Android/Windows Mobile Smart Phone의 취약점 분석과 Mobile Forensic 기술

천우성°, 박대우*
°*호서대학교 벤처전문대학원 IT응용기술학과
e-mail: deux8522@gmail.com · prof1@paran.com

A Study of Vulnerability Analysis and Mobile Forensic Technology about Android/Windows Mobile Smart Phone

Woo-Sung Chun°, Dea-Woo Park*
*Dept. of IT Application Technology, Hoseo Graduate School of Venture

● 요 약 ●

Smart Phone의 OS로 많이 사용하는 Android/Windows Mobile Smart Phone의 사용이 급격히 증가하고 있다. 무료 WiFi Zone과 인터넷 사용에 대한 취약점이 존재한다. Mobile Forensic의 증거 자료를 추출하는 방법은 SYN, JTAG, Revolving 방법이 있지만, 기존 휴대폰과 달리 Smart Phone은 OS와 구조, 사용방식과 기술의 차이로 인한 Mobile Forensic 연구 방법도 달라야 한다. 본 논문에서는 Smart Phone에서는 많이 사용되는 Windows Mobile/Android Smart Phone의 OS와 구조 차이를 분석한 데이터 백업과 스펙 분석 및 증거자료 분석을 한다. 또한 무료 WiFi Zone을 통한 인터넷 사용시에 취약점을 분석한다. 그리고 Android/Windows Mobile Smart Phone의 Forensic 자료를 생성하여 증거를 추출하고, Mobile Forensic 보고서를 생성한다. 본 연구를 통하여 Mobile Forensic의 기술 발전에 초석을 제공할 것이다.

키워드: Smart Phone, Mobile Forensic, Windows Mobile, Android

I. 서론

그림 1의 세계 스마트폰 시장 규모에서 2007년도에 전체 10.5%로 약 1억 2,100만대 규모인 스마트 폰 시장의 규모가 2013년도에는 약 6억 400만대 이상으로까지 성장할 것이라고 예측하고 있다. 2007년 대비 2013년까지 전체 이동통신단말 시장은 약 25% 정도가 증가할 것이라고 전망하는데 반해서, Smart Phone 시장은 150% 가까이 증가할 것이라고 예상하고 있다. 또한 2013년에는 전체 이동통신단말의 38.5%를 Smart Phone이 차지하게 될 것으로 전망하고 있다[1].

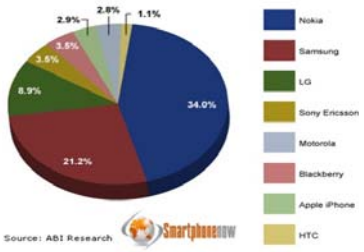

그림 4. Smart Phone 운영체제 점유율과 세계 시장 규모
Fig. 1. Smart Phone operating systems, and global market share

2.5세대 휴대폰에서 음성통신 및 데이터통신 등 멀티미디어 통신과 APP 프로그램을 사용하는 3세대 이동통신 기술이 발전하였다. 여 업무를 편리하게 이용 할 수 있는 Smart Phone의 가치를 높여 주었다. 특히 2010년 Smart Phone 시장이 급속히 성장하는 것은 3세대 이동통신 기술의 발전과 휴대인터넷을 사용하려는 편리성과 연관이 되어 있다.

3G에서 빨라진 데이터통신은 외부에서 인터넷 웹서핑과 e메일 확인, 지도 찾기, 스케줄관리 등 개인 이 Smart Phone을 이용하여 기존의 인터넷 PC가 수행하던 업무를 Smart Phone으로 대체하고 있다.

또한 기존의 휴대폰 시장이 포화상태에 이르고 있기 때문이고 Smart Phone으로 처리 할 수 있는 업무의 발달과 휴대인터넷을 사용하려는 편리성과 연관이 되어 있다. 기존 휴대폰 시장을 대체할 수 있는 블루오션이다.

또한 Smart Phone 운영체제도 기존의 심비안에서 Google Android와 Windows Mobile OS가 확대될 것으로 전망하고 있다. 특히 Android Smart Phone의 경우 개방형 OS 라서 상대적으로 OS 자체의 취약점을 공격하는 행위가 발생할 가능성이 높으며, Windows Mobile의 경우에도 기존에 밝혀진 Windows의 취약점들을 지니고 있는 OS로서 Smart Phone에서의 취약점에 대한 공격이 예상된다. 또한 Smart Phone의 사용이 급속히 증가하

고, 이동 단말기의 휴대성과 사용의 편리성으로 범죄에 이용이 높아지면서 Smart Phone의 Mobile Forensic에 대한 연구가 필요하다[2][3].

본 논문에서는 본 논문에서는 Google Android와 Windows Mobile Smart Phone의 취약점 분석을 위하여 Smart Phone 스펙과 OS 분석, 데이터 분석을 연구 한다. 또한 WiFi Zone을 통한 무료 인터넷 사용시에 취약점을 분석한다.

그리고 Google Android와 Windows Mobile Smart Phone의 증거자료를 추출하고, Mobile Forensic 보고서를 생성하여 범죄로 부터의 증거자료를 생성하고, 법정의 증거로 사용 할 수 있는 기술에 대한 연구를 한다[4].

본 논문의 구성은 Ⅰ장 서론에서는 논문의 필요성과 Ⅱ장 관련 연구에서는 Windows Mobile, Google Android, Mobile Forensic에 대해 연구하고, Ⅲ장 Smart Phone 데이터 백업과 스펙 및 취약점 분석에서는 Windows Mobile 데이터 백업, Google Android 데이터 백업, Smart Phone 스펙과 무결성 검증, Smart Phone WiFi Zone에서의 무료 인터넷과 취약성 분석을 하고, Ⅳ장 Windows Mobile과 Google Android Smart Phone Forensic 자료 생성 보고에서는 Windows Mobile Smart Phone Forensic 자료 생성, Google Android Smart Phone Forensic 자료 생성, Smart Phone Forensic 자료 생성, Smart Phone Forensic 보고서 작성을 하고, Ⅴ장 결론으로 이루어져 있다.

Ⅱ. 관련연구

2.1 Android

Google에서 개발 한 Linux OS 기반의 개방형 휴대폰용 플랫폼(Android의 SDK를 2007년 11월 12일 공개)으로 OHA(Open Handset Alliance)를 구성하여 Google 서비스에 최적화된 플랫폼으로 UI, Application Layer 개발을 Google이 주도하고, 그 밖의 Kernel 개발은 GPL 진영의 소스를 이용하여 개발하였다. 단말기를 위한 소프트웨어 스택으로 OS, 미들웨어, 주요 어플리케이션으로 구성되고 Application은 Java VM으로 실행되고, 버츄얼 머신은 Linux Kernel 위에서 돌아가는 Dalvik(재사용과 교체가 가능한 App framwork으로 Mobile 디바이스에 최적화된 Dalvic virtual machine)을 사용하였고 오픈소스의 Webkit 엔진 기반의 통합된 브라우저와 2D 그래픽 및 OpenGL ES 1.0 스팩 기반의 3D를 지원하는 최적화된 그래픽 지원한다[6].

2.2 Windows Mobile

PDA 및 스마트폰에 사용하는 운영 체제로 포켓 PC라고 불렸다. 이 운영체제는 마이크로소프트사에서 내놓은 Mobile 운영체제로 임베디드용 운영 체제인 Windows CE 위에 .NET Compact Version을 올린 것으로 Visual Studio 통합개발환경과 연동하여 개발이 용이하며 Mobile 환경에 적합한 새로운 터치식 사용자 인터페이스를 추가하여 개발되고 있으며, 윈도 CE의 기본적인 기능에 휴대전화 기능이 추가되어 있고 Native Head File 및 다양한 Library File 제공하고 Kernel, Middleware, AEE, Application Suite사이에 완벽한 소프트웨어 스택을 지원한다[5].

2.3 Mobile Forensic

Mobile Forensic은 기존의 휴대폰 Forensic과, 새로운 스마트폰 Forensic, 그리고 이동기기에 대한 자동차 Forensic, 기차 Forensic, 선박 Forensic, 비행기 Forensic 등으로 구분 할 수 있다[6]. 하지만 기존의 Forensic 현장의 경험과 Forensic 실무에 적용하기 위한 임의의 분류는 아래와 같다.

1) 휴대폰(mobile phone)의 음성 및 SMS 기록 자료
2) PDA(Personal Digital Assistant)의 자료
3) Digital Voice Record의 자료
4) 디지털카메라와 휴대폰의 사진 및 동영상 자료
5) 차량, 선박, 기차, 비행기 등 이동기기들의 전자기록 자료
6) 이동저장장치에 부가된 전자자료 등

Mobile Forensic의 특징은 디지털 장비 중에서 이동성을 부여한 것이고, 대표적인 것으로는 휴대폰, PDA, 디지털 녹음기, 디지털 카메라와 이동기기 등에 임베디드 시스템이 활용되는 분야라고 할 수 있다. 특히 휴대폰은 전 세계적으로 가장 많이 사용하는 Mobile 장비이고, 무선 네트워크가 구성되어 있으므로 Mobile Forensic에서 압수수색 등 절차 상 가장 유의하여야 하는 분야다[7].

Ⅲ. Android/Windows Mobile Smart Phone 취약점 분석

3.1 Android 데이터 저장

Android OS를 탑재한 갤럭시S는 삼성 Mobile에서 제공하는 프로그램인 Kies를 사용하여 Smart Phone 환경에 최적화된 프로그램으로 멀티미디어가 강화된 S/W로 컨텐츠 매니저, 컨텐츠 스토어, 아웃룩 동기화 등 다양한 기능을 지원한다. 별도의 USB 인식 유틸리티를 받을 필요없이 Kies만 설치하면 PC에서 Smart Phone의 자료를 백업 할 수 있다. 그림 3은 Kies 프로그램을 사용하여 갤럭시S에서 문자메세지를 백업받은 PC의 폴더에서 확인한 것이다.

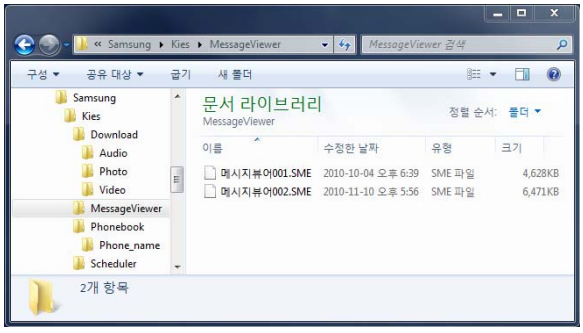

그림 3. 갤럭시S 백업 파일
Fig. 3. Galaxy S file backup

백업된 데이터를 살펴보면 문자메세지의 경우 .SME 파일로 압축되어 저장이 되고, 폰북에 경우에는 .SPB 파일로 압축되어 저장되고, 스케줄의 경우 .SSC로 압축되어 저장이 되어진다. 그리고 멀티미디어 자료들은 원형 그대로 저장되는 것을 볼 수 있다.

3.2 Windows Mobile 데이터 저장

Windows Mobile OS가 탑재된 옴니아의 경우 운영체제가 Windows Mobile 6.1이라서 Windows XP에서는 ActiveSync 4.5, Windows VISTA나 Windows 7의 경우에는 Windows Mobile Device Center를 통해 Smart Phone과 USB로 연결을 하면 인식을 하고 프로그램이 작동을 한다. 업체에서 제공하는 USB 통합 드라이버를 설치하면 삼성 Mobile에서 제공하는 MITs Store Installer에 PC 유틸리티에 있는 MITs Wizard 3.0을 PC에 설치하여 Smart Phone과 동기화 하여 이메일이나 전화번호부나 문자 등을 PC에 백업 받을 수 있다.

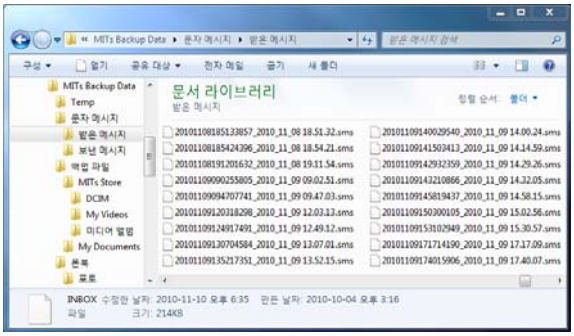

그림 2. 옴니아 백업 파일
Fig. 2. Omnia file backup

그림 2에서와 같이 옴니아에서 백업받은 문자메세지 파일을 PC에서 확인 할 수 있다.

3.3 Smart Phone 스펙과 무결성 검증

옴니아 스펙은 모델명 : SCH-M490, CPU : Marvall Monahans PXA312 806MHzLV, 메모리 : Internal 160MB, 운영체제 : Microsoft Windows Mobile 6.1, 통신규격 : DMA HSDPA으로 구성되어 있다.

갤럭시S 스펙은 모델명 : SHW-M110S, CPU : S5PC111 1GHz, 메모리 : 512MB RAM, 16GB Storage, 운영체제 : Android Platform ver 2.1(Eclair), 통신규격 : WCDMA HSPDA 7.2Mbps, HSUPA 5.76Mbps으로 구성되어있다.

Desktop 스펙은 CPU : Inter(R)Core(TM)2Quad Q9400@2.66GHz, 메모리 : 3.0GB RAM, 운영체제 : Windows 7 Ultimate K로 구성되어 있다.

Smart Phone의 경우 PC와 동기화를 하여 Smart Phone의 내용을 PC로 전송하고 그 데이터들을 똑같게 만드는 동기화를 한다. 이 동기화 과정은 Smart Phone이 켜져 있고 PC와 Smart Phone을 연결하였을 때 이루어지는 것으로, 동기화의 특성을 사용하여 백업을 하게 된다. 동기화로 백업을 정확하게 하기 위해서는 설정이 필요한데, 그 설정에 따라 Smart Phone 위주의 백업을 할것인지, PC위주의 백업을 할 것인지 결정을 하고 백업을 하게된다. 백업 과정에서는 Smart Phone이 켜져 있어야하고 Smart Phone의 데이터가 그대로 PC로 전달되기 때문에 동기화 과정 중에 Smart Phone이나 PC중 한군데에서도 틀린부분이 나오게 되면 오류메세지가 뜨게 된다.

3.4 무료 WiFi Zone에서의 Smart Phone 인터넷과 취약성 분석

Smart Phone의 기능중 하나인 WiFi를 이용하여 통신사 마다 무료로 제공해주는 WiFi Zone이 늘어나고 있다. WiFi Zone은 특성상 무선으로 서비스가 이루어 지기 때문에 이를 악용해 가짜 무선랜을 만들어 해킹을 시도할 수가 있다. WiFi 신호 중에 해킹을 위한 바이럴 SSIA(무선인터넷 식별번호) 형태의 에드혹(Ad-hoc) 네트워크를 설정하고 무선 해킹을 할 수 있다. 확장 안테나가 부착된 노트북을 WiFi Zone 이름으로 위장한 네트워크 피싱 AP모드로 전환 후 강제 연결 해제(DOS Attack)를 주기적으로 하면 사용자가 Smart Phone으로 웹 페이지 인증을 시도할 때 이미 웹 피싱 페이지에서 개인정보를 입력받을 수 있다. Smart Phone에 대한 결함이 아닌 무선 네트워크(802.11) 자체 연결 과정에서 결합 및 인증 절차 취약점과 사회공학을 이용한 Wifi Phising 공격으로 사용자 ID와 패스워드, 그리고 신용카드 정보 등 다양한 개인 정보 갈취 및 악성코드 전파가 가능하다.

IV. Mobile Forensic 자료 생성과 보고서

4.1 Android Smart Phone Forensic 자료 생성

Kies 프로그램을 사용하여 백업하는 과정에서 볼 수 있듯이 갤럭시S가 활성화 되어 있어 Kies프로그램과 동기화를 하면서 Smart Phone의 데이터와 PC에 백업 데이터가 같다는 것을 그림6과 같이 알 수 있다.

갤럭시S의 경우 문자메세지나 전화번호부같은 정보는 압축된 파일로 백업이 되지만 Kies 프로그램으로 백업받은 데이터를 볼 수가 있다.

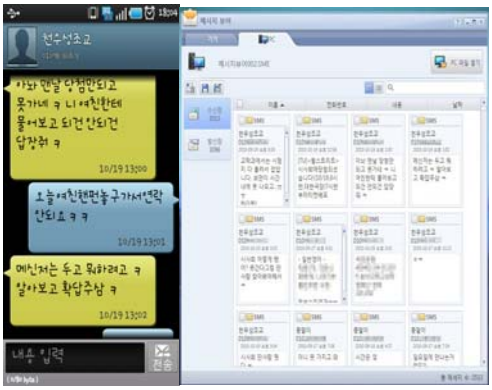

그림 6. 갤럭시S Forensic 자료 추출
Fig. 6. Galaxy S extract forensic data

4.1 Windows Mobile Smart Phone Forensic 자료 생성

동기화 특성과 백업을 통해 Forensic 자료 추출과정을 거치게 되는데 그림 4에서와 같이 동기화되어 똑같은 자료가 생성된 것을 볼 수 있다.

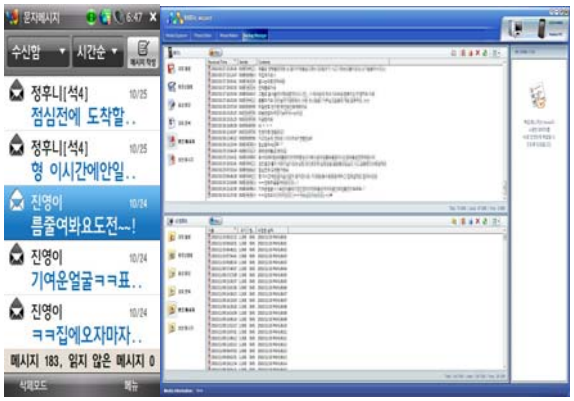

그림 4. 옴니아 Forensic 자료 추출
Fig. 4. Omnia forensic data extraction

옴니아에서는 Smart Phone 내에서는 .EDB파일로 문자메세지가 저장되는데 MITs Wizard 3.0을 사용하여 동기화하여 백업을 하게 되면 .SMS라는 파일로 PC에 저장이 되된다. 저장된 파일을 메모장으로 열어보면 그림 5와 같은 정보가 그대로 나오는 것을 볼 수 있다.

그림 5. 문자메세지 자료
Fig. 5. SMS data

4.3 Smart Phone Mobile Forensic 자료 생성

Forensic 자료를 추출할 때 각 통신사 업체에서 제공해주는 프로그램으로 Forensic 데이터를 추출하였다. 이 데이터들은 동기화라는 개념에서 현재 있는 데이터를 Forensic 자료화 한 것이다. 따라서 삭제된 데이터에 대한 Forensic 자료를 추출하기 위해서 그림 7과 같이 Forensic툴을 사용하여 삭제된 그림이나 동영상, 문서 파일들을 복원하여 Forensic 자료로 사용할 수 있다.

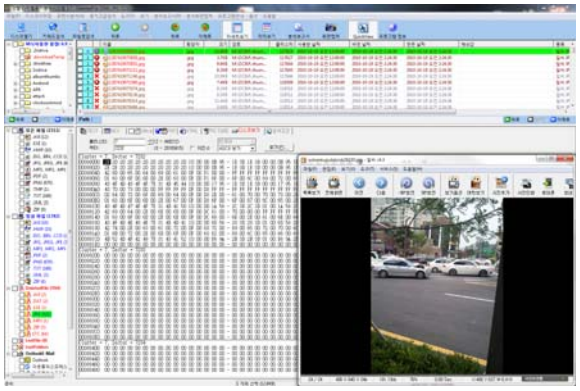

그림 7. 삭제된 데이터 복구
Fig. 7. Data recovery

갤럭시S와 옴니아에서 백업을 통해 Forensic 자료를 추출하였는데, Smart Phone이 활성화 되어 이있을 때 Smart Phone과 PC가 동기화라는 것을 하기 때문에 PC로의 백업을 하는 자체가 Forensic 자료를 추출하는 방법이 된다.

그림 8. Smart Phone Forensic 자료 추출
Fig. 8. Smart Phone forensic data extraction

그림 8과 같이 Smart Phone을 PC와 동기화 하는 과정에서 법적 자료로 입증되기 위한 과정으로 Forensic 자료를 생성하는 것을 사진자료로 날짜가 나오도록 해서 사진을 찍고 백업된 데이터의 무결성을 보장하기 위해서 이미징 작업을 한다.

4.4 Smart Phone Mobile Forensic 보고서 작성

Forensic 보고서는 법정에서 증거자료로 사용하기 위한 작업으로서, Forensic 분석 보고서를 프린트하고, Forensic 문서로 제출하기 위해 Forensic 보고서를 작성한다. Forensic 기법을 사용하여 Forensic 자료를 생성하고 백업 프로그램을 통해 추출할수 있는 데이터와 백업 프로그램을 사용하지 않고 USB로 연결시켰을 때 이동디스크 장치로만 SmartPhone을 인식하게 하고 메모리로 인식하여, 저장되어있는 자료와 삭제된 자료를 확인한다. 확인 결과를 분석 보고서에 맞춰 그림 9와 같이 작성한다. Smart Phone에서 Forensic 자료를 확인하였을 경우 증거를 수집하여 Forensic

보고서 형태로 작성한 다음, 수사에 착수하여 증거기록으로 사용한다.

V. 결론

Smart Phone의 사용이 급속히 증가하고, 이동 단말의 휴대성과 편리성으로 범죄에 이용 가능성이 높아지면서 Smart Phone의 Forensic에 대한 연구가 필요하다. Windows Mobile의 기존 알려진 OS의 취약성과 Google Android 의 공개 OS의 성격으로 취약성이 존재하므로 취약성을 분석하고, 사용중인 Smart Phone을 이용하여 데이터 백업을 하고, Forensic 자료를 생성하고 보고서를 작성하였다.

Smart Phone에서의 Forensic 자료의 생성을 위하여 Google Android의 갤럭시S와 Windows Mobile의 옴니아를 백업프로그램을 사용하여 Smart Phone의 특징인 동기화를 통하여 Smart Phone의 데이터를 백업받아 Forensic 자료 추출하고 생성하여 Forensic 보고서 작성을 하였다. 본 연구를 통하여 실험된 기술 연구는 Mobile Smart Phone Forensic 기술 발전에 기여할 것이다.

향후 연구로는 Smart Phone에서 삭제된 데이터의 복원과 원본성을 입증하는 연구를 하여 Mobile Forensic 자료의 법정 증거자료에 대한 연구가 필요하다.

참고문헌

[1] 방송통신위원회, 한국인터넷진흥원, 스마트폰 이용실태조사, pp.9, 2010.07.

[2] 제갈병직, 스마트폰 시장과 Mobile OS 동향, Semiconductor Insight, pp.9~18, 2010.05~06.

[3] 박영태, 스마트폰 가입자 절반 “PC 대신 휴대폰으로 이메일·SNS 이용”, 한국경제, 2010.09. 29.

[4] 김진환, 조혁규, 서창진, 차의영, “스마트폰용 동적 서명인증의 Mobile 구현”, 한국해양정보통신학회, 제11권 제9호, 2007.

[5] 김동민, 이칠우, “스마트폰 사용자 인터페이스 기술 동향”, 한국정보과학회, 제28권 제5호, pp 15~26, 2010.

[6] 정현철, 김미주, 최은영, “스마트폰 보안 강화를 위한 방안 연구”, 한국인터넷정보학회, pp 781~785, 2010

[7] 박대우, “스마트폰 저작권과 Forensic 적용방안,” 2010년 불법복제물 단속 유관기관 합동 워크숍, 한국저작권위원회, 2010. 5.