

## 저작권 위반과 포렌식 기법의 Smart Phone 적용 방법 연구

박대우<sup>○</sup>, 이정훈<sup>\*</sup>

<sup>○</sup>호서대학교 벤처전문대학원 IT응용기술학과

<sup>\*</sup>한국저작권위원회

e-mail: prof1@paran.com, yyyjjhh@paran.com

## A Study on Copyright Violation and Forensic Technique applying Method for Smart Phone

Dea-Woo Park<sup>○</sup>, Jeong-Hoon Yi<sup>\*</sup>

<sup>○</sup>Dept. of IT Application Technology, Hoseo Graduate School of Venture

<sup>\*</sup>Korea Copyright Commission

### ● 요약 ●

2010년에는 국내에 Smart Phone이 확산되면서, Smart Phone은 단순한 음성통신정보 전달 이외에 기존의 인터넷 PC가 정보를 전달 할 수 있는 전자책, 영화, 음악, 콘텐츠 영역으로 확장되고 있다. 하지만 Smart Phone 사용자들은 멀티미디어 저작권 콘텐츠를 불법으로 이용하고 있다. 또한 이동통신 단말로서 Smart Phone관련 범죄 증거의 생성, 저장된 디지털 증거는 증거의 활용도가 높아 모바일 포렌식 연구가 필요하다. 본 논문에서 Smart Phone에서 저작권 위반 내용들을 전자책, 영화, 음악, 콘텐츠 영역으로 조사한다. 저작권 위반 Smart Phone 증거자료를 추출하고 분석하기 위한 SYN 방식과 JTAG 방식을 연구한다. Smart Phone SYN 방식과 JTAG 방식으로 Smart Phone의 저작권 위반 자료를 추출하여 복원하고, 자료를 분석하였다. 본 연구 결과는 저작권위반 단속 기술 향상과 포렌식 수사 기술 발전에 기여 할 수 있을 것이다.

키워드: Smart Phone, 저작권 위반(Copyright Violation), Mobile Forensic

### I. 서론

방송통신위원회 통계에 따르면 휴대전화를 쓰는 세계 인구는 2008년 말을 기준으로 40억 명, 보급률은 약 61%이다. 2013년에는 세계 보급률이 90% 가까이 치솟을 전망이다. 그 중 최첨단 이동통신 강국인 대한민국은 2008년 기준으로 4,500만 명(보급률 95.2%)이 휴대전화를 쓰고 있으며, 경제활동인구를 고려하면 보급률은 100%를 웃도는 수준이다[1].

2010년에는 국내에 Smart Phone이 확산되면서 국내 모바일 IT 시장의 규모는 커지고 있으며, Smart Phone은 단순한 음성통신정보 전달 이외에 기존의 인터넷 PC가 정보를 전달 할 수 있는 영역으로 확장되어 가고 있다.

하지만 Smart Phone을 사용하는 역기능으로 개인 정보가 수집되거나 저장된 자료의 침해사고가 발생함에 따라 사이버범죄가 증가하고 있다.

표 1. 사이버범죄 발생·검거 현황

Table 1. Cyber crime · arrest Added

구분 연도	총계		사이버테러형범죄		일반사이버범죄	
	발생	검거	발생	검거	발생	검거
2003	68,445	51,772	14,241	8,891	54,204	42,881
2004	77,099	63,384	15,390	10,339	61,709	52,391
2005	88,731	72,421	21,389	15,874	67,342	56,547
2006	82,186	70,545	20,186	15,979	62,000	54,566
2007	88,847	78,890	17,671	14,037	71,176	64,853
2008	136,819	122,227	20,077	16,953	116,742	105,274

경찰청의 사이버 테러대응센터의 자료에 의하면 표 1과 같이 사이버 범죄는 매년 증가하고 있으며 이는 경찰청에 신고와 검거 등의 자료임을 감안할 때, 실제 사이버 범죄의 발생 건수는 더 많을 것으로 예상된다[2].

무어의 법칙(Moore's Law)으로 해석해 보면 과거 100년간에 저장된 정보의 량과 현재 1년에 생산되는 정보의 량이 비슷하다. 유비쿼터스 시스템 인프라가 설치되면서, 정보는 지식산업의 가치로서 유무선 통신단말기에서 디지털화 되어 전송되고 저장된다.

현재 생산되는 자료의 90% 이상이 디지털 형태로 만들어지고 있으므로, 디지털 자료 속가 범죄에 이용되고 있고, 범죄의 증거가 되는 자료를 추출하고 분석하는 디지털 포렌식은 인권보호와 과학수사의 한 축 이라고 말할 수 있다.

또한 이동 중에 업무나 생활과 관련된 정보를 이용하는 도구로서 휴대폰과 Smart Phone이 범죄에 이용되어지고 있으며, 이 결과 휴대폰과 Smart Phone에 저장된 디지털 자료는 범죄수사 과정에서 증거를 추출하는 것이 중요한 방법으로 등장하게 되었다.

최근 Smart Phone의 기능에서 다양한 어플리케이션을 사용자가 사용하기 위해 Jail Breaking을 통한 기존의 멀티미디어 자료를 사용하고 있다. 불법 어플리케이션 유통으로 애플 매출액 손실액 약 4억 5천만 달러로 추정하고 있다. 특히 동영상으로 저장되는 영화나, 게임, 음악, 전자책 등은 국가 간의 경계를 두지 않고 불법 복제되거나 해비업로드에 의해 불법적으로 다운로드 되어 사용되어 진다.

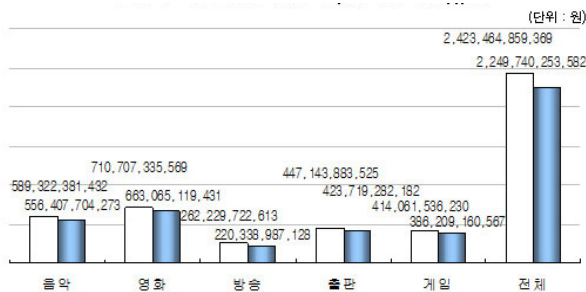


그림 1. Smart Phone에서 저작권 위반 규모  
Fig.1. copyright violation scale of Smart phone

이 결과 그림 1과 같이 Smart Phone에서 저작권 위반이 발생하고 있다. Smart Phone 저작권 침해문제는 한미 FTA(Free Trade Agreement)가 체결되면 저작권과 관련한 손해 배상 소송과 처벌의 대상이 되어 국가 간 문제로 대두될 것이다. 따라서 Smart Phone에서 저작권 침해문제와 관련한 단속과 책임의 한계를 판단하기 위한 Smart Phone 포렌식을 연구 할 필요가 있다[3].

## II. 관련 연구

### 2.1 포렌식 분류

디지털 포렌식의 절차와 기술은 현장에서부터 연구되어져, 학문적으로 명확한 구분을 하기는 어렵지만 일반적으로 사용 장치와 단말에 따라서 디스크 포렌식, 데이터베이스 포렌식, 네트워크 포렌식, 모바일 포렌식 등으로 구분하며 위치적으로 육상장비 포렌식, 해상장비 포렌식, 항공장비 포렌식, 우주장비 포렌식 등으로 나누어 생각 할 수 있다. 또한 디지털 자료의 추출하는 기법에 따라 휘발성 자료의 추출 기법과 비휘발성 자료를 추출하는 기법으로 구분 할 수 있다.

### 2.2 모바일 포렌식 종류

모바일 포렌식은 PDA, Laptop, 전자수첩, Smart Phone, 디지

털 카메라, MP3 플레이어, 휴대용 메모리카드, USB 저장장치 등 모바일기기와 이동장치를 대상으로 하여 범죄나 수사에서 디지털 증거를 수집, 식별, 추출, 보존, 문서화하여 법정에 제출하는 일련의 행위를 말한다.

수사 요원들은 범죄 증거의 가능성이 높은 Smart Phone에서의 증거 확보를 위한 압수 수색을 하여야 한다. 압수 수색한 Smart Phone의 전자파 차단은 무결성을 입증하는 조건이다. Smart Phone의 경우 소형저장장치의 효율성을 높이기 위하여 각 회사별로 별도의 메모리 저장 공간을 사용한다. Smart Phone에서 압수 수색을 진행하기 전에 전원이 켜져 있는 상태라면 Smart Phone의 사용자나 임회인에게 현재 상태를 확인한 후, 전원을 끄고 전자파가 차단되도록 되어 있는 보존봉투에 밀봉 보관하여 그 내용을 기재한 후 서명을 받도록 한다. 이때 Smart Phone의 제작사에서 제공하는 통신 프로토콜을 이용하여 컴퓨터와 Smart Phone의 자료를 전송할 수 있으므로 컴퓨터와 통신여부를 확인한 후 통신케이블, 통신 프로그램, 외장형 메모리 등도 압수하여 전자파 차단 봉투에 밀봉하고 그 내용 등을 상세히 기재하여야 한다. 만약 전원이 꺼져있다면 외관 상태와 Smart Phone의 동작 상태 등을 Smart Phone의 사용자에게 확인 후에 전자파 차단 봉투에 밀봉 보관하고 그 내용을 기재한다[4].

## III. Smart Phone에서 저작권 위반 사례

### 3.1 Smart Phone의 특징 별 범죄 가능 내용

이동통신 단말기 및 이동통신 서비스와 관련하여 자기 또는 제3자의 위법적인 이득을 위하여 이동통신 단말기 소유자 및 서비스 활용자에게 행하는 제반 범법행위라 할 수 있다. 또한 휴대폰을 수단으로 하거나 또는 그 제도를 이용하여 발생된 것으로서 형사적 제재의 대상이 될 수 있는 반사회적 위법행위라고 할 수 있다[8]. 이 정의를 바탕으로 Smart Phone의 범죄 가능성을 표 2와 같이 나열하였다.

표 2. Smart Phone의 범죄 가능성[9][10]  
Table 2. The possibility of phone crime

특징	내용
접근의 용이성	Smart Phone을 이용한 범죄는 전문적인 범죄자가 아닌 일반인도 눈앞의 경제적인 이득을 위해 손쉽게 활용할 수 있음
비인간성	사리분별이 부족한 노숙자, 장애인, 노인과 당장 급전이 필요한 사람들에게 접근하여 금전 등의 제공을 미끼로 범죄를 저지름
전문성·기술성	Smart Phone 복제 같은 경우 Smart Phone에 대한 전문적인 지식과 기술을 갖추고 있어야 가능함
광역성·국제성	명의도용 되거나 불법복제 된 Smart Phone의 경우 전국적인 유통망을 통해 거래되거나 우리나라와 동일한 방식의 이동통신망을 쓰는 국가들로 해외까지 반출됨
비대면성과 익명성	명의도용 되거나 불법복제 된 Smart Phone의 경우 전국적인 유통망을 통해 거래되거나 우리나라와 동일한 방식의 이동통신망을 쓰는 국가들로 해외까지 반출됨
시간적·공간적 무제한성	Smart Phone 통신망은 공간의 제약을 거의 받지 않고, 24시간 동안 개방됨
빠른 전파성	스팸문자는 단 한번의 조작으로 수많은 사람에게 동시다발적으로 전파가 가능함

### 3.2 도서 유출 사례

한국만화가협회와 젊은만화가가모임은 2009년 8월 31일 작가들의 저작권을 지키고 과거 불법행위에 대한 책임을 묻기 위해 100여 개 업체를 형사고발하고 민사소송도 병행 하였다. 웹 하드와 P2P 사이트에서의 저작권 침해 행위에 대한 채증작업을 진행 중이며, 한국만화출판인협회 산하 만화저작권보호협회의 자료에 따르면 2003~2008년 6년간 불법 파일 유통으로 인한 피해액은 1913억원이다[11].

### 3.3 영화 유출 사례

2009년 말 개봉한 '전우치'는 주문형비디오(VOD) 서비스를 시작한지 수일 만에 동영상 불법 유포 되었다. 영화 '용서는 없다' 제작사인 시네마서비스도 2010년 3월 11일 VOD 서비스를 시작한 지 하루 만에 영화 동영상이 인터넷에 유출돼 경찰에 고소장을 냈다. 2009년에는 '해운대'와 '박쥐' 등의 동영상이 유출 된 사례가 있었다[12].

### 3.4 음악 유출 사례

2010년 4월 9일 음저협 소속 저작권보호센터는 최근 음저협의 요청으로 웹 하드 업체 10여 곳에 대해 음악이 불법 공유되는지 여부를 모니터링 했다. 모니터링한 웹 하드 업체 대부분에서 음악이 파일이나 동영상 형태로 계속적으로 가입자들을 통해 업로드 되고 있음을 확인해 형사 고소 조치 하였다. 웹하드 사이트인 '디스크팻'과 '토토디스크'에서는 이 사이트에서 음악을 불법 다운로드 받으려는 가입자에게 신용카드나 휴대폰으로 '패킷'이나 '토토머니'라는 포인트를 구매토록 하였고, 이런 포인트를 팔아 발생한 수익을 해당 음악을 업로드한 자에게 '토토포인트' 등의 인센티브를 주는 방식으로 나누어 줬다[13].

### 3.5 콘텐츠 유출 사례

EBS는 2010년 4월 29일 (주)소프트라인(서비스명: 토토디스크), (주)나우콤(클럽박스), (주)미디어넷(짱파일, 엠파일, 파일온) 등을 포함한 18개 웹하드 업체(22개 사이트)에 대해 저작권법 위반 혐의로 서울중앙지검에 고소장을 제출했다. 이와는 별도로 EBS와 저작권 침해방지 협약을 체결한 49개 웹 하드 업체와는 기존 침해 콘텐츠에 대한 삭제와 침해 예방을 위한 상시 모니터링 조치 등을 시행하기로 했다[14].

## IV. 압수수색 Smart Phone의 저작권 위반에 대한 포렌식 기법 적용

현재 국내의 모바일 포렌식은 SMS, 전화번호부, 통화목록, 메모, 스케줄, 사진, 동영상 등의 자료는 휴대폰 단말기 플래시 메모리에 저장 되어 증거자료 분석이다. Smart Phone도 휴대폰을 모태로 발달한 이동단말기기로 휴대폰에 대한 모바일 포렌식 방법을 준용하여 연구하고 실험을 실시한다.

### 4.1 압수수색

Smart Phone에서 저작권 위반 증거 자료를 추출하기 위해서는 압수수색을 실시하여야 한다. 그림 2는 Smart Phone 압수수색 절차를 나타낸 것이다[15].

Smart Phone을 압수 수색 후에 포렌식 증거 분석을 실시 할 때, 삭제된 자료를 복구 할 필요가 있는지 결정 후, Smart Phone에서 삭제된 자료를 복구할 필요가 있을 경우, Smart Phone의 자료를 다운로드 복제하거나 원본성을 입증 할 수 있는 헤시함수값을 적용한 후에 복사본을 생성한다.

Smart Phone에서 삭제된 자료를 복구하기 위해 복제 및 복사본을 생성하였을 경우 복제 및 복사본에 대해 검사 및 복구를 시행한다. 전파차폐장치를 사용하여 통신을 차단하고 쓰기방지장치를 사용하여 노트북 및 분석 컴퓨터에 연결한다. 노트북 및 분석 컴퓨터에서 Smart Phone과 상호작용하는 응용프로그램을 실행시켜 Smart Phone에 저장된 정보를 이동한다. 추출된 Smart Phone 자료의 복사본 또는 저장한 증거 파일의 헤시 값을 확인 후 보관한다.



그림 2. Smart Phone 압수수색 절차  
Fig.2. Phone confiscated search procedures

### 4.2 모바일 포렌식 실험 환경

Smart Phone 포렌식 자료 추출을 위하여 표 3과 같이 실험 환경을 구성하였다.

표 3. Smart Phone 포렌식 증거 추출 사양  
Table 3. Smart Phone forensic evidence extracted Spec

항 목	사 양
Smart Phone	명 칭 : SCH-M490
	통신사 : SKT
	CPU : PXA270 570Mhz
	Memory : ROM- 256MB, RAM-64MB
	OS : Windows Mobile 6.0
	통신방식 : WCDMA / GSM
	사양 : 3.3형 LCD 65K / TFT LCD (Touch 지원)
	카메라 : 500만화소 카메라 / Auto Focus 지원
	영상전화/플래시
	슬롯 : MicroSD 카드 슬롯(MicroSD / MicroSDHC 지원)
PC	CPU : Intel(R) Core(TM)2 Quad CPU Q9400 @ 2,66 GHz
	Memory : 3,00GB
	OS : Windows 7 Ultimate K
	HDD : 460GB
Cable	SYN 방식 : USB케이블
	JTAG 방식 : 자체제작 케이블
추출 도구	SYN 방식 : MITs wizard
	JTAG 방식 : Trace32, JTAG 디버거

### 4.3 SYN 방식 Smart Phone 포렌식 자료 추출

SYN 방식은 통신의 프로토콜 중에서 SYN 신호를 통하여 동기 신호의 교환이 이루어진 후에 자료를 송수신하는 방식으로 Smart Phone의 제작사에서 제공하는 프로그램을 이용한다.



그림 3. Smart Phone 제작사에서 지원하는 SYN 통신 프로그램

Fig.3. SYN communications programs that are supported by the phone manufacturer

Smart Phone을 이용하여 사진, 동영상 등의 촬영을 하거나 수신된 자료를 컴퓨터에 저장하거나 다른 저장장치에 사용하기 위해서 휴대전화 단말기의 입출력 단자 접속 표준을 사용하도록 권고하고 있다. 그림 3은 Smart Phone 제작사에서 지원하는 SYN 통신 프로그램을 실행 시킨 모습이다.

Smart Phone 제조사에서 제공하는 툴을 활용하여 그림 4, 그림 5와 같이 SMS, 사진 등의 자료를 추출 한다.

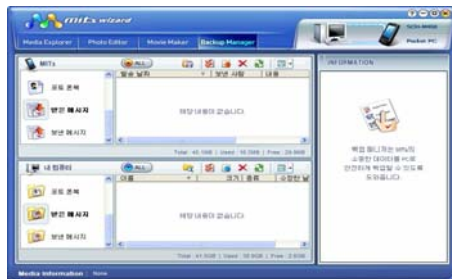


그림 4. Smart Phone 제조사의 툴을 이용한 SMS 추출

Fig.4. SMS phone manufacturers with the tools to extract

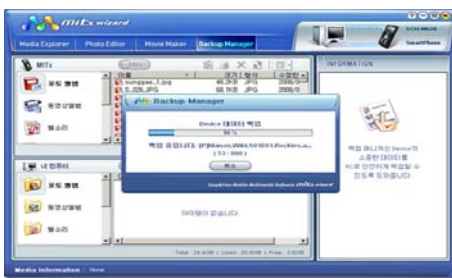


그림 5. Smart Phone 제조사의 툴을 이용한 사진 추출  
Fig.5. Using the manufacturer's tool extract phone photos

Smart Phone의 전원을 켜진 상태에서 메시지를 확인 할 수 있고 저장된 사진을 추출 할 수 있다. 하지만 삭제된 자료는 추출해 낼 수 없다. Smart Phone의 전원이 켜지지 않는 상태 일 때는 그림 6과 같이 자료를 추출 할 수 없다.

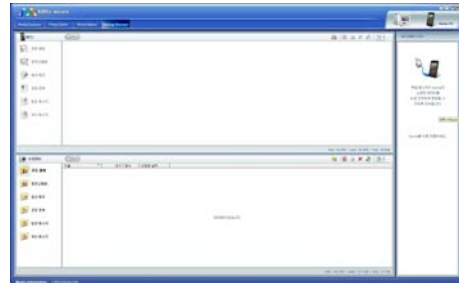


그림 6. Smart Phone 전원이 꺼졌을 때의 상황

Fig.6. What happens when the power is turned off phone

### 4.4 JTAG 방식 Smart Phone에서 포렌식 자료 추출

JTAG 인터페이스는 핀에 의해서 제어되며 회로의 배선과 소자의 전기적 연결 상태의 테스트, 디바이스간의 연결 상태 테스트, 플래쉬 메모리의 조작 등 이라고 할 수 있다. Smart Phone 자료를 추출하기 위해서는 Smart Phone의 JTAG 핀을 찾고, JTAG 디버깅 환경을 설정하고, 메모리 바이너리 자료를 획득한다.

JTAG 방식을 이용하여 SRAM과 플래쉬 메모리 부분까지 자료를 추출하는 방법은 각 제작사 및 제품별로 Smart Phone의 PCB(Printed Circuit Board)에 JTAG의 통신을 위한 포트가 존재하게 되는데 이러한 포트를 찾아내어 JTAG 핀 맵과 연결하므로 통신을 위한 인터페이스가 완성된다.

실제 실험실 환경에서 Smart Phone의 JTAG 핀을 찾고, JTAG 디버깅 환경을 설정하였으나, Smart Phone 포렌식 자료의 추출은 성공 하였으나, 자료의 분석에는 실패하였다.

### 4.5 SYN 방식과 JTAG 방식 자료 비교

SYN 방식을 이용하여 자료를 추출하는 Smart Phone 분석 방식은 삭제되지 않은 자료를 추출하기에 유용한 방법이지만 삭제된 자료를 추출하는 것은 불가능하였다. 일부 Smart Phone에서 수사에 필요한 자료가 추출되었지만 삭제된 것이 아니라 자료의 주소가 변경되어 참조주소를 추적하여 추출되는 것으로 나타났다.

JTAG 방식을 이용하여 자료를 추출하고 분석하는 기법은 SYN 방식과는 달리 전원이 꺼져 있는 상태에서 자료를 추출 하는 것이 가능하였다.

## V. 결론

Smart Phone에서 저작권을 위반하거나 침해 사건이 발생 하였을 때, Smart Phone을 압수수색 한 후에 모바일 포렌식 기술을 적용할 수 있다.

본 논문은 실험실에서 선정된 임의의 Smart Phone을 압수수색

된 Smart Phone으로 가정하고, 삭제된 저작권 위반 자료를 추출을 하는 Smart Phone 포렌식 기술을 통한 SYN 방식과 JTAG 방식을 이용하여 자료를 추출하여 비교 분석하였다. SYN 방식은 삭제되지 않은 자료를 추출하기에 유용한 방법이지만 삭제된 자료를 추출하는 것은 불가능하였고, JTAG 방식은 삭제되지 않은 자료는 추출하였으나, 추출된 자료를 분석과정을 거쳐 시각화되는 것에는 실패를 하였다.

향후 연구로는 Smart Phone JTAG 방식과 리볼빙 방식의 포렌식 자료 추출과 삭제된 자료의 분석 및 여러 기종의 Smart Phone 으로부터 포렌식 자료를 추출하고 분석 할 수 있는 포렌식 도구에 관한 기능 연구가 필요하다.

## 참고문헌

- [1] 신성원, “휴대폰 범죄의 실태 및 효율적 대응방안에 관한 연구,” 한국콘텐츠학회논문지, 6(9), 75-84쪽, 2006. 9.
- [2] 사이버범죄 발생·검거 현황, 경찰청 사이버테러 대응센터, <http://www.ctrc.go.kr>, 2010. 5.
- [3] 김윤명, “모바일 인터넷 보급에 따른 저작권 환경 변화”, 저작권문화 제187호 2010. 3. pp.10-11
- [4] 노한영, 김장성, 김광조, “포렌식을 고려한 휴대폰 개인정보 보호 기법,” 한국정보보호학회, 한국정보보호학회지, 2008.
- [5] 임경수, 박종혁, 이상진, “디지털 포렌식 현황과 대응 방안,” 보안공학연구논문지, 5(6), 461-474쪽, 2008. 12.
- [6] 김기환, 박대우, “모바일 포렌식 자료의 추출과 무결성 입증 연구,” 한국컴퓨터정보학회논문지, 12(6), 177-185쪽, 2007. 12.
- [7] 경찰청 사이버테러대응센터, “제2회 디지털 포렌식 세미나 발표자료,” 한국디지털포렌식학회, 2007.
- [8] 이규안, 박대우, 신용태, “휴대폰 압수수색 표준절차와 포렌식 무결성 입증,” 한국통신학회, 한국통신학회논문지, 33(6), 512-519쪽, 2008. 6.
- [9] 광영길, “사이버상 권리침해 실태 및 대응방안,” 한국자치행정학보, 23(1), 477-498쪽, 2009. 6.
- [10] 김홍석, “사이버 테러와 국가안보,” 한국법학원, 저스티스, 121, 319-356쪽, 2010. 12.
- [11] 아시아경제, “만화기들, 저작권 침해 웹하드 P2P사이트에 소송,” <http://www.asiae.co.kr/news/view.htm?idno=2009090107284610178>, 2009. 9.
- [12] 연합뉴스, “영화 ‘전우치’·‘용서는 없다’ 인터넷 유출,” [http://app.yonhapnews.co.kr/YNA/Basic/article/new\\_search/YIBW\\_showSearchArticle.aspx?searchpart=article&searchtext=%ec%98%81%ed%99%94%20%ec%a0%84%ec%9a%b0%ec%b9%98%20%ec%9a%a9%ec%84%9c%eb%8a%94%20%ec%97%86%eb%8b%a4%20%ec%9d%b8%ed%84%b0%eb%84%b7%20%ec%9c%a0%ec%b6%9c&contents\\_id=AKR20100324073100005](http://app.yonhapnews.co.kr/YNA/Basic/article/new_search/YIBW_showSearchArticle.aspx?searchpart=article&searchtext=%ec%98%81%ed%99%94%20%ec%a0%84%ec%9a%b0%ec%b9%98%20%ec%9a%a9%ec%84%9c%eb%8a%94%20%ec%97%86%eb%8b%a4%20%ec%9d%b8%ed%84%b0%eb%84%b7%20%ec%9c%a0%ec%b6%9c&contents_id=AKR20100324073100005), 2010. 3.
- [13] 보안뉴스, “음저첩, 웹하드 업체 2곳 저작권법 위반으로 형사 고소,” <http://www.boannews.com/media/view.asp?page=10&gpage=1&idx=20344&search=&find=&kind=0>, 2010. 4.
- [14] EBS, “저작권 침해 웹하드사에 소송 제기,” <http://about.ebs.co.kr/board/bbs?boardTypeId=1&boardId=31&cmd=view&pageNo=35&no=6&postId=1232323&searchCondition=title&searchKeyword=>, 2010. 5.
- [15] 디지털증거 처리 표준가이드라인, 경찰청, 42쪽, 2006. 12.