 스마트폰 포렌식 관련 연구가 필요로 하고 있다. 스마트폰 포렌식은 스마트폰에서 발생되는 다양한 범죄에 대해 법적 증거를 획득하여 분석하고 분석된 결과를 토대로 범죄 수사에 사용하는 기술이다. 스마트폰에서는 기존 모바일 기기에서 제공되는 SMS/MMS, 연락처, 일정, 통화목록, 메모정보 이외에 이메일, 웹 검색 히스토리, 소셜 네트워크 서비스(Social Network Service) 데이터를 통해 다양한 증거 데이터를 제공한다.

현재 웹의 발전과 더불어 스마트폰에 운연체제가 탑재되어 사용자는 스마트폰에서 소셜 네트워크 서비스를 이용하여 콘텐츠를 공유한다. 따라서 SNS에서 불법 콘텐츠를 다운 받아 사용하는 행위가 종종 발행하고 있어 저작권법을 위반하는 행위 뿐 아니라 우리나라 콘텐츠산업에 부정적인 영향을 끼치고 있다. 본 연구는 SNS에서 발생하는 불법 콘텐츠 유통 증거를 수집하여 저작권 위반 등 불법 행위를 대응하고자 한다.

2. 관련 연구

2.1 스마트폰 포렌식 기술

스마트폰 포렌식[1]은 스마트폰에서 발생되는 다양한 범죄에 대해 법적 증거를 획득하여 분석하고 분석된 결과를 토대로 범죄 수사에 사용하는 기술이다. 스마트폰에서의 콘텐츠의 이용 형태는 기존의 파일 공유사이트에서 보던 것과 크게 다르지 않고, 사용 환경이 바뀌었다는 것을 제외하고는 이용 형태나 불법 콘텐츠 사용으로 인한 저작권 침해[2] 사례가 기존의 침해 사례와 유사하다. 스마트폰의 기술적 구조는 플랫폼인 OS-어플리케이션 소프트웨어 구조를 갖는 컴퓨터와 매우 유사한 구조를 가지고 있고 스마트폰의 이동성 때문에 불법 콘텐츠의 이용이 쉽다는 특성이 있으며 동시에 누가 침해하는지 파악하기 쉽지 않은 특성도 있다.

스마트폰에서는 기존의 모바일 디바이스에서 제공되었

던 문자메시지, 송수신 히스토리, 전화번호부, SMS 데이터등에 대한 주요 디지털 증거 뿐만 아니라 이메일 송수신 상대, 브라우저 히스토리, 채팅 로그정보, 웹브라우저 접속 관련 정보 등의 응용프로그램 기록도 중요한 정보로 제공되고 있다. 따라서, 스마트폰 포렌식은 기존의 컴퓨터 포렌식[3]과 모바일 포렌식[4]에서 적용되어오던 기술들을 응용하여 스마트폰 환경에서 발생하는 다양한 범죄 형태로부터 유용한 증거 획득 및 분석을 하기 위한 보다 발전된 기술이 필요하다.

2.2 SNS 사용 흔적 분석기술

트위터, 페이스북, 마이스페이스, 미투데이와 같은 SNS 서비스는 웹 브라우저를 통한 접근 방법을 제공하므로 웹 서핑과 같은 사용자 흔적을 남긴다. 스마트폰이 대중화 됨에 따라 스마트폰용 SNS 클라이언트를 이용해 장소의 제한 없이 접근이 가능해 졌다.

○ 웹 브라우저를 이용한 분석

SNS는 웹 기반 접근을 제공하므로 웹 브라우저 사용 흔적을 분석하여 SNS 사용 내역을 분석할 수 있다[5]. 일반적으로 웹 브라우저 사용 기록 파일에 공통으로 저장되는 정보는 캐시, 히스토리, 쿠키정보이며 그 중 히스토리 정보를 분석하여 URL 정보와 방문 시간, 방문 횟수, 검색어 등의 기록을 확인할 수 있다. SNS 접근시 기록되는 URL의 특성을 이용해 사용내역을 확인할 수 있다. 그림 1에서는 SNS사용자의 웹 브라우저 사용 URL 정보이다.

	정보	URL 정보
Twitter	방문	twitter.com/{USERACCOUNT}
	검색	twitter.com/#search?q={SEARCHKEYWORD}
	즐겨찾기	twitter.com/favorites/{FEEDNUMBER}
Facebook	방문	facebook.com/profile.php?id={ACCOUNTNUMBER}
	검색	facebook.com/search/?post_form_id={FORMID}&q={SEARCHKEYWORD}&init=quick&sid={SIDNUMBER}
MySpace	방문	myspace.com/{USERACCOUNT}
	검색	searchservice.myspace.com/index.cfm?fuseaction=sitesearch.results&orig=search_Header&origpfc=Splash&type={people,myspace,web,image,music,video}&qry={SEARCHKEYWORD}&submit=Search
Me2Day	방문	me2day.net/{USERACCOUNT}
	검색	me2day.net/search?search_at=all&query={SEARCHKEYWORD}

(그림 1) SNS 웹 브라우저 사용 URL 정보

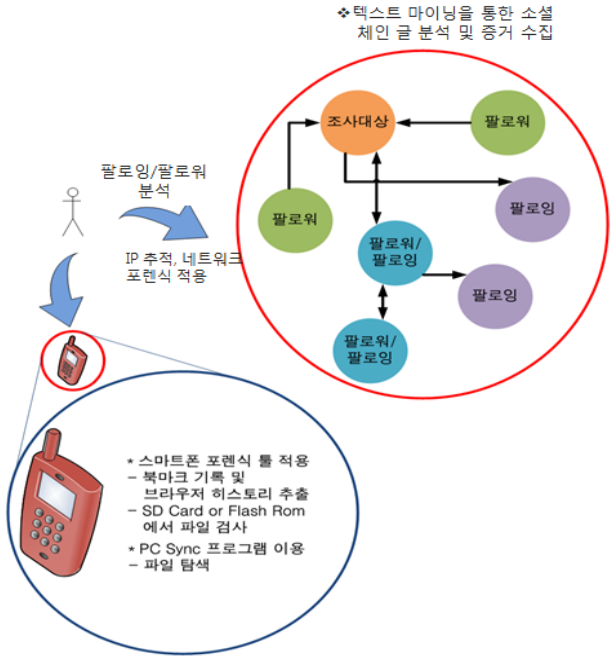
○ 물리 메모리의 SNS 데이터 분석

또한 물리 메모리 영역을 분석[6]하여 사용자 계정, 비밀 번호,메일 주소, 메신저 대화 내용, URL 주소 등의 SNS 사용 흔적을 확인할 수 있다.

3. SNS 스마트폰 내 불법 콘텐츠 식별

3.1 증거 수집 과정

본 절에서는 스마트폰을 사용한 소셜 네트워크 서비스(SNS)를 통해 불법 콘텐츠 공유 및 스마트폰에 불법 콘텐츠를 다운로드하는 행위에 대한 증거 수집 과정을 그림 2와 같이 제시한다.



(그림 2) SNS상 불법 콘텐츠 증거 수집 과정

SNS에서 제공된 불법 콘텐츠 이용 정보 및 웹사이트 접속 기록 등을 통해 스마트폰 내 다운로드 된 불법 저작물에 대한 포렌식 증거 획득단계를 그림 2에서 표시된 바와 같이 불법 콘텐츠 다운여부를 추적 및 분석이 가능하다. 팔로잉(following)은 조사대상이 친구로 추가한 사람들을 의미하고, 팔로워(followed)는 조사대상을 친구로 추가한 사람을 의미한다. 상세한 절차는 다음과 같다.

○ 우선 사용자의 스마트폰을 획득한 후 플래시 롬(Flash Rom) 상태를 확인한다. 손상·삭제된 파일이 있으면 훼손된 파일 또는 파일 시스템에 대한 복구 작업을 진행한다.

○ 스마트폰 포렌식툴을 이용한 파일 검사, 북마크 및 브라우저 히스토리 정보를 추출한다.

○ SD카드 존재 여부를 확인하고, 있다면 PC Sync[7]를 이용하여 파일을 탐색하고 스마트폰 포렌식툴을 사용

하여 파일 검사를 진행한다.

○ 불법 콘텐츠 정보 및 SNS에 대한 주소 정보나 캐쉬 정보를 획득한 후 사용자의 SNS로 가서 텍스트 마이닝을 통해 남긴 문자 데이터를 분석한다.

○ SNS에서 임의의 사용자 한명을 선택하여 사용자(조사중인 사용자)와의 친분 관계를 확인한다. 사용자와 공통점을 찾는 사람들은 높은 우선순위를 부여한다. 즉 SNS를 중심으로 저작권 침해를 일으키는 파일 공유는 친분 또는 연관이 있는 사람들 사이에서 일어날 가능성이 높기에 불법 콘텐츠 공유 혐의가 높다는 것을 의미한다.

○ 우선순위 별로 불법 콘텐츠 공유 여부에 대한 수사 작업을 수행한다.

○ 불법 콘텐츠 사용여부 및 사용자 정보를 보고서로 작성해서 보여준다.

3.2 증거 추출 실험

본 절에서는 스마트폰 포렌식 기술을 적용하여 사용자의 웹브라우저 히스토리 정보를 확인하여 해당 사용자의 증거 데이터를 추출한다. 추출과정을 아래 실험을 통해 설명한다.

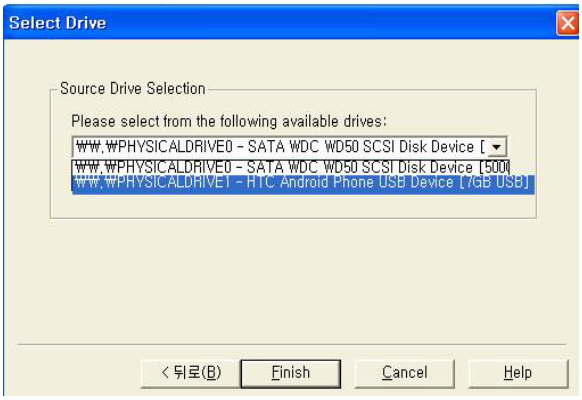
3.2.1 실험 환경

○ 스마트폰 모델명 : HTC Legend
○ 플랫폼 : Android2.1(Eclair)
○ 메모리 : ROM(512MB), RAM(384MB)
○ 포렌식툴 : AccessData's FTK Imager v3.0.0

3.2.2 AccessData's FTK Imager v3.0.0를 이용한 물리적 데이터 획득

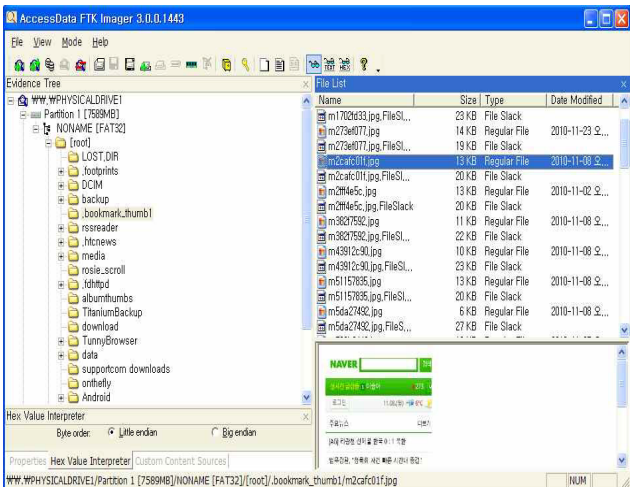
① 데이터 케이블을 이용하여 안드로이드 폰과 연결한다.

② 스마트폰 디바이스 메모리 카드 포렌식을 위해 AccessData's FTK Imager v3.0.0을 설치한 후 Source Evidence Type에서 Physical Drive를 선택 후 그림 3과 같이 안드로이드 폰을 선택 한다.



(그림 3) 물리적 디바이스 선택 정보

③ 추출된 북마크 파일 리스트는 그림 4에 표시되어 있다.

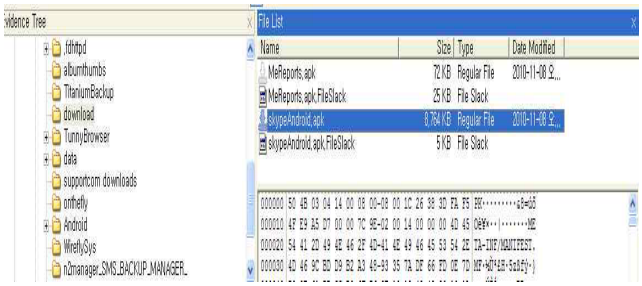


(그림 4) 북마크 파일 리스트 정보

④ 북마크 XML 정보는 그림 5에 표시된다.

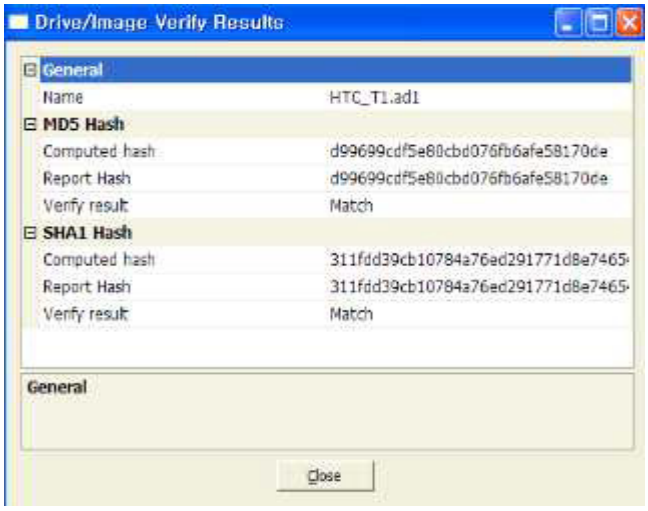
(그림 5) 북마크 파일 정보

⑤ 다운로드 파일 리스트는 그림 6에 표시된다.



(그림 6) 다운로드 파일 리스트 정보

⑥ 다운로드 된 이미지 파일에 대한 일관성 체크를 위해 그림 7에서 이미지 해쉬 값을 체크한다.



(그림 7) 일관성 체크 정보

스마트폰에서 다운로드 된 불법 콘텐츠에 관한 증거 자료를 추출하기 위한 포렌식 툴이 현재 많이 개발 되었다. 그중에서 본 연구는 추출과정을 가시화하기 위해 'AccessData's FTK Imager v3.0.0' 물리적 이미징 포렌식 툴을 사용한다. AccessData's FTK Imager v3.0.0을 이용하여 스마트폰 메모리 카드 이미징을 통해 물리메모리를 수집하고 분석하였다. FTK Imager를 이용하여 추출된 디렉토리 내의 북마크 파일 리스트, 다운로드 파일 리스트 등의 정보들에 대한 분석을 수행하였다. 실험된 결과 정보 가운데 북마크 파일 정보는 XML 파일 형태로 스마트폰 사용자가 방문한 URL 주소, 날짜 등의 정보를 제공하며, 다운로드한 파일 정보들에 대한 해쉬 값을 확인하여 일관성을 체크 한다. 체크 결과를 기반으로 침해 보고서를 작성하여 불법 행위 증거자료를 유출한다.

4. 결론 및 향후 과제

최근 스마트폰 사용자와 웹 2.0 기술이 발달됨에 따라 IT세상은 새로운 패러다임 시대를 맞게 되었다. 이로 인하여 디지털 증거 데이터를 획득할 수 있는 저장매체는 컴퓨터가 아닌 모바일 기기로 옮겨가고 있다. 본 연구는 주로 스마트폰을 통한 소셜 네트워크 서비스에서 발행하는 불법 콘텐츠 공유에 관한 포렌식을 진행 중이다. 포렌식 디지털 증거 수집 및 분석을 위한 포렌식 솔루션이 많이 존재하고 있는 현 상황에서 AccessData사에서 제공한 FTK Imager v3.0.0을 이용하여 스마트폰 메모리 카드에서 증거 수집과정을 보여주었다.

향후 연구에서는 운영체제 별 적합한 스마트폰 포렌식 기법, 다양한 포렌식툴을 비교·분석하여 증거 데이터 추출 프로세스 성능향상, 대량 증거 데이터 처리기법에 관한 연구를 계속 진행할 것이다.

참고문헌

[1] Mttiucci M, Olivieri R, "Smart & Cell Phone Forensics", ICTLAW International conference, Roma, 18 November, 2006.

[2] 하태진, 한승조, "디지털 방송 콘텐츠 복제 방지를 위한 DRM Module 설계", 한국정보기술학회논문지 제8권 제3호, 2010.

[3] Bill Nelson, Amelia Phillips, Christopher Steuart, "Guide to Computer Forensics and Investigations, Fourth Edition", 2009.

[4] Jansen, W and Delaitre, A. "Mobile Forensic Reference Materials : A Methodology and Reification", 2009.

[5] Namheun Son, Sangjin Lee, "Forensic Investigation Method and Tool Based on the User Behaviour Analysis", Proceedings of the 9th Australian Digital Forensics Conference, 2011.

[6] 申明燮, "디지털 포렌식을 위한 NAND 플래시 메모리기반의 파일 복구기법", 2010.

[7] NIST, "Smart Phone Tool Test Assertions and Test Plan", 2010.