

# Smart Phone O.S. 분석 및 콘텐츠 저작권 위반과 포렌식 자료 추출

박 대 우\*

\*호서대학교 벤처전문대학원 IT응용기술학과

## 목 차

- I. 서론
- II. Smart Phone O.S. 분석
- III. Smart Phone 콘텐츠 저작권 위반
- IV. Smart Phone 탈옥 & 루팅 & 언락
- V. Smart Phone Forensic 자료 추출
- VI. 결론

## I. 서론

최근 정보기술(IT) 업계 이슈 중 하나는 Smart Phone 시장이다. 삼성전자와 LG전자 등 국내 기업을 비롯해 노키아, 소니에릭슨, HP까지 올해 Smart Phone을 앞 다퉈 내놓고 경쟁하고 있다. 글로벌 휴대전화 업체들이 Smart Phone 시장에 집중하는 이유는 전 세계 수십억 대에 달하는 휴대전화 시장이 점차 포화상태에 이르고 있기 때문이고 Smart Phone은 기존 휴대전화 시장을 대체할 수 있는 블루오션이다.

최근 Smart Phone 시장이 확산되는 것은 전 세계적인 3세대 이동통신 기술의 발전과 밀접한 연관이 있다. 음성통신 및 데이터통신을 모두 빠른 속도로 할 수 있는 3세대 이동통신 기술은 Smart Phone의 가치를 높여 주었다. 이전에 등장한 PDA폰도 기본적으로 Smart Phone이 할 수 있는 기능을 모두 제공했지만 3G에서 빨라진 데이터통신은 외부에서 인터넷 웹서핑과 e메일 확인을 더 유용하게 해주고 있다.

그림 1에서는 Smart Phone으로 분류되는 단말 시장의 성장세를 예측한 것인데, 2008년도에 약 1억 5천만 대에 못 미치던 Smart Phone시장의 규모가 2014년도에는 약 3억 7천만대 이상으로까지 성장할 것이라고 예측하고 있다. 2008년 대비 2014년까지 전체 이동통신단말 시장은 약 25% 정도가 증가할 것이라고 전망하는데 반해서, Smart Phone 시장은 150% 가까이 증가할 것이라고 예상하고 있다. 또한 2014년에는 궁극적

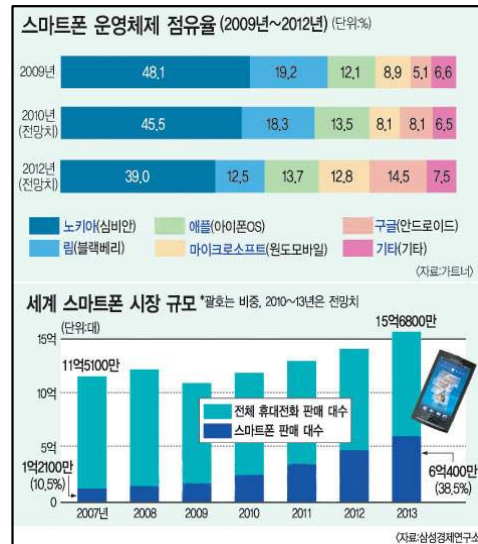


그림 1. Smart Phone 운영체제 점유율과 세계 시장 규모

으로 전체 이동통신단말의 20% 이상을 Smart Phone이 차지하게 된다고 전망하고 있다[1].

최근 Smart Phone 시장이 확산됨에 따라 Smart Phone에 대한 보안 위협도 확산되고 있다. 특히 Google Android가 탑재된 Smart Phone의 경우 Google Android가 개방형 O.S.(operating system) 라서 O.S. 자체의 취약점을 공격하는 행위가 발생할 가능성이 높다. 그리고 Windows Mobile의 경우에도 Windows의 취약

점들을 가지고 PC라는 매체에서 Smart Phone으로 옮겨진 것뿐이라서 기존의 가지고 있는 취약점을 그대로 가지고 있다.

## II. Smart Phone O.S. 분석

Smart Phone[2]은 PC와 같은 기능과 더불어 고급 기능을 제공하는 휴대전화로써, 어떤 사람들에게는 응용 프로그램 개발자를 위한 표준화된 인터페이스와 플랫폼을 제공하는 완전한 운영 체제 소프트웨어를 실행하여 전화나 e-mail, Internet, e-book, Game, Social Application, 내장형 키보드나 외장 USB 키보드, VGA 단자를 갖춘 고급 기능이 들어있는 소형 컴퓨터라 볼 수 있다.

### ■ Apple MAC O.S. X

Apple사가 Mac O.S. X를 기반으로 만든 모바일 O.S. 로서 iPhone, iPod, iPad 의 OS로 사용되고 있다. iPhone O.S. 는 O.S. 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 O.S. 이기 때문에

다른 O.S. 와의 호환이나 개발에 있어 어려움이 있다. 그림 2는 Apple MAC O.S. X를 탑재하여 출시된 iPhone의 제품 사양이다.

### ■ Google Android

Google에서 개발 한 Linux O.S. 기반의 개방형 휴대용 플랫폼(Android의 SDK를 2007년 11월 12일 공개) OHA(Open Handset Alliance)를 구성하여 구글 서비스에 최적화된 폰으로 UI, Application Layer 개발을 구글이 주도하고, 그 밖의 Kernel 개발은 GPL 진영의 소스를 이용하여 개발하였다. 단말기를 위한 소프트웨어 스택으로 O.S., 미들웨어, 주요 어플리케이션으로 구성되고 Application은Java VM으로 실행되고, 버추얼 머신은 Linux Kernel 위에서 돌아가는 Dalvik(재사용과 교체가 가능한 App framework으로 모바일 디바이스에 최적화된 Dalvic virtual machine)을 사용하였고 오픈소스의 Webkit 엔진 기반의 통합된 브라우저와 2D 그래픽 및 OpenGL ES 1.0 스펙 기반의 3D를 지원하는 최적화된 그래픽 지원한다[3]. 그림 3은 Google에서 Android를 개발하여 처음으로 Smart Phone으로 출시된 htc사의 Nexus One의 제품 사양이다.

항목	분석결과	설명
Multitasking	미지원	향후 버전에서 지원
OPEN OS	X	
OPENS API	0	<a href="http://developer.apple.com/iphone/library/navigation/index.html">http://developer.apple.com/iphone/library/navigation/index.html</a>
안전한 콘텐츠 공급 프로세스	0	<ul style="list-style-type: none"> <li>Apple 자체적으로 강력한 검증 프로세스 보유</li> <li>코드 서명은 의무화되어 있음</li> </ul>
네트워크 보호 기술	제공	<ul style="list-style-type: none"> <li>WPA/WPA2 Personal / Enterprise제공</li> <li>TLS/SSL, VPN기술제공</li> </ul>
기타 보안 이슈		<ul style="list-style-type: none"> <li>Sandbox 기반시스템: 각 어플리케이션은 아이폰내 안전한 공간에 설치되며, 다른 어플리케이션에서 접근을 할 수 없도록 OS가 설계 되어 있음</li> <li>Jailbreak : OS V3.1.3 이전버전에서 존재하는 아이폰 해킹 방법으로 애플 앱스토어에 의해 인가 되지 않은 어플리케이션의 설치 및 실행이 가능 하도록함, 해킹된 펌웨어 설치를 통해 root 권한을 획득 가능함.</li> </ul>

그림 2. iPhone 스펙

항목	분석결과	설명
Multitasking	지원	
OPEN OS	0	<a href="http://source.android.com/">http://source.android.com/</a>
OPENS API	0	<a href="http://developer.android.com/">http://developer.android.com/</a>
안전한 콘텐츠 공급 프로세스	△	<ul style="list-style-type: none"> <li>• Google 자체적으로 강력한 콘텐츠 검증 절차부재</li> <li>• 코드 서명은 의무화 되어 있음</li> </ul>
네트워크 보호 기술	제공	<ul style="list-style-type: none"> <li>• WPA/WPA2 Personal / Enterprise제공</li> <li>• TLS/SSL, VPN기술제공</li> </ul>
기타 보안 이슈		<ul style="list-style-type: none"> <li>• Permission 기반 <b>Secure Sandbox</b> 기반시스템: 타 <b>Application</b>의 <b>Permission</b> 없는 요청을 거부할 수 있기에 어플리케이션간 간섭이 발생할 수 없음</li> <li>• <b>User ID &amp; File Access</b> : 다른 어플리케이션의 데이터 접근 불가</li> <li>• Linux 기반 OS인 Android의 Root 권한을 획득하는 해킹 방법 존재</li> </ul>

그림 3. Nexus one 스펙

■ Windows Mobile

Windows CE 위에 .NET Compact Version을 올린 것으로 Visual Studio 통합개발환경과 연동하여 개발이 용이하며 Native Head File 및 다양한 Library File

제공하고 Kernel, Middleware, AEE, Application Suite사이에 완벽한 소프트웨어 스택 지원한다[3]. 그림 4는 Windows Mobile 6.1버전을 탑재하여 출시된 Show OMNIA의 제품 사양이다.

항목	분석결과	설명
Multitasking	지원	
OPEN OS	X	
OPENS API	0	MSDN 사이트를 통해 제공
안전한 콘텐츠 공급 프로세스	△	<ul style="list-style-type: none"> <li>• MS 별도 검증프로세스 부재</li> <li>• OS자체 코드서명이 존재하지만, 서명이 안된 프로그램에 대해 사용자가 설치를 허락할 경우 설치 가능</li> </ul>
네트워크 보호 기술	제공	<ul style="list-style-type: none"> <li>• WPA/WPA2 Personal / Enterprise제공</li> <li>• TLS/SSL, VPN기술제공</li> </ul>
기타 보안 이슈		<ul style="list-style-type: none"> <li>• 현재까지 12종의 바이러스 발견</li> <li>• Key Hooking API 공개를 통해 키보드 보안 이슈 존재</li> <li>• 친숙한 Windows 기반 데이터 관리 구조로 되어 있음</li> </ul>

그림 4. Show OMNIA 스펙

### III. Smart Phone 콘텐츠 저작권 위반

저작권법은 새로운 저작물을 창작할 때 다른 사람의 저작물에서 그 사상이나 창작 방법을 자유롭게 사용하는 것을 용인하고 있다. 보호받는 저작물을 저작권자의 허락 없이 또는 허락범위를 넘어 무단 이용하였을 때에는 저작권위반을 구성하게 된다.

기존의 저작물을 이용하여 새로운 작품을 만드는 행위는 첫째, 기존의 저작물에 의거하여 그대로 베껴거나 다소 수정, 변경이 있지만 기존의 저작물과의 동일성을 인정 할 수 있고 새로운 창작성이 부가되지는 아니한 경우, 둘째, 기존의 저작물을 토대로 하여 만들어진 작품에 새로운 창작성이 인정되지만 한편으로 기존의 저작물에 대한 종속적 관계가 인정되는 경우, 셋째, 기존의 저작물을 이용하였지만 단순히 시사 받은 정도에 불과하거나 또는 그것을 완전히 소화하여 작품 화함으로써 기존의 저작물과 사이에 동일성이나 종속적 관계를 인정할 수 없는 독립된 작품이 된 경우 등으로 분류할 수 있다[4][5][6].

#### ■ Smart Phone에서 저작물 다운로드 방법에 따른 침해 유형

인터넷 PC나 무료 WiFi Zone을 통해 Smart Phone 용 불법 저작물들을 유통하고 이를 PC에서 Smart Phone으로 전송하는 방식이다. 이에 대응하기 위해서는 헤비 업로드에 대한 모니터링 및 단속과 OSP 자체적으로도 필터링을 적용하거나, 불법소득자에 대해서도 적극적인 고소, 고발, 처벌에 대한 조치를 취해야 한다.

WCDMA(Wideband Code Division Multiple Access) 기반의 Smart Phone에서 저작권 침해는 개인이 소지하면서 이동하는 특성으로 인해 저작권 침해가 발생했는지 파악하기 어려워, 기본적으로 관련 저작권 침해 서비스에 대해 모니터링과 단속을 강화하는 방법과 사용자들 인식 전환에 대한 홍보와 교육이 함께 수반되어야 한다.

#### ■ 한미 FTA 체결과 지적재산권보호에 따른 Smart Phone 저작권

한미 FTA(Free Trade Agreement) 협정문에서 지적재산권에 있어 세계 경쟁력을 갖고 있는 미국이 한미 FTA 협상에서 지적재산권 강화의 성과가 표 1

과 같이 협정문 공개로 드러났다[7][8][9].

표 1. 한미 FTA 지적재산권 분야 협정문 주요 내용

지적재산권(IPR) 분야 협정문 주요 내용	
저작권 강화	보호기간 저작자 사후 70년까지 연장 연장시점은 협정문 발효 후 2년 유예 정부 정품 저작물 사용 의무화
일시적 저장에 대한 복제권 인정	‘공정한 이용’은 예외 인정
상표권 강화	상표 사용권의 등록요건 폐지 냄새, 소리 상표 인정 증명표장제도 도입
불법 촬영 금지	영화관 도촬촬영 시도만 해도 법적처벌
위조라벨 유통 금지	상품 포장 뿐 아니라 라벨도 형사처벌
범죄수의 몰수	저작권 침해에 대해서도 몰수 인정 지금까지 상표권 침해행위에 한해 인정
대학가 불법복제 감독 강화	저작물 불법 복제 집행수준 강화 합의 서적무단인쇄 금지 등 공공캠페인 실시

### IV. Smart Phone 탈옥 & 루팅 & 언락

#### ■ 탈옥(Jail Breaking)

iPhone의 잠금장치를 해제하는 것으로, 불법 어플리케이션 다운로드의 온상이다. 불법 어플리케이션 유통으로 애플 매출액 손실액 4억 5천만 달러 추정하고 있다(2010. 1.14, 아이뉴스24). 그림 5는 iPhone 4G를 탈옥한 그림이다.



그림 5. iPhone Jailbreak

■ 루팅(Rooting)

안드로이드 O.S.의 Root 권한을 획득하는 것으로 애플리케이션의 외장메모리 저장과 멀티터치 기능을 할 수 있게 해주고, 사용자가 원하는 형태로 O.S. 환경을 변경 가능하게 해주는 것이다. 개방형 구조인 안드로이드폰 특성상 iPhone에 비해 복잡하게 사용가능하며, O.S.를 조작하는 시도로 새로운 위협요소 가능성이 있다. 그림 6은 갤럭시S를 루팅한 그림이다.

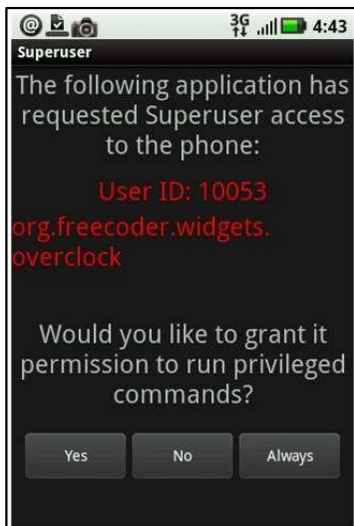


그림 6. Android Rooting

■ 언락(Unlock)

윈도우 모바일 폰의 언락을 통해 잠겨져 있는 기능을 사용할 수 있고, 롬업을 할 수 있거나 해외에서도 사용가능하게 USIM도 변경을 할 수 있으며, 카메라 소리를 무음으로 하거나 벨소리나 문자음을 음악파일형식으로 된 파일들을 사용할 수 있게 된다. 그림 7은 옴니아를 언락할 수 있는 T\*옴니아의 스마트튠 그림이다.



그림 7. 옴니아용 스마트튠

V. 스마트폰 포렌식 자료 추출

모바일 포렌식은 디지털 포렌식의 일종으로 휴대폰, 노트북, PMP, PDA 등의 모바일기기와 이동장치인 차량, 선박, 기차, 비행기 등에 장착된 블랙박스과 같은 이동장치를 대상으로 하여 범죄나 수사에서 디지털 증거를 수집, 식별, 추출, 보존, 문서화하여 법정에 제출하는 일련의 행위를 말한다. 외국의 경우에는 'Mobile Forensics'라는 명칭을 사용하거나 각각의 대상에 따라 'Mobile Phone Forensics' 또는 모바일 기기와 디지털카메라를 이용한 첨단기술자료 유출, HSDPA의 'Cell Phone Forensics', 'PDA Forensics' 등의 세부적인 명칭을 함께 사용한다[10][11][12].

■ iPhone SYN 방식

SYN 방식을 이용한 iTunes 프로그램을 사용하여 iPhone 4 Smart Phone을 연결한다. 그림 8처럼 iPhone 4에서는 음악, 동영상, 책, 응용프로그램 등을 확인 할 수 있으며, 동기화 방식을 사용하여 컴퓨터의 데이터를 iPhone에 저장하는 방식을 사용한다.



그림 8. SYN 방식으로 추출된 iPhone4의 내용

■ Android Phone SYN 방식 적용방법 연구

SYN 방식으로 Kies 프로그램을 이용, Smart Phone 을 연결하면 그림 9와 같이 휴대폰에 들어있는 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.

갤럭시 S Smart Phone을 컴퓨터에 연결 했을 시, 갤럭시 S의 메모리를 일반 하드 드라이브처럼 인식이 되는 것을 발견 하였다. 일반 하드 드라이브처럼 갤럭시 S의 카메라, 무비, 미디어, Pdf, Text, 사진, 콘텐츠, Ebook등의 폴더가 존재하고 있음을 알 수 있다. 따라서 여기서는 일반 하드드라이브 및 폴더와 같이 포렌식 수사도구의 적용이 가능하다는 것을 알 수 있다.

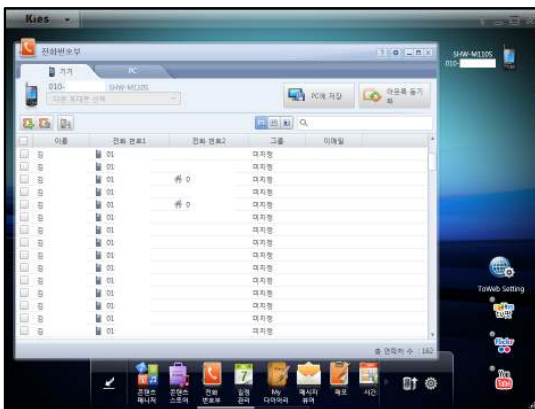


그림 9. SYN 방식으로 추출된 갤럭시 S의 포렌식 자료

■ Smart Phone 포렌식 도구

Smart Phone의 포렌식 도구는 다음의 표 2와 같이 정리하였다.

표 2. 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 Phone 직접 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

■ Final Data

Final Data는 그림 10과 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.

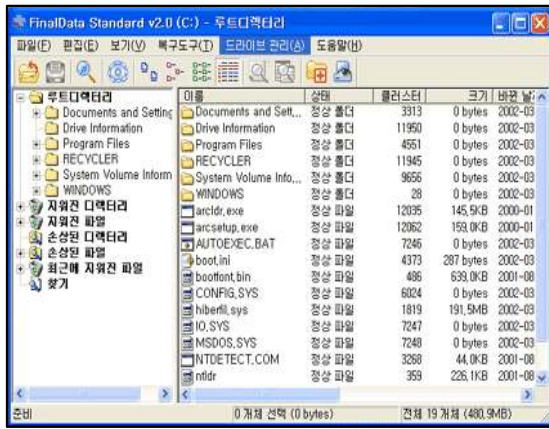


그림 10. Final Data 포렌식 도구

■ EnCase

EnCase는 그림 11과 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.

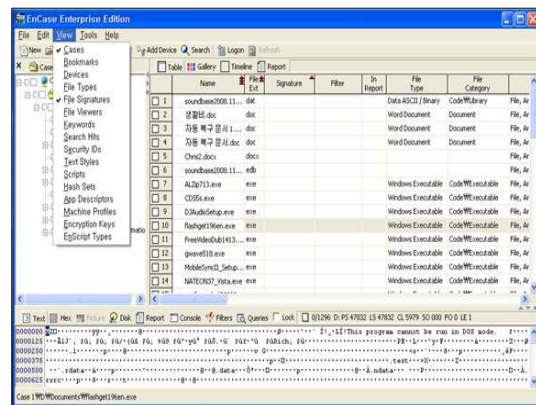


그림 11. EnCase 포렌식 도구

■ Smart Phone 포렌식 자료 추출

갤럭시S와 옴니아에서 포렌식 자료를 추출할 때 업체에서 제공해주는 백업 프로그램으로 포렌식 데이터를 추출하였다. 이 데이터들은 동기화라는 개념에서 현재 있는 데이터를 포렌식 자료화 한 것이다. 따라서 삭제된 데이터에 대한 포렌식 자료를 추출하기 위해서 그림 12와 같이 포렌식툴을 사용하여 삭제된 그림이나 동영상, 문서 파일들을 복원하여 포렌식 자료로 사용할 수 있다.

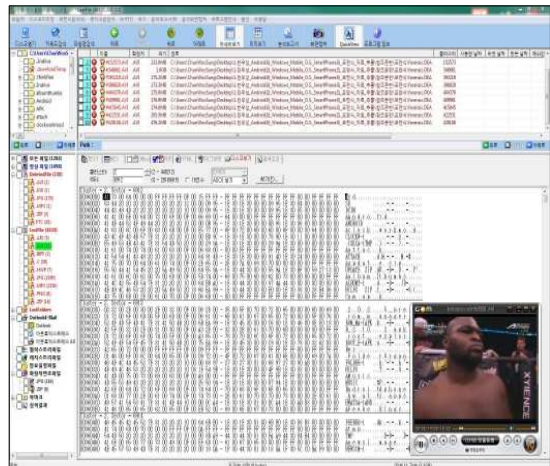


그림 11. 삭제된 데이터 복구

갤럭시S와 옴니아에서 포렌식 자료를 추출하였는데 Smart Phone은 PC와 동기화라는 것을 하기 때문에 PC로의 백업을 하는 자체가 포렌식 자료를 추출하는 방법이 된다.



그림 12. Smart Phone 포렌식 자료 추출

그림 12와 같이 Smart Phone을 PC와 동기화 하는 과정에서 법적 자료로 인증되기 위해 과정을 사진자료로 날짜가 나오도록 하고 백업된 데이터의 무결성을 입증하기 위해 이미징 작업을 해야한다.

### VI. 결 론

PC기반의 OS를 축소하고 축으로 가지는 Smart Phone의 OS가 탑재되어 잇는 Smart Phone의 확산으로 인해 기존의 가지고 있던 PC기반의 OS의 문제점들은 매체만 틀려진 Smart Phone에서도 역시 문제점을 가지게 된다. 그리고 휴대폰의 장점인 휴대성이 있어 범죄에 활용도도 높아지면서 Smart Phone의 보안 취약성이 나타나게 된다.

Smart Phone 사용자가 Jail Breaking과 Rooting을 통하여 Smart Phone에서 저작권을 위반하거나 침해 사건이 발생하고 있다. 이러한 위반 사고들을 막고 개발자의 저작권이나 손해를 보지 않기 위해 콘텐츠에 DRM(Digital Rights Management)을 적용시키는 작업이 활발하게 이루어지고 있다.

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.

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 추출할 수 있는 Smart Phone 포렌식 도구를 이용하여 분석한다.

Smart Phone에서 포렌식 자료를 추출 할 때 포렌식 자료의 무결성, 안전성 등을 확보하는 방안과 Smart Phone 파일포맷의 표준화 추출과 분석에 관한 기법을 지속적으로 연구하여 포렌식 자료 분석 및 여러 기종의 Smart Phone으로부터 포렌식 자료를 추출하고 분석 할 수 있도록 하여야 한다.

### 참고문헌

- [1] 한경매거진, “스마트폰 시장이 열린다 - 2015년 휴대전화 추월 ... 신제품 ‘붐물’”, 환경비즈니스, 11-676호, pp. 12-14, 2008.
- [2] Ravi Kalakota, Marcia Robinson, M-Business : Race to the Mobility, McGraw-Hill Companies, 2001.09.
- [3] 오석표, 최인호, “스마트폰의 OS 및 특장점 비교 분석 연구”, 대한전자공학회 하계학술대회, 제 33 권 제 1호, pp. 2002-2007, 2010.
- [4] 편석환, “영상저작물의 저작권 침해에 관한 연구”, 한국콘텐츠학회, 제7권, 제6호, pp.107-118, 2007.
- [5] J.A.L. Sterling, World Copyright Law, Sweet&Maxwell, pp.228-229, 2003.
- [6] 박홍진, “저작권침해의 구제에 관한 연구”, 한국법학회, 제19권, pp.409-427, 2005.
- [7] Industry Trade Advisory Committee on Intellectual Property Rights (ITAC-15), The U.S. - Korea Free Trade Agreement (FTA): The Intellectual Property Provisions, Report of the Industry Trade Advisory Committee on Intellectual Property Rights (ITAC-15), 2007.
- [8] 박덕영, “한미 FTA협정 저작권 분야 주요내용과 국내이행”, 새창출판사(창작과권리), pp.128-154, 2007.
- [9] 관계 부처 합동, “한미 FTA 상세설명자료,” 2007.
- [10] 김기환, 박대우, 신용태, “모바일 포렌식에서의 무결성 입증방안 연구”, 한국컴퓨터정보학회, 제15 권, 제1호, pp.37-46, 2007.
- [11] Wayne Jansen, Rick Ayers, “Guidelines on Cell Phone Forensics,” NIST, Draft Special Publication 800-101, 2006.
- [12] S.Y. Willassen, “Forensic analysis of mobile phone internal memory,” IFIP, vol. 194, pp.191-204, 2005.



## 저자소개

박 대 우 (Dea-Woo Park)



1998년 숭실대학교 컴퓨터학과  
(공학석사)

2004년 숭실대학교 컴퓨터학과  
(공학박사)

2006년 정보보호진흥원(KISA) 선임연구원

2007년 ~ 현재 호서대학교 벤처전문대학원 조교수

※ 관심분야 : 포렌식, 해킹, 정보보호, 유비쿼터스  
네트워크 및 보안, 보안시스템, CERT/CC, Hacking,  
VoIP 보안, 이동통신 및 WiBro 보안