웹 서비스 기반의 스마트폰 포렌식 프레임 워크 설계 및 구현

김형환*, 전상준*, 김도현*, 이상진*, 은성경**
*고려대학교 정보보호연구원, **한국전자통신연구원

{timemachine,heros86,exdus84,sangjin}@korea.ac.kr*, skun@etri.re.kr**

Framework for Design and Implementation of SmartPhone Forensic Based on Web Service

Hyoung-Hwan Kim*, SangJun Jeon*, DoHyun Kim*, Sangjin Lee*,
Sungkyong Un**
*Center for Security Information & Technologies, **ETRI

요 약

현재의 스마트폰 기반의 모바일 애플리케이션은 기본적인 전화, 문자와 같은 기능들 외 네비게이션과 같은 유용하고 편리한 기능들이 사용되고 있다. 이러한 애플리케이션에는 사용자와 관련된 많은 개인 정보들이 포함되어있고, 저장된 개인 정보는 사건 발생 시 사건의 직접적인 증거 혹은 간접적은 증거로 활용될 수 있다. 스마트폰에 저장된 증거를 수집하고 분석할 때 조사관들이 사용할 수 있는 기존의 도구는 복잡한 사용방법을 숙지해야 하고, 인증된 소프트웨어가 설치되어 있는 컴퓨터에서 국한되어 분석이 가능했다. 본 논문에서는 이와 같은 문제를 해결하기 위한 웹 서비스 개념의 스마트폰 포렌식 프레임워크를 제시한다.

1. 서론

생활을 편리하게 해주는 스마트폰 기반의 애플리케이션들이 등장하면서 스마트폰의 사용량이 크게 증가하고 있다. 사용자가 증가하는 만큼 많은 애플리케이션이 개발되고 있고 이러한 애플리케이션들은 사용자와 관련된 시간정보, 위치정보, 문자내역등 다양한 개인정보를 기기 내부에 특정 파일로 저장한다. 특히, SNS(Social Network Service)와 무료 SMS(Short Message Service)가 이슈가 되면서 Facebook과 Twitter, KakaoTalk 등의 서비스 애플리케이션이 많이 사용되고 있다. 이러한 애플리케이션의 사용으로 저장된 데이터들은 디지털 포렌식 조사 관점에서 사건 관련 조사 시 용의자의 행위를 파악하고, 인적네트워크 관계를 확인하여 범행 증거를 찾아낼 수 있는 중요한 단서가 된다.

따라서 디지털 포렌식 조사관은 사건 발생 시 스마트폰 내의 정보를 신속하게 추출하여 다양하게 분석할 수 있는 도구가 필요하다. 하지만 스마트폰의 정보를 추출하여 분석하는 도구가 많지 않고, 기존에 개발된 분석 도구들은 조사관의 컴퓨터에 특정 분석 도구가 조사관의 설정에 맞추어 설치가 되어 있거나, 인증을 위한 비용을 지불해야 한다. 또한 동글키와 같은 인증 메커니즘을 사용하는 경우 동글키를 분실한다면 그 소프트웨어의 기능을 100% 활용할 수 없게 된다. 이와 같은 문제를 해결하기 위해 본 논문에서는 저렴한 비용으로 다양한 환경에서 유동적으로 스마트폰 분석을 수행할 수 있는 서비스 개념의 스마트폰 포렌식 프레임워크를 제시한다. 또한 설계된 프레임워크에 따라 구현하여 실험해봤고 언급한 문제의 해결 가능성을 확인하였다.

* 본 연구는 지식경제부 및 한국전자통신연구원의 산업원천기술개발사업의 일환으로 수행되었습니다.
[10035157, 실시간 분석을 위한 디지털 포렌식 기술 개발]

2. 관련연구

iPhone 데이터를 추출하는 방식에는 물리적 방법과 논리적 방법이 있다. 물리적 방법에는 직접 iPhone에서 nand memory 추출 방법이 있고, 논리적 방법에는 물리적인 방법보다 더 많은 데이터를 추출할 수 있는 Jailbreak(탈옥)을 이용하는 방법, iPhone backup utility를 이용하는 방법이 있다[5].

2.1 Jailbreak(탈옥)을 이용한 추출 과정

iPhone 복구 모드로 초기화 한 후 커널 부트로 암호를 우회한다. Recovery toolkit은 device' s communication protocol인 AFC(Apple File Connection)을 이용하여 설치

한다. Recovery toolkit은 Open SSH, netcat tool, md5 tool, dd disk copy/image utility으로 구성되어 있다. 파일 시스템에 대한 shell access 획득이 가능하여, 전통적 방식의 포렌식 조사를 수행할 수 있다.

2.2 iPhone backup utility를 이용한 추출 방법

탈옥 없이 iPhone의 Livedata를 복사할 수 있고, 무결성을 유지할 수 있다. 기본적으로 iPhone은 미리 설정된 <표 1>의 디렉토리 위치에 백업파일을 저장한다.

<표 1> iPhone 백업파일 위치

Mac	~/Library/ApplicationSupport/MobileSync /Backup
Windows XP	\Documents and Setting\(username)\ ApplicationData\AppleComputer\MobileSync \Backup

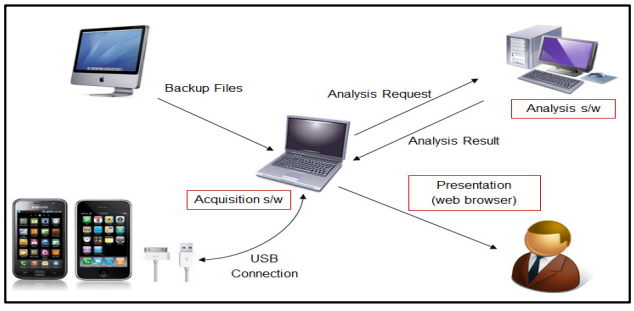
백업폴더 이름은 40문자 길이의 숫자와 문자의 조합으로 이루어져 있고, iPhone에 대한 Unique identifier을 표현하며 Unique identifier는 hashed value를 표현한다.

이 논문에서는 iPhone 데이터를 추출할 수 있는 방법을 제시하였다. 본 논문에서는 제시된 방법을 응용하여 iPhone 데이터를 추출하였고, 추출한 데이터를 분석하여 조사관이 웹브라우저에서 포렌식 조사를 할 수 있도록 서비스하는 모델을 소개한다.

3. 웹 기반 스마트폰 포렌식 도구(SPFO)

3.1 웹 기반 스마트폰 포렌식 도구(SPFO) 구조

웹 기반 휴대용 포렌식 도구인 SPFO(Smart Phone Forensic Service)는 현장에서 사건 조사에 필요한 스마트폰에서 데이터를 추출하는 추출기, 추출된 데이터를 분석하는 분석기 분석된 데이터를 웹 서버와 연동해 웹브라우저에 출력하는 출력기로 구성되어 있다. 모든 서비스는 웹 서버를 중심으로 작동 되며, 포렌식 조사관은 웹 서버에 접속하여 수집기를 다운받아 분석기와 통신한다.



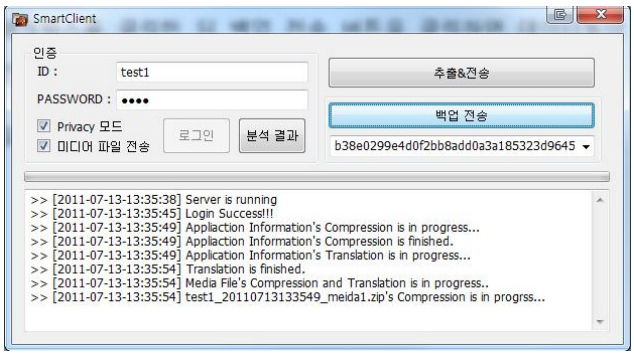
(그림 1) 아키텍쳐 구성 화면

3.1.1 추출기

추출기는 Apple iPhone iOS 초기모델부터 4.3 버전의 스마트폰 기기의 정보를 추출한다. iOS는 itunes를 이용한 백업 데이터 정보를 이용하고, 추출 가능한 애플리케이션은 <표 2>과 같고, 구현된 추출기의 모습은 (그림 2)와 같다.

<표 2> 추출 가능한 애플리케이션 항목

기본App	전화	전화번호부, 발신내역, 수신내역
	미디어	사진, 비디오
	웹브라우저	북마크, 쿠키, 접속기록, 캐시
	기타	메모, 캘린더, 알람, 지도, SMS
사용자 설치 App	SNS	Twitter ,me2day, Facebook
	클라우드 스토리지	Dropbox, Evernote, uCloud
	지도	네이버지도, 다음지도
	노트	Awesome Note
	일정관리	2Do
	Voip	Skype, Viber
	무료 SMS	Kakao Talk

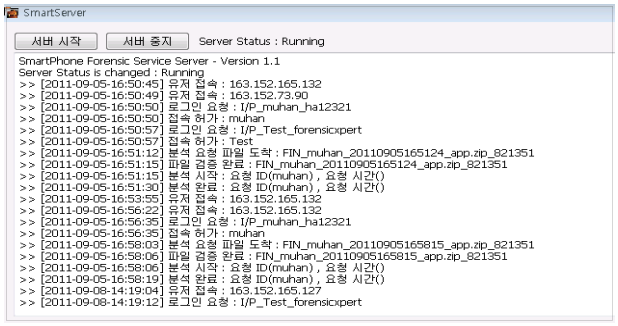


(그림 2) 추출기의 동작화면

스마트폰 사용자의 개인정보를 보호해야 할 경우, 추출된 데이터를 Privacy 모드로 전송하게 되면 일부 텍스트가 *** 로 표시되어 개인정보를 보호할 수 있다.

3.1.2 분석기

분석기는 클라이언트(추출기)로부터 받은 다양한 애플리케이션 데이터를 하나의 공통된 스키마 형식으로 통합하여 문자 및 대화내역을 분석한 contact 테이블과, 위치정보인 map_info 테이블, 인적 네트워크를 분석하여 저장한 relationship 테이블, 모든 정보를 시간순으로 정규화시킨 timeline 테이블로 구성된 sqlite 데이터베이스로 저장된다.



(그림 3) 분석기의 동작화면

3.1.3 출력기

출력기는 분석기에서 생성된 데이터를 조사관이 좀 더 직관적이고, 다양한 관점에서 분석할 수 있도록 제작된 웹사이트이다. 조사관의 인증을 위한 별도의 도구를 휴대할 필요 없이 계정정보를 이용하여 사용이 가능하며, 사건 발생시 전문소프트웨어가 설치된 컴퓨터가 없어도 신속한 조사가 가능하다.

데이터 추출직후 동일한 계정을 통하여 다른 조사관들도 시각화된 데이터의 공유 및 분석이 가능하고, 웹사이트에 출력되는 모든 데이터들은 최근 널리 사용되고 있는 스마트폰이나 테블릿pc에서도 확인할 수 있기 때문에 로컬 분석프로그램에 한정되어 분석이 가능한 한계점을 극복하여 언제 어디서든 분석이 가능한 장점이 있다.

3.2 분석기능

분석한 데이터를 출력하는 출력기(웹사이트)는 웹언어 php와 그래프 및 도표를 표현하는 flex, 분석된 데이터인 sqlite를 연동하여 제작된 사이트이다. 정보, 요약, 인적관계, 지도정보, 계정정보, 전체데이터의 메뉴로 나눠져 분석이 가능하다.

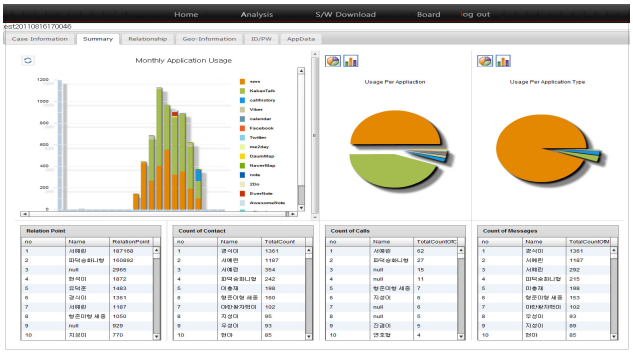
3.2.1 정보(Case Information)

Case Information메뉴는 스마트폰의 ID와 SPFO 도구의 버전, 추출된 시간과 분석 완료된 시간, Device ID 정보를 출력한다. 이 메뉴에서 조사관은 사용자 스마트폰의 기본 정보를 알 수 있다.

(그림 4) Case Information 정보 출력 화면

3.3.2 요약(Summary)

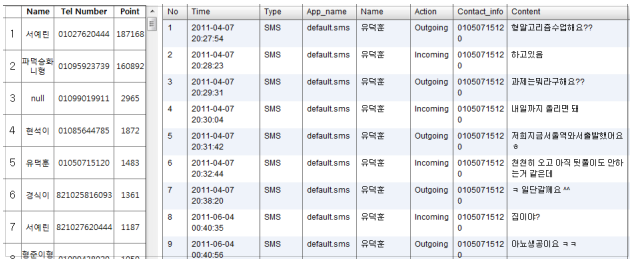
Summary에서는 스마트폰 애플리케이션의 상세 사용빈도, 사용 시간, 사용자와 사용자의 전화 및 문자 빈도를 계산하여 친밀도를 측정한 Relation Point, 전화빈도, 문자빈도 등을 (그림 5)와 같은 인터페이스로 조사관들에게 좀 더 직관적인 조사를 할 수 있도록 구축하였다. 한 화면에 평소에 자주 연락하는 사람과 즐겨 사용하는 애플리케이션 사용 시간 등을 알 수 있어 분석된 정보의 전반적인 내용을 파악하는데 유용하다.



(그림 5) 웹브라우저 출력기의 Summary 출력화면

3.3.3 인적관계(Relationship)

Relationship 메뉴는 전화, SMS, SNS에 공통적으로 저장되어 있는 이름과 전화번호를 사용하는 모든 애플리케이션의 데이터를 통합하였고, Relation Point를 기준으로 순위를 나열하고, 해당 순위에 따른 통신 내역을 화면에 출력한다. 스마트폰 사용자의 통화와 문자등 사용 내역을 기반으로 주변인에 대한 친밀도 순위나, 전반적인 인적관계를 추론할 수 있다.



(그림 6) 웹브라우저 출력기의 Relationship 화면

3.3.4 지도정보(Geo-Information)

Geo-Information은 NaverMap 애플리케이션과 Daum-Map 애플리케이션을 사용자가 실행 후 특정 지역을 검색

하였을 때 스마트 폰 내부에 검색 정보가 저장되는 것을 추출하여 분석한 화면이다. 정보는 (그림 7)과 같이 시작 위치, 시작위치의 위도와 경도, 도착위치, 도착위치의 위도와 경도, 검색 시간, 사용한 애플리케이션과 같은 조사관점에서 매우 중요한 정보들을 확인할 수 있다.

No	Time	AppName	Action	StartPoint
1	2011-06-09 00:40:38	navermap	RouteSearch	서경빌딩

	StartPointLatitude	StartPointLongitude	Destination	DestinationLatitude	DestinationLongituc	SearchC
2	127.022872924805	37.5884399414062	고대병원앞	127.027198791504	37.5861396789551	
3	127.022872924805	37.5884399414062	동대문운동장	127.01099395752	37.5673027038574	
4	127.02075958252	37.5842628479004	동대문운동장	127.01099395752	37.5673027038574	
	505678.0	1136311.0	서울 종로구 인사동	497560.0	1130870.0	1

(그림 7) 웹브라우저출력기의 Geo-Information 일부 화면

3.3.5 계정정보(ID/PW)

인터넷 사용자 중에는 사이트 마다 계정정보를 동일하게 사용하는 경우가 있는데, 이런 경우 계정정보만으로 온라인에서 사용자의 활동 계획과 활동 내역을 추론할 수 있다. ID/PW 메뉴에서는 AwesomeNote, Ucloud, Viber 애플리케이션을 사용하였을 때 사용자의 스마트폰에 아이디와 비밀번호가 평문으로 저장되는데, 이 데이터를 추출한다.

No	Application_Name	ID	PassWord
1	AwesomeNote	fait[illegible]	jjy[illegible]5
2	AwesomeNote	fait[illegible]	c5[illegible]ns
3	AwesomeNote	Aw[illegible]Note P[illegible]de	25[illegible]
4	ucloud		

(그림 8) 추출된 ID/PW 출력화면

3.3.6 전체 데이터(AppData)

포렌식 조사관이 서비스를 제공하는 분석 내용에 따르지 않고, 통합 데이터베이스에 저장된 통화내역, 문자 calendar note, map, sns등 추출된 모든 애플리케이션 데이터를 분석할 때 이용할 수 있다.

2011-06-08 23:30:29	Call	default.callhistory	Incoming	010[illegible]120	30
2011-06-08 22:44:42	SMS	default.sms	Incoming	010[illegible]79	니랑 한잔해야되는데ㅋㅋㅋ 소맥이 먹을만해
2011-06-08 22:44:39	SMS	default.sms	Incoming	010[illegible]79	니랑 한잔해야되는데ㅋㅋㅋ 소맥이 먹을만해
2011-06-08 22:12:34	Call	default.callhistory	Outgoing	010[illegible]35	04:05
2011-06-08 21:05:37	SMS	default.sms	Incoming	010[illegible]54	전화 하셨엇어요?
2011-06-08 19:21:10	SMS	default.sms	Outgoing	010[illegible]58	지금강남에해동관련세미나왔어ㅋㅋ
2011-06-08 19:20:04	Call	default.callhistory	Incoming	010[illegible]35	12
2011-06-08 18:46:20	SMS	default.sms	Incoming	010[illegible]58	어디세요?ㅎ
2011-06-08 18:00:41	Call	default.callhistory	Outgoing	010[illegible]35	0
2011-06-08 17:57:25	Call	default.callhistory	Incoming	010[illegible]37	16
2011-06-08 16:37:44	Call	default.callhistory	Outgoing	010[illegible]77	59

(그림 9) AppData 출력화면

4. 결론 및 향후 계획

본 논문에서는 기존의 로컬 컴퓨터에서만 국한되었던 스마트폰 포렌식 분석에서 웹브라우저를 이용하여 서비스 개념의 스마트폰 포렌식 분석이 가능함을 보였다. 디지털 포렌식 조사과정에서 스마트폰 분석이 필요할 경우 유용하게 사용 될 수 있을 것으로 기대된다, 차후 스마트폰에서 삭제된 데이터를 복구한 데이터가 분석된다면 더욱 효율적이고 정확한 포렌식 수행이 가능할 것이다. 따라서 스마트폰에서 삭제된 데이터를 복구하는 추가적인 연구가 필요하다.

참고문헌

[1] Mohammand Iftekhar Husain “iForensics : Forensic Analysis of Instant Messaging on Smart Phones” NY 14260-2000.

[2] Appli-iPhone-Mobile phone.iPod and Internet device. http://www.apple.com/iPhone/

[3] How to Jailbreak Your iPhone in Under a Minute. http://www.appleiPhonereview.com/iPhone-tutorials/iPhone-jailbreak/

[4] Williamson, B., Apeldoorn, P., Cheam, B., and McDonald, M. (2006). Forensic analysis of the contents of nokia mobile phones. In Australian Digital Forensics Conference. Edith CowanUniversity.

[5] Mona Bader, Ibrahim Baggili, PhD, iPhone 3GS Forensics: Logical analysis using Apple iTunes Backup Utility, SEPTEMBER 2010.

[6] 이승봉, 권혁돈, 임경수, 이상진, 웹 브라우저 사용 정보 분석을 위한 도구 설계 및 구현, 디지털 포렌식 연구, 한국디지털포렌식학회, 2008.