Smart Phone OS별 포렌식 기술과 도구에 관한 연구

이보만* · 박대우*

*호서대학교 벤처전문대학원

A Study of Forensic Techniques and Tools on Smart Phone OS Types

Bo-Man Lee* · Dea-Woo Park*

*Hoseo Graduate School of Venture

E-mail : bomans@nate.com □ prof1@paran.com

요 약

iPhone과 갤럭시S의 국내 출시와 함께 Smart Phone의 국내 시장이 활성화 되면서 사용자들이 증가하고 있다. 이에 따라 기존의 휴대폰 관련 범죄 증거 자료 수집을 위한 포렌식 기법으로는 새 기술과 WiFi 등 Convergence된 Smart Phone에 대한 모바일 포렌식 기술 연구가 필요하다. 본 논문에서는 Smart Phone OS별 포렌식 기술과 도구 연구를 위해, iPhone Apple MAC OS X와 갤럭시S Google Android를 연구한다. Smart Phone OS별 포렌식 기술로는 SYN 방식을 이용하여 포렌식 기술을 연구하고, 모바일 포렌식을 하기 위해 컴퓨터 포렌식 방법과 도구들을 살펴보고 포렌식 적용 방법을 연구한다. 본 논문 연구가 IT 강국으로서 한국의 Smart Phone 포렌식 기술 발전에 기여할 것이다.

ABSTRACT

iPhone and Smart Phone domestic markets are activated with domestic coming out of galaxy S together and the users are increasing. It follows hereupon and with forensic techniques for the cellular phone relation criminal evidence collection of data of existing the mobile forensic engineering research is necessary in about Smart Phone where it has become new techniques and WiFi etc. Convergence. It respects Smart Phone OS star forensic technique and a tool research, iPhone Apple MAC OS X and it researches galaxy S Google Android from the present paper. Smart it uses SYN methods with Phone OS star forensic techniques and it researches in order mobile forensic description below it observes it sees and forensic application methods computer forensic methods and the tools and it researches forensic techniques. The present paper research as IT powerful country will contribute in Smart Phone forensic technical advances of Korea.

키워드

Smart Phone, Forensic, Forensic Tool, Smart Phone Forensic

Ⅰ. 서 론

iPhone의 국내 출시로 우리나라에 Smart 시장[1]이 활성화 되었다. 최근에는 갤럭시S의 판매증가로 Smart Phone 사용자[2]가 급속하게 증가하고 있다.

Smart Phone은 데이터 통신이 가능하며, 음성통신만 가능한 전통적인 휴대폰[3]에 WAP 또는 모바일[4][5] 인터넷이 가능한 향상된 기술[6]이 Convergence되고 있다. Smart Phone에서는 무선으로 응용 프로그램을 다운로드 받아서 실행할 수 있고 타 업체에서 개발된 수많은 App 응용 프로그램들을 동작시킬 수 있다. Smart Phone에서는 EMS, MMS, 이메일 전송, MPEG 및 MP3, 소셜 네트워크 서비스[7] 등이 구현됨에 따라 사용자들이 Smart Phone에서도 인터넷 PC에 버금가는 기능들을 체험할 수 있다.

이와 같이 Smart Phone에서 다양한 기능을 할 수 있게 된 것은 Smart Phone 용 운영 체제가 탑재되었기 때문이다. 현재 단말기에 탑재되고 상용으로 성공하고 있는 Smart Phone 운영 체제는 Symbian OS, Apple MAC OS X, Google

Android, Microsoft Windows Mobile 등이 있으나, 국내에서 많이 사용되는 단말기의 운영체제[8]는 Apple MAC OS X, Google Android이다.

기존의 일반 휴대폰이 Smart Phone 으로 대체되면서, 스마트폰 보안[9]에 대한 관심과 기존 휴대폰 관련 범죄 사실을 증거 자료로 수집하는 모바일 휴대폰 포렌식만으로는 Smart Phone 포렌식을 효과적으로 하기 어렵기 때문에 Smart Phone을 위한 포렌식의 필요성이 증대 되고 있다.

따라서 본 논문에서는 Smart Phone 범죄 관련 증거 자료 추출 및 수집을 위하여 Smart Phone OS 별로 포렌식 기술을 연구한다. 또한 기존의 휴대폰 포렌식 분야에서 사용하는 포렌식 기술 및 도구에서 SYN방식을 응용한 모바일 Smart Phone 포렌식 기술을 이용한 방법들을 연구한다. Smart Phone 포렌식 도구와 Smart Phone DB에서 정보를 추출할 수 있는 컴퓨터 포렌식 도구인 Final Data[10], EnCase[11] 등의 포렌식 기술을 연구하고자 한다.

II. 관련 연구

2.1. Google Android

Google에서 개발한 Linux OS 기반의 개방형 휴대폰용 플랫폼으로 오픈소스이기 때문에 개발자들이 편리하게 사용할 수 있다. OHA를 구성하여 구글 서버스에 최적화된 OS 이고, 단말기를 위한 소프트웨어 스택으로 OS, 미들웨어, 어플리케이션으로 구성되며 어플리케이션은 Java VM에서 실행한다.

그림 1. Google Android Smart Phone

2.2. Apple MAC OS X

Apple사가 Mac OS X를 기반으로 만든 모바일 OS로서 iPhone, iPod, iPad 의 OS로 사용되고 있다. iPhone OS 는 OS layer, Service layer, Media layer, Touch layer의 4개 주요 가상 layer로 구성되어 있으며, safari 웹 브라우저를 사용하고, 메일 링크 및 pdf 파일 이용이 가능하다. Apple 전용 OS 이기 때문에 다른 OS 와의 호환이나 개발에 있어 어려움이 있다.

그림 2. Apple MAC OS X
iPhone, iPad

2.3. Windows Mobile

Windows CE 위에 .NET Compact Version을 올린 것으로 Visual Studio 통합 개발 환경과 연동하여 개발이 가능하며 Native Head File 및 다양한 Library File을 제공한다. 또한 Kernel, Middleware, AEE, Application Suite 사이에 소프트웨어 스택을 지원한다.

그림 3. Windows Mobile
Smart Phone

III. Smart Phone OS별 포렌식 기술 적용

3.1. Apple MAC OS X

3.1.1 Apple MAC OS X 실험 환경

- Smart Phone : iPhone 4
  - 운영체제 : iPhone OS
  - 통신 프로그램 : iTunes
  - 제조사: Apple
- 컴퓨터 사양
  - 운영체제 : Windows 7 / 32 bit
  - CPU : intel(R) Core(TM) i3 CPU
  - RAM : 4.0 GB

3.1.2 SYN 방식

SYN 방식을 이용, iTunes 프로그램을 사용하여 iPhone 4 Smart Phone을 연결하였다. 그림 10처럼 iPhone 4 에서는 음악, 동영상, 책, 응용프로그램 등을 확인 할 수 있으며, 동기화 방식을 사용하여 컴퓨터의 데이터를 iPhone에 저장하는 방식을 사용한다. 하지만 폐쇄적인 iPhone OS의 구조상 iPhone 4에서 자료를 추출하는 방법은 찾을 수 없었다.

그림 4. SYN 방식으로 보여지는
iPhone4의 내용

3.1.3 포렌식 도구 적용방법 연구

iPhone 4 Smart Phone을 컴퓨터에 연결 했을 시, iPhone 4에 내장된 카메라 기능이 인식되어 그림 5처럼 휴대용 장치, 즉 카메라로 보여지는 것을 알 수 있다. Windows 탐색기로 iPhone 4의 안을 살펴보면, iPhone 4 자체는 인식이 되지만, 사진만이 보여지고 추출이 가능하다.

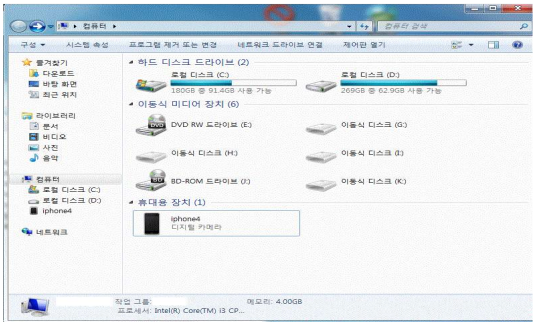

그림 5. iPhone 4 사진 추출

3.2. Google Android에 대한 적용 방법

3.2.1 Google Android 실험 환경

- Smart Phone : 갤럭시 S
  운영체제 : Android 2.1
  통신 프로그램 : Kies
  제조사 : 삼성전자
- 컴퓨터 사양
  운영체제 : Windows 7 / 32 bit
  CPU : intel(R) Core(TM) i3 CPU
  RAM : 4.0 GB

3.2.2 SYN 방식 적용방법 연구

SYN 방식으로 Kies 프로그램을 이용, Smart Phone을 연결하면 그림 8와 같이 휴대폰에 들어 있는 연락처, 문자 등의 메시지, 사진, 메모, 일정 관리, 콘텐츠, 시간표 등을 확인하고 추출 할 수 있다. 그렇지만 SYN 방식으로는 갤럭시 S Smart Phone 포렌식을 위한 삭제된 파일의 확인이나 복원 할 수 있는 방법이 발견되지 않았다.

그림 6. SYN 방식으로 추출된
갤럭시 S의 포렌식 자료

3.2.3 포렌식 도구 적용방법 연구

갤럭시 S Smart Phone을 컴퓨터에 연결 했을 시, 갤럭시 S의 메모리를 일반 하드 드라이브처럼 인식이 되는 것을 발견 하였다.

그림 9처럼 일반 하드 드라이브처럼 갤럭시 S의 카메라, 무비, 미디어, Pdf, Text, 사진, 컨텐츠, Ebook등의 폴더가 존재하고 있음을 알 수 있다.

따라서 여기서는 일반 하드드라이브 및 폴더와 같이 포렌식 수사도구의 적용이 가능하다는 것을 알 수 있다.

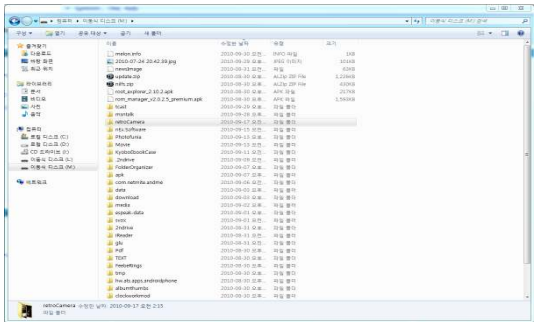

그림 7. 갤럭시 S의 메모리 포렌식 데이타 추출

IV. Smart Phone 포렌식 도구 분석

4.1. Smart Phone 포렌식 도구

Smart Phone의 포렌식 도구는 다음의 표 1과 같이 정리하였다.

표 1. Smart Phone 포렌식 도구

포렌식 도구	특 징
Device Seizure	데이터에 따른 파싱된 결과 제공 MD5, SHA-1 해쉬 및 HTML 보고서
UFED	SIM 카드/외부 장치에 대한 다양한 수집 메모리 덤프로 파일시스템 논리적 추출
MacLock Pick	백업 디렉토리가 주요 수집 대상 Smart Phone직접 연결 없이 사용
WOLF	논리 데이터 복사 2G 및 3G 지원 Firmware 1.0 ~ 2.0
CellDEK	포터블 포렌식 장비 USB 인터페이스를 이용하여 데이터 취득
Physical DD	Firmware 덮어쓰기 Raw Image 획득 Signature 기반 Carving

4.2. 컴퓨터 포렌식 도구

4.2.1. Final Data

Final Data는 그림 8과 같은 복구를 전문으로

하는 툴 킷으로서 Smart Phone에서의 DB를 복제하여 삭제되거나, 나타나지 않는 통화기록, SMS, MMS, 사진 동영상 등의 증거자료를 수집하기 위하여 FinalData 을 사용한다. 휴지통을 비운 경우, 포맷한 경우, 파티션을 지운 경우의 복구가 가능하며 전 파일 미리 확인 기능, 파일 삭제 관리 마법사, 폴더 보호 기능, 이메일 파일 복구 기능, Microsoft Access 복구 기능, Linux 파일 시스템 지원 (EXT2 / EXT3), Mac 파일 시스템 지원 (HFS / HFS Plus) 등의 기능을 제공한다.

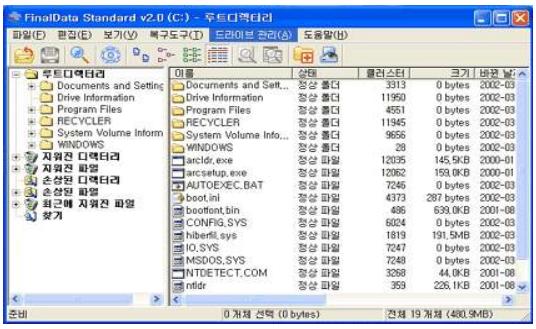

그림 8. Final Data 포렌식 도구

4.2.2. EnCase

EnCase는 그림 9와 같은 통합 도구로써 Smart Phone에서의 DB를 복제하여 삭제되거나, 나타나지 않는 통화기록, SMS, MMS, 사진 동영상 등의 증거자료를 수집하기 위하여 압수 수색된 Smart Phone에서 포렌식 자료를 추출한다. 또한 EnCase는 법정에서 증거자료로 인정이 된 예가 있다.

EnCase의 고급 기능은 원본 디스크의 복사 및 사본 작성, 데이터복구, 증거자료 보존과 탐색, 운영체제의 로그, 패턴, 해쉬, 서명 분석, 북마크, 발견물 관리, 보고서 작성, 암호 복호화 기능(옵션), 휴지통, 전자우편, IP, 전화번호 등 추출, 인터넷 히스토리 분석이 가능하다.

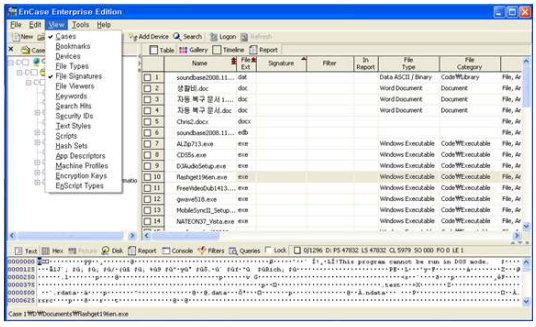

그림 9. EnCase 포렌식 도구

V. 결 론

Smart Phone 시대의 도래가 기존의 휴대폰을 Smart Phone으로 대체 시켜 가면서, 기존의 휴대폰 관련 범죄 사실을 증거 자료로 수집하는 모바일 휴대폰 포렌식만으로는 Smart Phone 포렌식을 효과적으로 하기 어려워 Smart Phone에 적합한 포렌식 기술과 도구의 연구가 필요하다.

본 논문에서는 Smart Phone 범죄 관련 포렌식 증거 자료 추출 및 수집을 위하여 Smart Phone OS 인 Apple MAC OS X, Google Android를 SYN방식을 응용한 포렌식 기술을 실험하고, Smart Phone DB에서 포렌식 자료를 추출 할 수 있는 Smart Phone 포렌식 도구와 컴퓨터 포렌식 도구인 Final Data와 EnCase를 이용하여 분석하였다.

향후연구로는 Smart Phone에서 포렌식 자료를 추출 할 때 포렌식 자료의 무결성, 안전성, 등을 확보하는 방안에 관한 연구가 이루어져야 한다.

참고문헌

[1] 제갈병직, “스마트폰 시장과 모바일 OS 동향”, 시스템-반도체포럼, pp 9~18, 2010
[2] 김태한, “스마트폰 시대의 사용자 환경”, 한국정보과학회, 제28권 제6호, pp 27~31, 2010
[3] 이규안, 박대우, 신용태, “휴대폰 압수수색 표준 절차와 포렌식 무결성 입증”, 한국통신학회논문지, 제33권 제6호, pp 512~519, 2008
[4] 강동호, 김기영, “개방형 모바일 환경에서 스마트폰 보안기술”, 한국정보보호학회, 제19권 제5호, pp 21~28, 2009
[5] 김진환, 조혁규, 서창진, 차의영, “스마트폰용 동적 서명인증의 모바일 구현”, 한국해양정보통신학회, 제11권 제9호, 2007
[6] 김동민, 이칠우, “스마트폰 사용자 인터페이스 기술 동향“, 한국정보과학회, 제28권 제5호, pp 15~26, 2010
[7] 강대기, 장원태, “스마트폰 상에서 프로젝트 관리를 위한 소셜 네트워크 서비스 기반의 일정 통지 및 이슈추적 시스템”, 한국해양정보통신학회, 제14권 제3호 pp 669-677, 2010
[8] 이상윤, 이환구, 김우식, 이재호, 김선자, “스마트폰 운영 체제 개발 동향”, ETRI, 제19권 제6호, 2004
[9] 정현철, 김미주, 최은영, “스마트폰 보안 강화를 위한 방안 연구”, 한국인터넷정보학회, pp 781~785, 2010
[10] FinalData, http://www.finaldata.co.kr/
[11] EnCase, http://www.encase.com/